



Smart Attack-Resistant Internet of Things

**STATE OF THE ART IN SECURITY FOR LOW-POWER WIRELESS
MESH NETWORKS**

Thiemo Voigt, Joakim Eriksson, Niclas Finne, Joel Höglund, Nicolas Tsiftes,
Saptarshi Hazra, RISE, Sweden

Tomas Jonsson, Zhitao He, ASSA ABLOY, Sweden

Johannes Arvidsson, LumenRadio, Sweden

Anders Mattsson, Husqvarna, Sweden

George Suciu, Mari-Anais Sachian, Sorina Mitroi BEIA, Romania

Pusik Park, KETI, South Korea

JeongGil Ko, Yonsei University, South Korea

Youngki Lee, Seoul National University, South Korea

Kyung mo Kim, Security Platform, South Korea

EXECUTIVE SUMMARY

The STACK project is focused on delivering a comprehensive suite to protect wireless IoT networks from the ever-growing list of threats. These devices are typically resource constrained, making the conventional tools already available on the market unsuitable. With the goal of guaranteeing some Quality-of-Service for the networks, even during periods of active attacks, it is important to limit the scope of which attack vectors that the project should focus on.

This white paper describes the state of the art in security for wireless mesh networks. We start by motivating why we focus on mesh networks while, for example, long-range low-power networks such as LoRa are getting attention. We then provide a list of potential attack vectors that the project deems interesting to protect against. The different vectors are divided into six different categories: Jamming, Sniffing, Flooding Spoofing, Routing Protocol Attacks and Remote Code Execution. These generalized topics are presented in a manner which is focused on reader comprehension, rather than implementation-specific details.

In the Jamming chapter, attacks which are based on frequency-specific jamming are presented. This category is focused on attacks which can be performed with little knowledge of the networks' implementations. The Sniffing chapter will primarily focus on attacks which relate to passive observation of the network traffic, and the methods which can be used to draw conclusions from this. The Flooding chapter will focus on attacks which overload the network with more traffic than it is intended to handle, with a focus on resource exhaustion. The Spoofing chapter will delve into attacks which rely on impersonating other types of devices and what can be accomplished through this approach. The chapter on Routing Protocol Attacks is split into two, detailing attacks which are specific to the routing protocol RPL, as well as attacks that are independent. The focus herein will be on sabotaging and confusing the network routing. Finally, the chapter on Remote Code Execution will take a brief look at how an attacker may attempt to run arbitrary and malicious code in the networking devices.

We then discuss the severity of the different attacks. In particular, we evaluate how easy it is to perform an attack and discuss the severity of a successful attack. Finally, in the appendix we provide an overview over the state of the art in industry.

TABLE OF CONTENT

EXECUTIVE SUMMARY 2

1 INTRODUCTION 5

2 WIRELESS LOW-POWER MESH NETWORKS FOR IOT 5

3 ATTACK SCENARIOS..... 7

4 ATTACK VECTORS..... 8

4.1 JAMMING 8

4.2 SNIFFING..... 8

4.3 FLOODING 9

4.4 SPOOFING 10

4.5 ROUTING PROTOCOL ATTACKS..... 10

4.6 REMOTE CODE EXECUTION 12

5 INDICATORS OF COMPROMISE 12

5.1 MESSAGE-RELATED INDICATORS..... 12

5.2 INTERNAL STATE INDICATORS..... 13

6 SEVERITY OF ATTACKS..... 14

7 CONCLUSIONS 15

REFERENCES 16

APPENDIX 1: STATE OF THE ART – INDUSTRY / MARKET ANALYSIS 17

1 COMMON TRENDS 17

1.1 NETWORK SCANNING 17

1.2 PASSIVE VULNERABILITY SCANNING..... 18

1.3 ACTIVE VULNERABILITY SCANNING..... 18

1.4 ZERO-TRUST NETWORK MICROSEGMENTATION 18

1.5 BEHAVIOR ANALYSIS 18

1.6 WHERE THESE TOOLS RUN 21

2 COMPETITORS 21

2.1 ARMIS 21

2.2 ATONOMI (OWNED BY CENTRI)..... 23

2.3 BASTILLE..... 24

2.4 BEYONDTTRUST RETINA IOT SCANNER 25

2.5 BITDEFENDER BOX 26

2.6 BITDEFENDER IOT SECURITY PLATFORM..... 27

2.7 BROADCOM (SYMANTEC)..... 28

2.8 BULLGUARD IOT DOJO 29

2.9 CHECKPOINT 30

2.10 CISCO 31

2.11 CENTRI..... 33

2.12 CUJO AI 34

2.13 CYBERMDX..... 36

2.14 CYNERIO 37

2.15 DARKTRACE..... 38

2.16 FIRSTPOINT 39

2.17 FORESCOUT..... 40

2.18 FORTINET 42

2.19 IVANTI..... 43

2.20 IOTSPLOIT 45

2.21 MEDIGATE 46

2.22 NANOLOCK..... 47

2.23 OUTPOST 24 (ACQUIRED PWNIE EXPRESS)..... 48

2.24 OVERWATCH..... 49

2.25	PALO ALTO NETWORKS (ACQUIRED ZINGBOX).....	51
2.26	SECURITHINGS	52
2.27	SENSORHOUND	53
2.28	SHODAN	54
2.29	SNORT	55
2.30	STERNUM	56
2.31	TENABLE (NESSUS).....	57
2.32	TEMPERED AIRWALL.....	58
2.33	TRUSTEDOBJECTS	60
2.34	VDOO	61
2.35	ZEEK (FORMERLY BRO)	62
3	OTHER INTERESTING PROJECTS.....	63
3.1	OPENIOC.....	63
3.2	CHIPWHISPERER	63
3.3	MIDMARK RTLS	64

1 INTRODUCTION

The STACK project has the goal of developing technologies which can help protect wireless IoT networks from malicious adversaries. The goal of this report is to map out how an adversary may plan an attack on network infrastructure and what type of information that can help prevent exploitation.

This report first motivates the STACK project's choice to focus on wireless low-power mesh networks. We believe that these networks will even become more important in the future despite the current drive towards long-range wireless sensor networks.

The report then presents some attack scenarios that an attacker may contemplate. In essence, this boils down to what the goal of the adversary is. A simple-minded attacker may be satisfied with interrupting the network with for example jamming attacks, whilst a more advanced attacker may see the network as an entry-point into a larger network infrastructure, thus requiring more advanced attacks which infects networking devices with malicious code.

From this information, it is possible to start evaluating the different type of attack vectors which the adversary can utilize. To avoid going into discussions about implementation-specific attack vectors, this discussion will be made from a high-level viewpoint which may be applicable to multiple different communication stacks.

In order to be able to stop an attacker at an early stage it is then important to evaluate what type of information that can be retrieved from a nominal system and how this information may change over time as an attack takes place. This information will be referred to as the Indicators of Compromise, which will be discussed in the next section of the report.

The report then visually presents the severity of different attacks based on how easy they are to perform and the damage they can possibly make.

Finally, in the appendix the report presents the state of the art in industry.

2 WIRELESS LOW-POWER MESH NETWORKS FOR IOT

While many recent IoT wireless technologies such as LoRa and NB-IoT are based on single-hop (also called star) networks, there is also a need for IoT multi-hop networks, where some IoT devices forward packet from other IoT devices towards the base station. For example, in residential and smart homes the Matter ecosystem seems to be the common standard for the future. It contains the Thread mesh standard which is good for small building as homes and small offices where you have full control of the Wi-Fi network and can make sure you do not get into co-existence problems between Wi-Fi and Thread. Then, a Thread mesh provides high reliability against interfering objects due to its redundant routing paths. Matter also contains BLE for configuration and Wi-Fi for devices which need higher throughput. In China there, the BLE-mesh standard for lighting for residential is gaining momentum. Here, the driver seems to be to reduce cost and to avoid multi-stack support in future devices.

In commercial buildings there are no mature and standard wireless technology for low power and low cost IoT devices. Wi-Fi and macro cellular technologies consumes too much power and do not have good enough coverage in all buildings. Therefore, device manufacturers often build own wireless infrastructure and use different standard wireless technologies or proprietary solutions. This is challenging and only companies that have competence to build wireless infrastructure can do it. The wireless networks need to be operated and today the building/system owner are forced to do that even though in many cases they do not have necessary competence. Therefore, there is a need for self-healing and self-organizing networks.

For lock systems, one of the application areas of the STACK project, the most common technologies in commercial buildings today are star networks based on BLE, 802.15.4 and 802.15.4g. These star networks are based on 2.4GHz. They are often not very reliable since they do not offer redundant routing paths. The 802.15.4g (sub-gig Hz) can penetrate through objects in a better way and is also more reliable. Hence, there is a smaller need for redundant routing paths. These networks are, however, costly and require a lot of wiring to the hubs (access points or coordinators). They often lead to high maintenance costs since they do not have any built-in self-healing. In such application scenarios, mesh networks can increase reliability

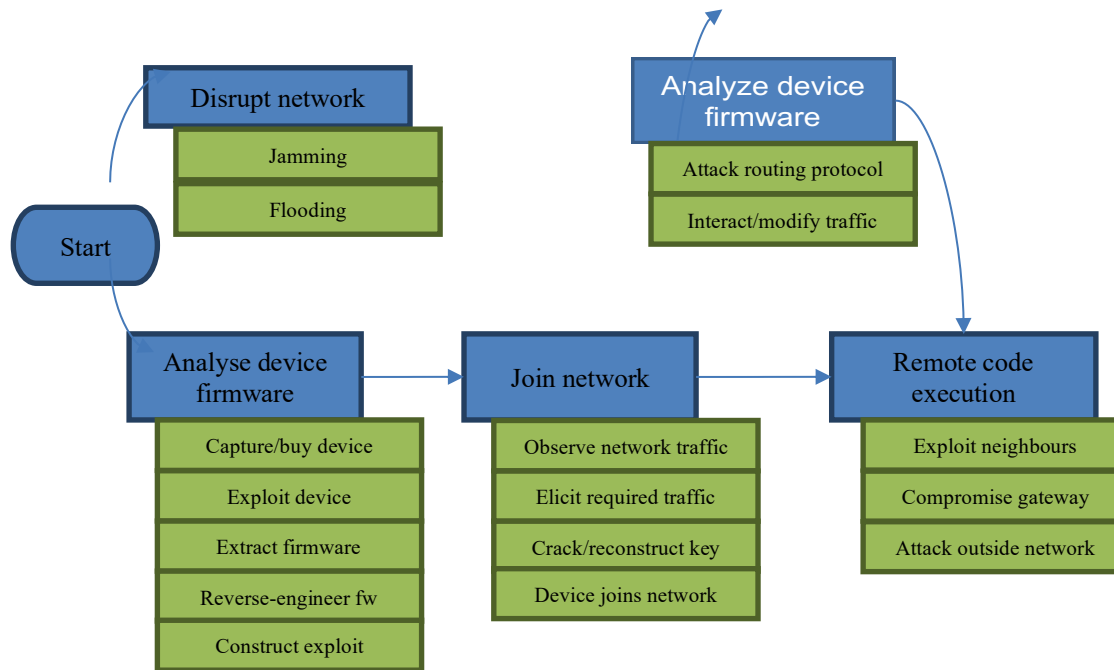
and decrease the total cost of ownership compared to start networks. Other applications as for example lightning and control of HVAC use mesh networks based on BLE or proprietary solutions.

There are new wireless technologies and initiatives for commercial buildings. The DECT2020 mesh standard is based on 5G hardware, but a new standard mesh stack will have low power products available 2022. The Matter standard/ecosystem starts to discuss opportunities to have a standard for commercial buildings also. The 5G private networks which use small cells inside buildings will enable lower power devices and the plan is also to support mesh in the future (see below). This will allow better coverage than Wi-Fi. For 6G, first deployments are expected in 2028. 6G also plans for extremely low-power and low-cost devices. Hence, 6G devices will most likely compete with the low-power and low-cost IoT networks today.

To summarize it seems that the most important new wireless technologies inside buildings for low power and low cost will be based on mesh in the future. In the far future, the IoT networks will be standardized. All this together will lead to lower total cost of ownership for customers but also better coverage and interoperability between devices. A key issue for the success will be security which is a focus of the STACK project.

3 ATTACK SCENARIOS

When analysing the attack surface of an IoT network, it is important to take the adversary's goal and capacity in consideration. Just because an attacker may be unsophisticated, it does not mean he or she will be unable to inflict damage on the network. The simplest method of attacking a wireless network is perhaps through the ability to jam the radio frequencies which the network utilizes. Devices which block a wide frequency spectrum are readily available for purchase online, even though they are illegal to obtain and operate in many countries. Adversaries with more resources will likely be able to perform more advanced attacks on a network infrastructure, typically going through a multi-step approach to fulfilling their goals. Illustrated below is a high-level view of how an adversary may plan an attack.



As illustrated above, disrupting the network can in most cases be performed without much prior knowledge of the network. Typical attacks associated with this stage is jamming and flooding attacks, which are presented in the next chapter under 4.1 Jamming and 4.3 Flooding.

In order to launch more sophisticated attacks on a network, an adversary will likely start out with gaining as much knowledge as possible about the devices which constitute the network. A common starting point would thus be to get physical access to a device to perform low level attacks on the hardware itself, such as side-channel and fault-injection attacks. These attacks will have the goal of extracting device firmware in order to reverse-engineer it and retrieve keying material or construct malicious exploits from. Seeing as this is a topic not included in the STACK project's scope, these attacks will not be further investigated, but it is important to keep in mind that these attacks exist and are likely to be used as the first step of reconnaissance.

After the device firmware analysis step, an attacker may proceed to join the network. Most networks will be protected by some form of encryption on the MAC layer which will need to be bypassed. A naïve device manufacturer may have stored these credentials in the device firmware itself and could potentially have leaked in the earlier firmware analysis step. A more likely scenario however is that the network key would be unique to each installation, and thus an attacker would need to retrieve it before being able to join the network as a legitimate device. Attacks which help in this step would be sniffing, flooding and spoofing style attacks, which are presented in chapter 4.2 Sniffing, 4.3 Flooding and 4.4 Spoofing.

Once an attacker has been able to join the network, the link layer encryption will have been bypassed, allowing for attacks targeting the OSI-layers up to, but not including, the transport and application layers. The latter are likely protected by an additional layer of encryption. Most interesting would thus be attacks on the routing protocols themselves, which is something that will be covered in chapter 4.5 Routing protocol attacks.

The final stage depicted above, remote code execution, will allow an attacker to traverse the network by compromising adjacent network devices, progressing up towards the gateway and the outside network. At

this stage, attacks are focused on leveraging implementation-specific exploits, such as attacks on the TCP/IP protocol stack. This topic is further presented in chapter 4.6 Remote code execution.

4 ATTACK VECTORS

The goal of this chapter will be to present the attack vectors which are deemed to be relevant to the partners in the STACK-project. Most of these are presented in a general manner which does not depend on any particular networking stack. An attempt has been made to categorize these attack vectors into the categories Jamming, Sniffing, Flooding, Spoofing, Routing protocol attacks and Remote code execution. This categorization should be seen more as a guide rather than an absolute truth, primarily intended to alleviate reader comprehension.

4.1 Jamming

Jamming is the process of disrupting the radio signals transferred between a transmitter and receiver. The process can typically be divided into two categories, proactive and reactive jamming. Proactive jamming transmits jamming signals regardless of whether there is legitimate traffic being sent or not. Reactive jamming on the other hand is the process of transmitting a jamming signal based on what type of traffic the target network is actively transferring, normally with the intention of only blocking the network when necessary.

For a jamming attack to be successful, the jammer has to transmit at a power output which is sufficient to drown out normal network traffic. This effectively puts a limit on where an attacker can be located, and if physical distance is a hinderance, certain type of flooding attacks may be more suited to disrupting network communications.

4.1.1 Barrage jamming

A proactive form of jamming, where the jamming signal covers a wide frequency spectrum in which the target network operates [1]. If an attacker would opt for this method in jamming a Zigbee network, he or she would probably block the entire 2.4GHz ISM band.

4.1.2 Traffic-specific jamming

Traffic-specific jamming is a reactive approach to jamming with the intention of blocking specific traffic [2]. One example to this could be to block ACK packages in the network, which in many cases have a smaller frame than those that carry data. In effect, this would result in transmitters being forced to retransmit data packages since they never received acknowledgement from the receiver.

4.1.3 Network-specific jamming

Network-specific jamming aims to target a certain portion of a network [3]. In some cases, the physical distance between jammer and target may be used to accomplish this. Other approaches include beamforming, where radio waves are directed at the particular location which features the target device.

4.2 Sniffing

Sniffing is the process of capturing traffic from a given network. In cabled networks, this would entail physical access to cables or devices. Listening in on wireless traffic is much easier, and can even be done from a distance, since all traffic is sent through the air. One problematic aspect of sniffing is that most of the traffic is likely encrypted, typically down to the link layer. It may therefore be difficult to determine the exact contents of packages, but an adversary will still be able to gain useful information even if the payloads are never decrypted.

As long as an adversary remains passively listening in on traffic, it will be difficult to detect him or her. Active sniffing attacks on the other hand, rely on specific packet injection to generate interesting data packets to record. The prospects of detecting such an attack are thus better.

4.2.1 Communication pattern analysis

A well-positioned adversary may collect a lot of traffic from a network. Since most of the routing information, such as who the sender and who the receiver is, is likely to be encrypted, it may not be straight forward to map out the communication patterns in a network. With the right setup however, an attacker will be able to discern position of individual devices in a network. This process could be alleviated by for example

triangulation and signal strength. Mapping out the communication patterns in a network may provide valuable insight for further attacks [4] [5].

4.2.2 Packet type deduction

Even though a lot of the traffic in the air is protected by encryption, an adversary will be able to draw some conclusions from the metadata that is available. One such thing is for example ACK packets, which typically have a smaller transmission frame than data packets. ACK packets are also often transferred very close in time to the reception of a data packet. It is not unlikely that a properly motivated adversary will be able to draw more conclusions about packet types from information such as length, periodicity, and entropy [4] [6].

4.2.3 Latency analysis

Latency analysis focuses on the study of time-related aspects in the network communication. Conclusions can for example be drawn from the amount of time it takes in between a node receives a message and a reply is sent back. Important messages which could potentially have a processor-heavy payload would then take a longer time to parse and handle than a smaller less important one.

4.2.4 Matching attack

In a communication system where the changes in the data transferred are minimal, an adversary can try to make use of the low entropy in the information. By generating a set of expected data transfers and then encrypting them with a large set of keys, the adversary may be able to find a match to a transmission he or she has previously picked up [7].

4.2.5 Network key reconstruction

The goal of a sniffing attack is often to decode the information which is transferred. This in turn requires the network key. Over the years, several of the WiFi encryption schemes have been cracked due to weaknesses in the cryptographic algorithms or their implementations [8]. Attacks at this level are implementation dependent, tailored towards specific protocols and algorithms.

4.3 Flooding

Flooding is a certain type of Denial-of-Service attack where a network is spammed with more messages than it is capable of handling. The goal of these attacks could for example be to tie up the resources of a target device, forcing it to stop processing normal information, potentially even seizing up and/or rebooting a device. Attacks could also attempt to cause enough congestion on the network so that normal packages do not arrive at their destinations.

4.3.1 Hello flooding

Certain wireless sensor networks utilize Hello packets to advertise themselves to the network, a sequence which can easily be captured through sniffing. An adversary may choose to spam a network with these recorded sequences with a high transmission power, making the legitimate devices believe that the malicious device is a neighbour, thus replying to the Hello messages, effectively wasting energy and confusing the network [9].

4.3.2 Battery-draining attacks

Sensor networks which are battery operated can be heavily affected by flooding attacks. Certain attacks may be designed with the intent of draining the battery of a device [10]. This could for example be achieved by continuously sending legitimate-looking packets to a device, which it will be forced to wake up and receive, effectively wasting battery power on each reception. These packets are likely discarded higher up in the communication stack, due to for example sequence number mismatches, but by then the damage has already occurred.

4.3.3 De-authentication flooding

De-authentication frames are present on multiple wireless networking technologies to signal for a device to leave the network. A de-authentication flooding attack attempts to kick devices off a network by spoofing de-authentication frames [11]. The goal of doing so may be varied. One example would be to interrupt communications of the networking devices. Another example would be to force the networking devices to perform authentication handshakes, which could potentially be sniffed and further exploited at a later point in time.

4.3.4 Buffer reservation attacks

Protocols such as 6LoWPAN rely on fragmentation of large message transfers into smaller packet frames. An attacker may target the buffering system that is responsible for keeping these separate packets in

memory until the complete message can be reassembled. This could then lead to the targeted device not being able to receive legitimate messages from other devices [12].

4.4 Spoofing

In a spoofing attack, an attacker attempts to forge the identity of a legitimate device, something which can be performed in a multitude of ways. In data communications for example, this could mean that the attacker sends data that looks like it came from another, already verified, device on the network.

4.4.1 Evil twin network

The attacker sets up a new gateway device, which only he or she has access to, with the goal of the devices joining this network instead of their regular one [13]. The attacker would have to overcome the fact that the network may have access credentials, but if successful it could allow him or her to communicate with and collect data from the networking devices.

4.4.2 Identity impersonation

In this broad category, the primary consideration for this project is the ability to impersonate the identity of another node in the mesh network. An attacker would have to capture identity credentials of another node, and then use this information in communications with other devices in order to appear as the legitimate node [14].

4.4.3 Man in the middle (MITM)

MITM attacks is another broad subject which can be applied to several different scenarios. The basic idea is to set up a device which acts as a proxy in the communication between two legitimate devices. This proxy would then need to be hidden from view, so that the two legitimate devices believe that they are communicating directly with each other. In addition to listening in on the traffic between the devices, a MITM attack could potentially allow the attacker to modify data in transit to further his or her needs [15].

4.4.4 Replay attacks

Packets captured through the process of sniffing could potentially be resent at a later time. They will then appear to originate from a legitimate device, just as when they were first sent. Systems which do not incorporate countermeasures such as nonces and timestamps may then be fooled into thinking that the packet is valid and execute the corresponding message handler. In a MITM-style attack, an attacker could also utilize replay attacks to delay messages until a point in time that is deemed more useful for the attacker's purpose, potentially bypassing certain countermeasures [15].

4.4.5 Reflection attacks

Reflection attacks target challenge-response authentication schemes used in certain network communications. Upon opening a connection, the attacker will be presented with a challenge it needs to respond to. By opening another connection, either to the same device or a completely different one, and sending out the received challenge as its own, it could potentially be able to receive a valid response. This response could then be forwarded and used to authenticate the first connection [16].

4.5 Routing protocol attacks

This chapter will focus on Denial-of-Service (DoS) style attacks on routing protocols. Since RPL (Routing Protocol for Low-Power and Lossy Networks) is a common protocol used in sensor networks, a separate subchapter dedicated to RPL-specific attacks is motivated, as detailed by [4] [17] [18].

4.5.1 RPL-specific attacks

In this subchapter, attacks which are unique to the RPL protocol will be discussed.

4.5.1.1 Rank attack

The Rank parameter in the RPL network determines the relative distance to the root node with respect to parameters such as link quality, hop count, etc. An attacker targeting the Rank parameter, for example by selecting the worst parent device rather than the best, can then provoke inefficiencies in the routing algorithms in the network.

4.5.1.2 Version number attack

The version number specifies the currently used revision of the RPL network hierarchy. By intentionally modifying the version number of a compromised node, the rest of the network can be forced to rebuild the

network hierarchy. The possibility of modifying the network version number is a mechanism intended for the root device, but there appears to be no protection from other nodes modifying this in the RPL standard.

4.5.1.3 Local repair attack

Individual devices in the network can initiate local repair procedures to sort out localized inefficiencies in the closest neighbourhood. This mechanism can be abused by an attacker, causing repair sequences to be initiated when there is no need for it. This will in effect cause increased control messages being issued, which in effect can lead to reduced availability.

4.5.1.4 DODAG inconsistency

DODAG inconsistency attacks target the RPL header in outgoing packets. By modifying flags intended to signal network inconsistencies, an attacker can force that packet to be dropped and local repair procedures to be initiated by the receiving device.

4.5.1.5 DIS attack

Upon joining a network, a new device will send DIS messages to ask for RPL-information from neighbouring devices. This mechanism can be abused to force neighbours to send more control information than they would normally do, effectively generating unnecessary traffic in the near vicinity.

4.5.2 Non-RPL attacks

In this subchapter, focus will be on attacks which are applicable, but not restricted, to RPL.

4.5.2.1 Neighbour attack

An adversary may choose to retransmit incoming routing information to its neighbourhood in order to confuse the devices in its near vicinity. These devices will then assume that node which the routing information originated from is closer than it actually is, giving rise to inefficiencies in the network hierarchy.

4.5.2.2 Sybil attack

In a network that is running voting mechanisms in a democratic fashion, an adversary could be interested in influencing the outcome by introducing more votes. This could be done by introducing a malicious node which presents multiple different identities, each having the possibility to cast a vote.

4.5.2.3 Sinkhole attack

An adversary may advertise a malicious node with a better rank than it actually has. This could in effect cause the neighbouring devices to select the malicious device as its primary parent. The malicious node would then receive a larger influx of messages than it would normally have if operating nominally. This approach can be useful for other attack scenarios that rely on incoming traffic to further the means of the adversary.

4.5.2.4 Selective forwarding

A selective forwarding attack may be preceded by a sinkhole attack in order to get a malicious node listed as the preferred parent of neighbours. The malicious node could then filter what traffic to forward and which traffic to discard, effectively creating inefficiencies in the network hierarchy or the regular communication routes.

4.5.2.5 Blackhole attack

As a close relative to the selective forwarding attack, a blackhole attack may simply choose to discard the incoming traffic it is supposed to relay, without informing the sender that its transmission has been lost.

4.5.2.6 Wormhole attack

In a wormhole attack, an adversary sets up a high-speed connection between two points in a network that would normally not be in communication range of each other. Having malicious nodes on either end, acting as a single device, he or she will be able to create a traffic tunnel that can cause confusion in the remainder of the network.

4.5.2.7 CloneID attack

The CloneID attack is a form of impersonation attack where an adversary is able to physically capture and extract identity and cryptographic material from one or multiple devices. This would then allow the adversary to produce clones of said devices, which can be placed at key positions within the network to further other attacks.

4.6 Remote code execution

In instances where an adversary is interested in performing ransomware-style takeovers of a network, it is important to consider the risk of remote code execution on the networking devices. Remote code execution (RCE) would allow the attacker to run arbitrary code on devices, spreading through and possibly out of the network as well. The ability to perform RCE is not tied to any specific layer of the OSI-stack, but are rather firmware-implementation dependent, where exploits can be custom designed for specific devices.

4.6.1 TCP/IP Stack exploits

Vulnerabilities in TCP/IP stacks can be relatively severe since they are prone to exploitation before a packet is passed up to the Application layer. Attacks that target the packet parsing in a stack can be triggered even without application ports being opened. A recent set of exploits are those published by Forescout in their Amnesia:33 release. The exploits therein mostly relate to memory corruption problems, allowing for attackers to perform remote code execution, Denial of Service, Infoleak and DNS cache poisoning attacks. This release covers four different IP stacks (uIP, FNET, picoTCP and NUT/NET), which according to Forescout can potentially impact millions of IoT devices [19].

4.6.2 Malicious firmware updates

To update the software of networking devices, manufacturers are likely to implement Firmware-Over-The-Air (FOTA) capabilities. This opens up another attack surface which adversaries may choose to target. Countermeasures such as firmware encryption and signing are likely to thwart such attempts, but a compromise of these schemes could lead to an adversary being able to reprogram the devices with a customized firmware, potentially pivoting into for example ransomware-style attack scenarios. Attackers could also target the update process itself, blocking certain parts of this communication could potentially render devices unusable [4].

5 INDICATORS OF COMPROMISE

To construct a mechanism to detect network intrusions, there needs to be a certain set of input data. In this chapter, suggestions will be made as to what parameters can be used to constitute this input. These parameters will from this point on be referred to as the Indicators of Compromise (IoC). Although not exhaustive at the time of writing, this list will likely be extended throughout the course of the STACK project.

5.1 Message-related indicators

In this section, focus will be on indicators which relate to the wireless communication in a network. For example, the size of packets, the interval at which they are sent and which devices that talk to each other.

5.1.1 Invalid message count

When processing messages, error detection is likely implemented at several stages. Messages which are incomplete, corrupt, or otherwise invalid, are typically discarded from further processing. By keeping track of the amount of such invalid messages over time, it should be possible to draw conclusions about whether for example a flooding or battery draining attack is in the process, since these attacks typically rely on messages which under normal circumstances would be deemed as invalid.

5.1.2 Authentication failure count

A normally functioning device will join the network successfully the first time, assuming it has the correct credentials. Certain type of fuzzing and brute-forcing attacks may rely on failed authentication frames to further their attack. Recording the amount of times a device fails the authentication steps may provide valuable insight into a potentially ongoing attack.

5.1.3 Communication interval and size

Communication within a network should to some extent follow a pattern. For example, there may be background keep alive messages at a low interval, whilst intermediate burst-style transmission can be observed as well. Discrepancies in the communication intervals as well as the size of packets could be used to detect anomalies in the communication patterns of a network, potentially highlighting ongoing attacks or otherwise faulty devices.

5.1.4 Source/Destination monitoring

Observations can also be made about which devices that talk to each other during normal circumstances. In a simple system for example, two sensors on either side of the installation should possibly never communicate directly with each other. Any indication that they are doing so may be an indicator of an ongoing attack.

5.1.5 Network rejoins

Devices will have to rejoin the network upon rebooting. Discrepancies in how often a sensor reboots or rejoins the network could indicate that a sensor is malfunctioning for example due to low battery. It could also be an indication of the device being targeted in an ongoing attack such as replay, fuzzing or brute-forcing, where reboots can be a tactic or a side-effect.

5.1.6 Signal strength

A location-static installation, where all devices are mounted in fixed locations, may to some extent have predictable signal strengths in between devices. Noticing drastic changes in the signal strength of a received signal could indicate that a unit has been moved, or that someone is trying to forge the identity of said device.

5.1.7 RPL-related indicators

For RPL-specific attacks (see Section 3.5), there are a number of possible attack indicators. These include the number of specific RPL messages during a time interval. For example, during blackhole attacks, the number of DODAG Information Solicitation typically increases when nodes try to find new routes.

5.2 Internal state indicators

In this chapter, focus will be on indicators which can be retrieved from the internal program state of a networking device.

5.2.1 Sleep monitoring

Battery-draining attacks will focus their attacks on keeping the networking device in a high power-consumption state so that the battery is depleted as fast as possible. One of the simpler ways to accomplish this is to prevent the device from putting the microcontroller to sleep by flooding it with invalid messages, which it may be forced to receive and parse. By monitoring the amount of time that a device is able to go into sleep mode, or the reverse – how much it stays awake, it could be possible to detect certain type of denial-of-service attacks.

5.2.2 Call stack monitoring

Code instrumentation could provide the possibility to monitor the program's call stack during operation. Information such as stack traces, return addresses, frame length and entropy could then help form a nominal picture of how the program operates. Deviations from the baseline could indicate an ongoing attack attempting to exploit bugs in the firmware of a device.

5.2.3 Checkpoint monitoring

Firmware-level exploits will to some extent attempt to run malicious code on a device, altering the normal behaviour of a program. By implementing a checkpoint module, acting as a high-level watchdog, which needs to be called at certain intervals from a pre-specified set of locations in the code, it could be possible to detect alterations in the program flow. This approach should also be able to catch other type of attacks which change the behaviour of a program, even without malicious code injection, for example battery depletion and other denial-of-service attacks.

5.2.4 Function pointer monitoring

Low-level applications, written in for example C, can rely on function pointers to provide a runtime-configurable change in which functions gets to execute. These function pointers provide a high value target for attackers and could potentially be used to branch into a malicious code segment previously uploaded to a device. Monitoring the function pointers in an application, making sure they stay within allowed ranges (e.g. certain flash addresses), could provide a low-effort solution for detecting exploitation attempts.

5.2.5 Shellcode detection

Certain types of attacks rely on the adversary uploading malicious code to the RAM region of a device. In certain microcontroller configurations, RAM is an executable region, even though code is normally executed from the FLASH region. A code module monitoring the RAM of a device could be on the lookout for certain

specific byte-code sequences that could indicate attempts to execute shellcode. An example of this could be instructions to modify critical memory addresses, operate the GPIO block, call certain functions or freeze up the microcontroller. This detection approach could then be likened to a signature based anti-virus, where certain data blocks are flagged as malicious. However, reliably accomplishing this detection may be difficult, since it may be difficult to decide whether a memory region contains executable code, or just random data which happens to look as something malicious.

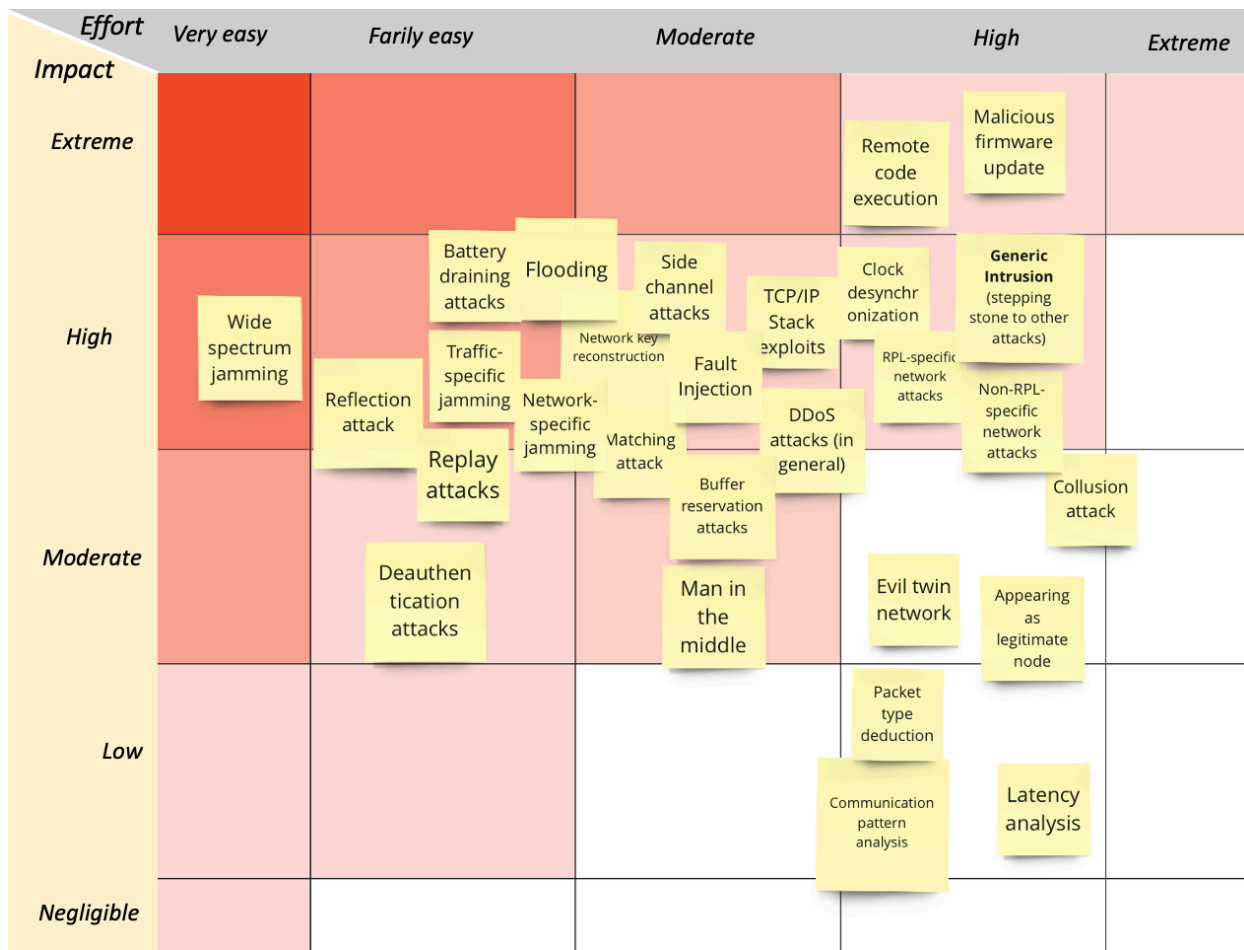
5.2.6 ROP-gadget detection

Under circumstances where the RAM memory of a device is non-executable, an attacker may attempt to piece together a malicious code segment by using ROP-gadgets (small, naturally occurring, reusable code segments in FLASH). A device firmware can be analysed for ROP-gadget addresses as a part of the build process. By then registering these addresses as known exploitable code segments, an observing code module can scan the RAM memory a device to detect attempts to leverage these addresses.

5.2.7 Heap exploit detection

On a case-by-case basis, firmware implementations may feature predictable HEAP-usage conditions over time. Exploits which target the HEAP for malicious code injection could potentially disrupt normal allocation patterns. By studying heap metadata such as allocation frequency, size, and addresses, it may be possible to detect abnormal behaviour that indicates an ongoing attack.

6 SEVERITY OF ATTACKS



The table above shows the severity or impact over attacks (low to extreme) and how high the effort of performing such an attack is. The effort ranges from very easy to extremely difficult. Many attacks do have a very impact. Among those, the easiest to perform is a wide spectrum jamming attack that can be

performed with equipment that is ready to buy on the Internet. Many other attacks are not as easy to perform since they require some knowledge of the protocols in use. The attacks with the most impact (malicious firmware updates and remote code execution) are also difficult to perform. We also note that these are generic attacks in the sense that they are not specific to the type of networks the STACK project considers.

7 CONCLUSIONS

In this deliverable, focus has been on providing a view of the attacks which are relevant in the STACK project. This has been done in a generalized manner in six different categories, which would allow for the multiple use-cases which are presented by the project partners. Although this list is not exhaustive of all possible attacks for networking IoT-devices, it aims to provide enough coverage to offer a baseline scope of which attack vectors the project can be limited to.

In addition to attack vectors, a list of Indicators of Compromise has been presented. This list is an attempt at detailing which parameters could be interesting to discover the previously covered attack vectors. The list is divided into two sections, one covering network traffic related aspects, and one covering the internal application state of the device processing unit. As the research in the project continues, this list is likely to be expanded to cover the finer details of different attack implementations.

REFERENCES

- [1] A. Mpitzopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou, "A Survey on Jamming Attacks and Countermeasures in WSNs," *IEEE Communications Surveys & Tutorials*, 2009.
 - [2] M. Çakıroğlu and A. Özcerit, "Jamming Detection Mechanisms for Wireless Sensor Networks," in *3rd international conference on Scalable information systems*, 2008.
 - [3] A. Wood, J. Stankovic and S. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks," in *24th IEEE Real-Time Systems Symposium*, 2003.
 - [4] I. Butun, Ö. P and S. H, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," *IEEE Communications Surveys & Tutorials*, 2019.
 - [5] C. Ozturk, Y. Zhang and W. Trappe, "Source-location privacy in energy-contained sensor network routing," in *2nd ACM Workshop on Security of ad hoc and Sensor Networks*, 2004.
 - [6] L. Sikos, "Packet analysis for network forensics: A comprehensive survey," *Digital Investigation*, 2020.
 - [7] C. Tan, H. Wang, S. Zhong and Q. Li, "IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks," *Information Technology in Biomedicine*, 2009.
 - [8] S. Fluhrer, I. Mantin and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," in *SAC 2001: Selected Areas in Cryptography*, 2001.
 - [9] V. Singh, J. Sweta and S. Jyoti, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks," *International Journal of Computer Science Issues*, 2010.
 - [10] E. & H. N. Vasserman, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks," *IEEE Transactions on Mobile Computing*, 2013.
 - [11] D. L. A. Lawrence and V. L, "A Survey of Denial of Service Attacks and it's Countermeasures on Wireless Network," *International Journal on Computer Science and Engineering*, 2010.
 - [12] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh and K. Wehrle, "6LoWPAN Fragmentation Attacks and Mitigation Mechanisms," in *6th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2013.
 - [13] H. Gonzales, K. Bauer, J. Lindqvist, D. Mccoy and D. Sicker, "Practical Defenses for Evil Twin Attacks in 802.11," in *Global Communications Conference*, 2010.
 - [14] A. Diaz and P. Sanchez, "Simulation of Attacks for Security in Wireless Sensor Network," *Sensors*, 2016.
 - [15] S. Udgata, A. Mubeen and S. Sabat, "Wireless Sensor Network Security Model Using Zero Knowledge Protocol," in *IEEE International Conference on Communications*, 2011.
 - [16] M. Kompara and M. Hölbl, "Survey on Security in Intra-Body Area Network Communication," *Ad Hoc Networks 70*, 2017.
 - [17] A. Arış, S. Oktug and T. Voigt, "Security of Internet of Things for a Reliable Internet of Services.," 2018.
 - [18] L. Wallgren, S. Raza and T. Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things.," *International Journal of Distributed Sensor Networks*, 2013.
 - [19] Forescout Research Labs, "Amnesia:33, How TCP/IP Stacks Breed Critical Vulnerabilities," 8 12 2020. [Online]. Available: <https://www.forescout.com/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices/>. [Accessed 07 12 2021].
-

APPENDIX 1: STATE OF THE ART – INDUSTRY / MARKET ANALYSIS

- [Common Trends](#)
 - [Network scanning](#)
 - [Passive vulnerability scanning](#)
 - [Active vulnerability scanning](#)
 - [Zero-Trust Network microsegmentation](#)
 - [Behavior analysis](#)
 - [Where these tools run](#)
- [Competitors](#)
 - [Armis](#)
 - [Atonomi \(owned by Centri\)](#)
 - [Bastille](#)
 - [BeyondTrust Retina IoT Scanner](#)
 - [Bitdefender BOX](#)
 - [Bitdefender IoT Security Platform](#)
 - [Broadcom \(Symantec\)](#)
 - [Bullguard IoT Dojo](#)
 - [Checkpoint](#)
 - [Cisco](#)
 - [Centri](#)
 - [Cujo AI](#)
 - [CyberMDX](#)
 - [Cynerio](#)
 - [Darktrace](#)
 - [FirstPoint](#)
 - [Forescout](#)
 - [Fortinet](#)
 - [Ivanti](#)
 - [IoTsploit](#)
 - [Medigate](#)
 - [NanoLock](#)
 - [Outpost 24 \(acquired Pwnie Express\)](#)
 - [Overwatch](#)
 - [Palo Alto Networks \(acquired Zingbox\)](#)
 - [SecuriThings](#)
 - [SensorHound](#)
 - [Shodan](#)
 - [Snort](#)
 - [Sternum](#)
 - [Tenable \(Nessus\)](#)
 - [Tempered Airwall](#)
 - [TrustedObjects](#)
 - [Vdoo](#)
 - [Zeek \(formerly Bro\)](#)
- [Other interesting projects](#)
 - [OpenIOC](#)
 - [ChipWhisperer](#)
 - [Midmark RTLS](#)

1 COMMON TRENDS

1.1 Network scanning

This is a basic feature that most companies provide. The tools scan the network for all devices it can find, and tries to figure out what they are, and who produced them. This is done by inspecting the response from different ports, for example port 80 where web interface is typically presented. Most company also provide some sort of alert for when new devices join the network.

1.2 Passive vulnerability scanning

Several companies offer passive vulnerability scanning, where device profiling can be compared to a database of known threats for said device. Typically, the most severe threats are highlighted, so that a network admin can focus on patching the most vulnerable and likely points of entry.

1.3 Active vulnerability scanning

Very few companies offer active vulnerability scanning, where attacks can be simulated on IoT networks. The ones that do are typically limited to basic attacks, such as login attacks with default credentials.

1.4 Zero-Trust Network microsegmentation

Zero-Trust networking seems to be the latest bussword for a lot of these companies. Commonly they offer some sort of network microsegmentation where devices are separated and isolated from each other via virtual networks. This approach seems to be especially relevant in cases where you would like to isolate a misbehaving node from the network.

1.5 Behavior analysis

Multiple companies provide some sort of analysis behavior for the connected devices. The sophistication of these methods are however very widely ranging. The most advanced solutions seem to utilize AI & ML to learn traffic profiles of each individual device. How well they manage to do this is however unclear.

Further analysis of the offered features show that only a few of the ones that list behavior analysis actually do so with AI/ML. Most companies seem to go toward the approach of classifying what device they see, and then applying a ruleset based on similar devices seen in other installations.

□	Armis	Atonomi	Bitdefender BOX	Bitdefender IoT Security Platform	Cisco	Cynerio	CujoAI
Country	US/Israel	US	Romania	Romania	US	US	US
Price	-	-	\$200 device, \$99 yearly	-	-	-	-
Customers (Target audience)	Enterprises	IoT Developers	Home users	IoT Developers	Enterprises	Hospitals	Internet Service Providers / Enterprises & Consumers
Usage area (Where product is used)	Supervising networking devices	Validate IoT device authenticity and reputation	All-in-one cybersecurity for smart homes	Anti-virus/Firewall software for IoT	Supervising networking devices	Supervising networking devices	Monitor and gain insight into device usage
HW/SW (What product consists of)	Cloud, integrates with switches, routers, firewalls, etc.	SDK for embedded, cloud for reputation	Dedicated hardware (Dual core A9 @1.2GHz, 4GB RAM)	Software (possibly cloud backend)	Cloud	Cloud (?)	Device agent in gateway, cloud backend
Device agents (Does each node need special software?)	No	Yes	Optional	Yes	No	No	Yes
Stacks (Means of communication monitored)	Ethernet, WLAN, Bluetooth, Zigbee	Independent	Ethernet, WLAN	Ethernet, WLAN (?)	Ethernet, WLAN. Others with Armis integration	Ethernet, WLAN	Independent
Isolation layer (Where in TCP/IP stack devices are cut off if misbehaving)	Network access layer	Application layer (?)	Network access layer	Internet layer	Network access layer	Network access layer	Network access layer
Monitoring (Passive=data only inspected. Active = device is probed)	100% Passive	Active, all transactions inspected and logged	Active discovery and vulnerability checks, passive monitoring	Active	Passive	Active discovery and vulnerability checks, passive monitoring	Passive, metadata sent to cloud
Compares behavior with (What is used to determine benign vs malicious behavior)	Crowd-sourced behaviour knowledgebase (8m device profiles)	Reputation from other nodes' reports	Trained behavior over time for each device. Probably also online database of device behavior, as commercial solution does	Threat database online. AI network trained on 500m devices	Crowd-sourced fingerprint database for endpoints.	Unclear, possibly just previously observed behavior of devices.	Normal trained behavior of devices as well as threat database
AI/ML used for behavior analysis	Yes	No	Yes	Yes	No	Possibly	Yes
Other	Only supplier that mentions zigbee monitoring.	Blockchain based.					
Comments	Has thorough traffic analysis framework, runs in cloud, compares traffic to trained behavior and behavior of similar devices in other installations. Can inspect zigbee as well.	Requires integration in firmware from project start. Whole project based around assumptions you need to make when developing a product.	States that it learns behavior of devices with AI/ML. Unclear how thorough this is.	Analysis engine needs to be installed on devices, and seem to require OS/Linux. Basically a antivirus/firewall solution for embedded systems with cloud control.	Seems like rulesets are derived based on device type. Does not appear to learn behavior of devices.	Startup with focus on hospital networking. Seems mostly focused on vulnerability scanning. Unclear/unlikely that it learns device behavior with AI/ML.	Heavily focused on AI/ML training on traffic patterns from multiple device categories. This is done both for commercial trend analysis as well as malicious pattern detection.

	Darktrace	Forescout	Fortinet	Medigate	Outpost24	Overwatch	Palo Alto Networks	SecuriThings
Country	UK	US	US	US	Sweden	US	US	Israel
Price	-	-	-	-	-	\$5/month	-	-
Customers (Target audience)	Enterprises	Enterprises	Enterprises	Hospitals	Enterprises	IoT Developers	Enterprises	IoT Developers
Usage area (Where product is used)	Supervising networking devices and users	Supervising networking devices	Supervising networking devices	Supervising networking devices	Supervising networking devices	Supervise IoT device communications	Supervising networking devices	Supervise IoT device communications
HW/SW (What product consists of)	Cloud, integrates with switches, routers, firewalls, etc.	Cloud, integrates with switches, routers, firewalls, etc.	IPS in firewall	Integrated with firewall. Cloud hosted (?)	Either HW or VM	Device agents, cloud backend	Software suite for firewall	Device agents, cloud backend
Device agents (Does each node need special software?)	No	No	No	No	Optional	Yes	No	Optional
Stacks (Means of communication monitored)	Ethernet, WLAN	Ethernet, WLAN	Ethernet, WLAN	Ethernet, WLAN	Ethernet, WLAN, Bluetooth	Independent	Ethernet, WLAN	Independent
Isolation layer (Where in TCP/IP stack devices are cut off if misbehaving)	Network access layer	Network access layer	Network access layer	Network access layer	Network access layer	Internet layer	Network access layer	Internet layer
Monitoring (Passive=data only inspected. Active = device is probed)	Passive	20+ active and passive discovery, profiling and classification techniques	Active profiling, passive monitoring with DPI	Passive monitoring with DPI	Active discovery and vulnerability checks, passive monitoring	Active, metadata sent to cloud	Active discovery and vulnerability checks, passive monitoring	Active, metadata sent to cloud
Compares behavior with (What is used to determine benign vs malicious behavior)	Normal behavior of devices and users	Crowd-sourced behaviour knowledgebase (12m device profiles)	~30000 rules, updated daily	Rule-based policies based on device type	Rule-based policies of known exploits	Security policies that you specify	Crowd-sourced behaviour knowledgebase (millions of device profiles)	Trained behavior of devices, possibly crowdsourced.
AI/ML used for behavior analysis	Yes	No	No	No	No	No	Yes (at least for profiling)	Yes
Other					Can monitor for rogue Access Points with their hw device.			
Comments	Learns normal behavior of users and devices. Compares with these baseline to detect malicious activities. Primary focus seems to be on computers and servers.	Proven market actor with good security products overall. Does not appear to learn behavior of devices, but simply compares behavior to knowledgebase with a ruleset.	Probably good at preventing malware in network, but relies on ruleset and deep packet inspection. Does not learn device behavior.	Focused on hospital networking. Seem to provide protection against malicious behavior with ruleset based on policies, fulfilled with DPI.	Probably very good at preventing malware in your networks, has active scanning. However, does not seem to learn behavior of devices.	Seems to have very limited usage. You need to install device agent on all your products, and then configure firewall properties from cloud.	Proven market actor with good security products overall. Unclear how well their system learns behavior of devices, possibly not at all. AI/ML is definitely used for figuring out what type of device it monitors.	Startup with multiple focus areas. Their security solution seems to be centered around uploading metadata from devices and then applying security policies. Unclear how thorough behavior training is.

1.6 Where these tools run

The evaluated companies vary wildly in terms of where their products run, in short we have these options:

Cloud - Analysis and configuration takes place in dashboard online.

On-device agent - Software you install on the IoT-device/computer which helps analyze its behaviour.

Firewall - Dedicated hardware firewall with extra processing capabilities.

Gateway - Some solutions are integrated in the gateway modem.

Additional device - Some solutions are based on a standalone box being plugged into the router. Some seem to take over role as the network gateway.

2 COMPETITORS

2.1 Armis



2.1.1 Technology

- Integrates with router/firewall, but runs in cloud
- Discovers all devices on network (including Bluetooth and IOT)
- Learns normal behaviour and alerts on anomalies
- Isolates/quarantines suspicious and malicious devices

2.1.2 Quotes

Armis discovers and classifies every managed, unmanaged, and IoT device in your environment including servers, laptops, smartphones, VoIP phones, smart TVs, IP cameras, printers, HVAC

controls, medical devices, industrial controls, and more. Armis can even identify off-network devices using Wi-Fi, Bluetooth, and other IoT protocols in your environment — a capability no other security product offers without additional hardware.

Armis goes beyond device and risk identification. The Armis Threat Detection Engine continuously monitors the behavior of every device on your network and in your airspace for behavioral anomalies. Working with our Device Knowledgebase, Armis compares the real-time behavior of each device with:

- *Historical device behavior*
- *Behavior of similar devices in your environment*
- *Behavior of similar devices in other environments*
- *Common attack techniques*
- *Information from threat intelligence feeds*

With these types of critical device and behavioral insights, Armis is uniquely positioned to take action to identify threats and attacks

When Armis detects a threat, it can alert your security team and trigger automated action to stop an attack. Through integration with your switches and wireless LAN controllers, as well as your existing security enforcement points like Cisco and Palo Alto Networks firewalls, and network access control (NAC) products such as Cisco ISE and Aruba ClearPass, Armis can restrict access or quarantine suspicious or malicious devices. This automation gives you peace of mind that an attack on any device — managed or unmanaged — will be stopped, even if your security team is busy with other priorities.

There's no learning period or tuning required for the Armis platform to start detecting and responding to threats. When the platform detects a new device, it immediately starts comparing its behavior with baseline behaviors of similar devices in the Armis Device Knowledgebase. The platform's Threat Detection Engine quickly analyzes massive volumes of data from Cortex Data Lake using various threat intelligence feeds. Combined with the platform's device behavior analysis, this results in highly-accurate threat and attack detection. When the Armis platform detects abnormal behavior or an active threat, it notifies Palo Alto Networks next-generation firewalls to block the device automatically. This helps provide security teams with peace of mind that an attack will be stopped, even if they're busy with other priorities.

2.1.3 Links

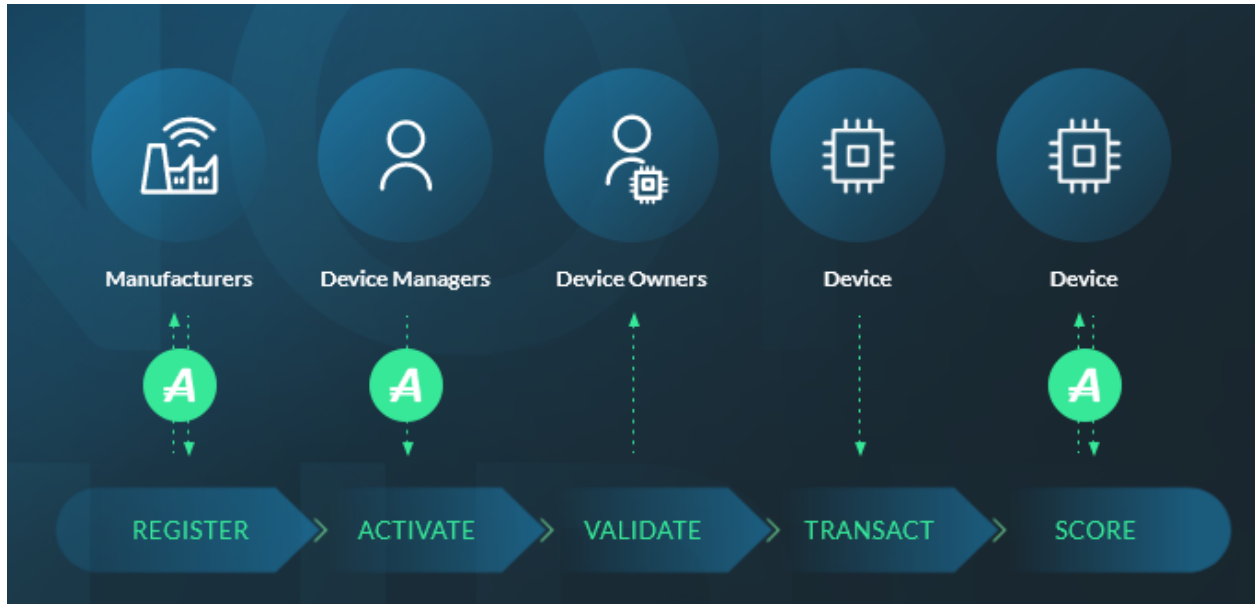
<https://www.armis.com/>

https://info.armis.com/rs/645-PDC-047/images/Armis_Solution_Brief.pdf

<https://info.armis.com/rs/645-PDC-047/images/Armis-Palo-Alto-Networks-SB.pdf>

<https://www.armis.com/platform/benefits-of-armis-security/>

2.2 Atonomi (owned by Centri)



2.2.1 Technology

- Platform based around blockchain
- Identity validation
- Device reputation (looks for change in behaviour to detect compromised nodes)
- Communication-interoperability between devices of different manufacturers.

2.2.2 Quotes

Atonomi provides IoT developers and manufacturers with an embedded solution to secure devices with blockchain-based immutable identity and reputation tracking. We help provide the identity and trust required for our increasingly connected world.

Atonomi registers the identity and reputation of devices on a blockchain-based immutable ledger. Atonomi accomplishes this by working with device manufacturers and other stakeholders facilitating an ecosystem of participants designed to maintain decentralized consensus for device identity and reputation. Combining on-chain and off-chain resources, and built on the Ethereum blockchain, Atonomi's architecture is extensible by developers across IoT verticals (for example, industrial IoT, healthcare, and smart cities) to help secure the vast realm of IoT devices ranging from healthcare and home automation systems, to smart-city infrastructure, to industrial sensors and controllers.

2.2.3 Links

<https://atonomi.io/>

https://assets.website-files.com/5b95e56c7572f5c98b3993d9/5bea12e1bc354be65c577c0c_Atonomi-White-Paper-v0.9.4b.pdf

2.3 Bastille



2.3.1 Technology

- Sensor-arrays that scans airspace for devices
- Demodulates and analyze data
- Positions devices on a map

2.3.2 Quotes

The core and multi-patented technology of our sensor arrays and analytics continuously scans your airspace and detect wireless emitters, digitally demodulate those signals, identify protocols and individual unique devices. This allows Bastille to put an accurate dot on a floor plan map of your facility to show the location of each individual device.

Bastille provides context information about the devices it locates. This allows you to tell whether the device that is represented by the dot is connected with other devices, what kind of data it's streaming, or if it's being actively attacked in certain cases.

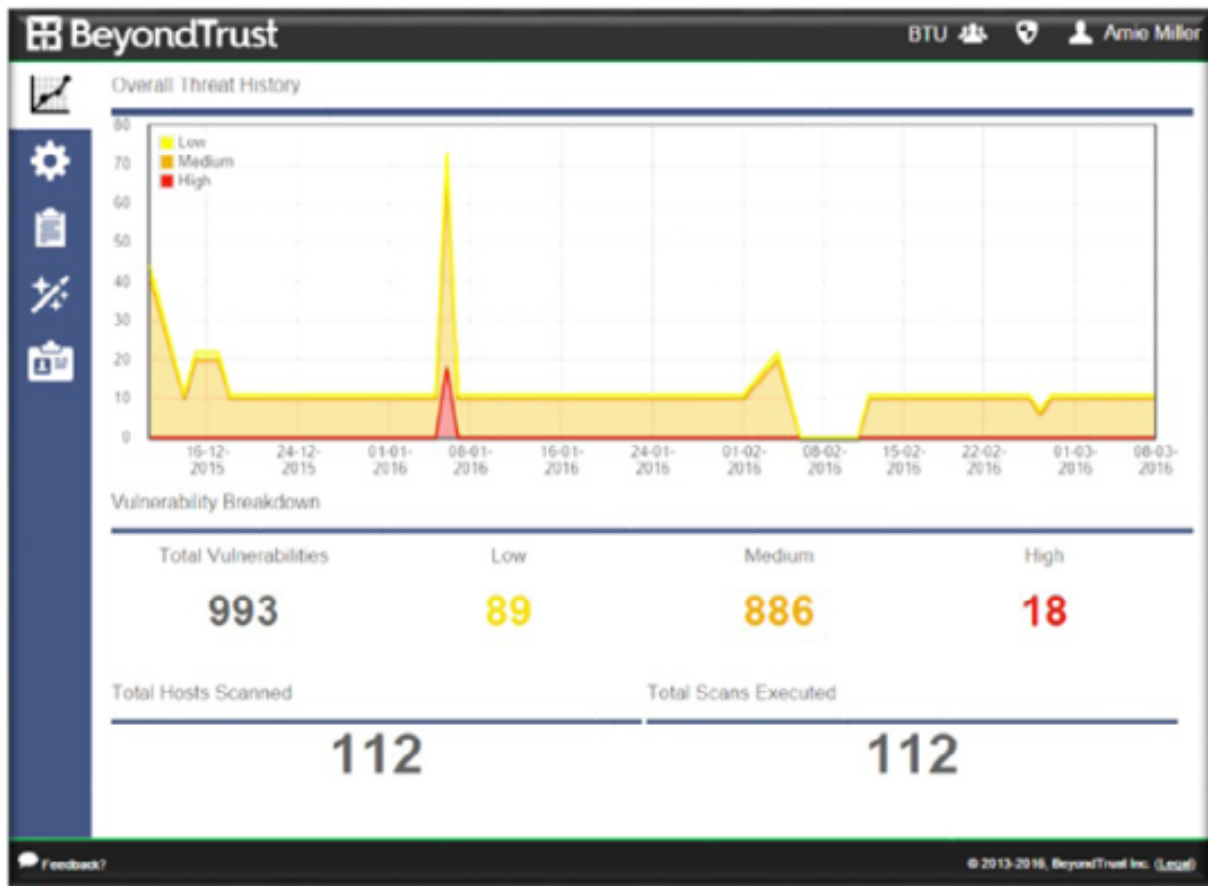
Rule-based alerts can be established that interact with your incident response workflow. Using integrations, Bastille alerts can be used to send emails, text message phone calls, or to instantiate tickets in an external incident response system like PagerDuty, ServiceNow, or Lenel OnGuard.

You can use Bastille's DVR feature to go back in time and see a given device's presence and location history. Through this forensic analysis, it may become clear that the device has been in or near restricted areas, or that the device has been present during off-business hours in a way that is indicative of involvement in a malicious event.

2.3.3 Links

<https://www.bastille.net/>

2.4 BeyondTrust Retina IoT Scanner



2.4.1 Technology

- Scans network for devices
- Uses port-scan to discover open services
- Tests default and hard-coded credential to discover vulnerabilities
- Product launched 2017, but seems discontinued? Very little information available

2.4.2 Quotes

Utilizing precise information, such as server banner and header data, RIoT is able to pinpoint the make and model of a particular IoT device. From there, RIoT safely tests whether or not that device is using default or hard-coded credentials for Telnet, SSH, or Basic HTTP Authentication, which are the preferred attack vectors that botnets (most notably, Mirai) initially use to breach a system. It's worth reiterating that RIoT does not endanger your devices or network by subjecting them to dictionary-style probes, instead RIoT checks a specific set of credentials known to be used by a specific IoT device. From the cloud, RIoT conducts fast, highly accurate security assessments of your IoT devices, while delivering straightforward and actionable reports. As a result, you're able to quickly identify IoT-related vulnerabilities, clearly understand their potential impact, and decisively act to mitigate threats. Simply specify a target IP or IP range, and RIoT handles the rest.

2.4.3 Links

<https://www.beyondtrust.com/press/offers-free-cloud-based-enterprise-iot-vulnerability-scanner>

<https://www.seguridadar.com/bt/ds-retina-iot-s.pdf>

2.5 Bitdefender BOX

How Bitdefender BOX Works



WiFi & Home Network Security

Secure all Internet-connected devices — even those that can't run anti-virus. Block malware, stolen passwords, identity theft, hacker attacks and more. Protects Windows, macOS, Android & iOS devices against advanced threats. Includes VPN for extra privacy.



Secure Work & Study

Experience the Internet like you should: safe & care-free. Bitdefender BOX is the best solution to secure your entire family, whether you work from home or your children study online. We make sure your WiFi stays safe.



High-Quality Hardware

Bitdefender BOX comes with high-performance hardware for lightning-fast connectivity and virtually instant response to all threats.



Award-Winning Technology

Bitdefender is a world leader in computer and internet security. Enjoy complete protection guaranteed by powerful, innovative technologies recognized by multiple awards from the most trusted testing labs in the industry.

2.5.1 Technology

- Dedicated hardware solution connected to your home router
- Scans whole network for devices, alerts your smartphone when a new one connects
- Scans all devices for vulnerabilities, including IoT devices
- Monitors and blocks malicious behavior on the network

2.5.2 Quotes

Secure all Internet-connected devices — even those that can't run anti-virus. Block malware, stolen passwords, identity theft, hacker attacks and more. Protects Windows, macOS, Android & iOS devices against advanced threats. Includes VPN for extra privacy.

Bitdefender BOX is the innovative security hub for the connected home. It protects all internet-connected devices in your digital life, at home and on the go. With Bitdefender BOX you get complete, multi-layered cybersecurity for your computers, smartphones, tablets, baby monitors, game consoles, smart TVs, and everything that's connected in your household. Bitdefender BOX lets you control all your connected devices from a single app. It employs machine-learning algorithms and intrusion prevention systems to pick up new threats and unsafe behavior and keep your smart home safe.

Bitdefender BOX employs machine-learning algorithms and intrusion prevention systems to pick up new threats and unsafe behavior and keep your smart home safe. It will constantly scan the traffic your IoT devices do and learn their normal behavior. Once Bitdefender BOX observes abnormal traffic through its Anomaly Detection engine, it will block it.

2.5.3 Links

<https://www.bitdefender.com/box/>

<https://www.bitdefender.com/box/compare/>

2.6 Bitdefender IoT Security Platform

		Cloud Essentials	IoT Advanced	IoT Full Stack Customizable
At-home service	Device Detection, Identification & Management	×	✓	✓
	Vulnerability Assessment	×	✓	✓
	Anomaly Detection	×	×	✓
	Brute Force Protection	×	×	✓
	Web Protection	✓	✓	✓
	Network Parental Controls	✓	✓	✓
	DDoS Detection & Protection	×	✓	✓
	Exploit Prevention (IDS/IPS)	×	×	✓
	Sensitive Data Protection	×	×	✓
On-the-go security	Bitdefender Total Security	✓	✓	✓
	Bitdefender Parental Control	✓	✓	✓
	Bitdefender VPN	✓	✓	✓
	Mobile management app (SDK)	✓	✓	✓
xSP Subscription Management Platform (API & GUI)		Yes	Yes	Yes
Space requirements		No footprint	<5 MB required	Flexible

2.6.1 Technology

- Security solution for product developers
- Targeted to IoT devices with OS (assumed from library size)
- Anomaly detection, brute force, DDoS, etc.

2.6.2 Quotes

Bitdefender IoT Security Platform's self-improving design supports the rapid adoption of Internet-connected devices on new or existing infrastructures. It protects the whole networking ecosystem against cyber attacks, malware, and spying attempts. And Bitdefender is uniquely positioned to deliver the best protection available: drawing on the intelligence of more than 500 million endpoints, each new detection automatically improves the platform for all users globally.

Whether you provide your customers services for using the Internet, networking equipment for connecting to the Internet, or taking care of their physical home security, with the Bitdefender IoT Security Platform you can launch or complement your current offering with cyber security.

2.6.3 Links

<https://www.bitdefender.com/iot/>

2.7 Broadcom (Symantec)

2.7.1 Technology

- Lots of file scanning, in part with neural networks. "File reputation", database with trustscore for every file ever seen.
- Zero-trust networking
- "Symantec Critical System Protection", all-in-one, firewall, file integrity, intrusion detection, OS hardening, etc.

2.7.2 Quotes

What Is Zero Trust?

Zero Trust is a data-centric security framework centered on the belief that organizations should not automatically trust anything inside or outside their perimeters and must verify the identity and trustworthiness of everything trying to connect to its resources before granting access-based on identity and trustworthiness. Or simply put, "Trust no one."

Symantec Critical System Protection provides a host firewall, device and configuration control, file integrity monitoring, intrusion detection, operating system hardening, application whitelisting, automatic sandboxing, and many more features

McCorkendale believes the answers to IoT security lie in Manufacture Usage Description (MUD) and secure routers like Norton Core. [Manufacture Usage Description](#) is an open source "nutrition label" for IoT devices. If a device has the MUD specifications employed then the device can be limited to the specific functions for which it's built. A person's refrigerator, for example, can be limited to storing a grocery list that is sent to the user's smart phone each week instead of listening to a conversation where a credit card number is spoken aloud and reports it back to a hacker.

2.7.3 Links

<https://www.broadcom.com/solutions/integrated-cyber-defense/zero-trust-ecosystem>

<https://docs.broadcom.com/doc/critical-system-protection-en>

<https://symantec-enterprise-blogs.security.com/blogs/feature-stories/buyer-beware-iot-security-your-hands>

<https://docs.broadcom.com/doc/internet-of-things-protecting-against-industrial-cyber-attacks-en>

<https://docs.broadcom.com/doc/iot-security-reference-architecture-en>

2.8 Bullguard IoT Dojo



2.8.1 Technology

- Scans network for devices
- Uses cloud-based scanner to analyze vulnerability of devices
- Launched 2018 but seems discontinued?

2.8.2 Quotes

The Dojo Intelligent IoT Vulnerability Scanner features:

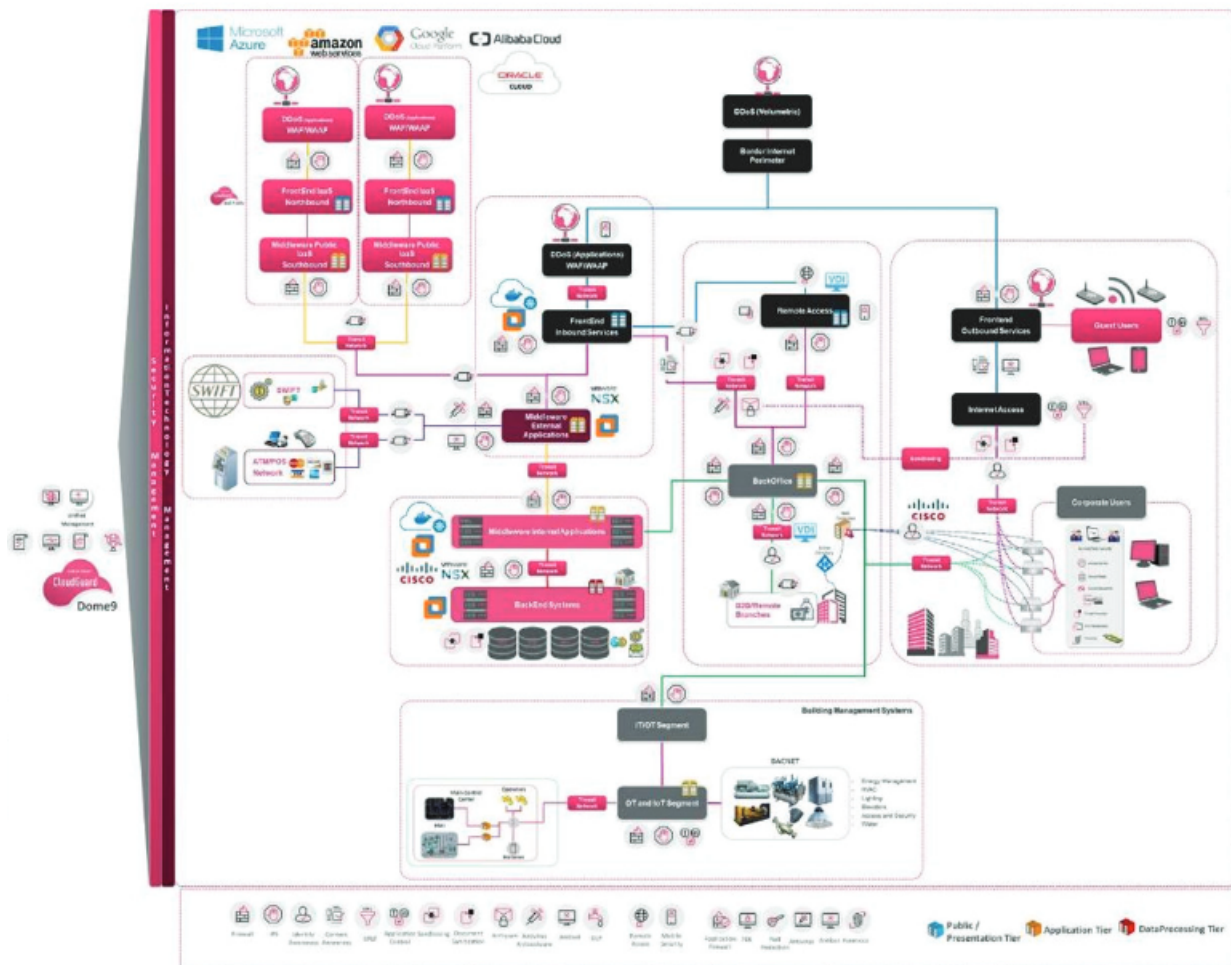
- *Automatic Device Discovery: scans an individual's home Wi-Fi network without having to install any software or connect any devices to their router, and uses combination of both local and cloud-based intelligent detection engines for fast and accurate device discovery. The Dojo app provides the user with full transparency into their home network by identifying every connected device on their network and providing the consumer with comprehensive insight into their Wi-Fi network and all its connected devices.*
- *Network Security Score: the Dojo Intelligent Scanner utilizes Dojo by BullGuard's cloud-based security risk assessment platform to analyze vulnerabilities at the device level. Following each full network scan, the Dojo Intelligent Scanner displays the vulnerabilities and an overall score from 10 (best) to one (worst).*
- *API-based open platform: the Dojo Intelligent IoT security platform is an open, API-based platform that enables integration of third party apps to its discovery and vulnerability engine.*

2.8.3 Links

<https://www.bullguard.com/>

<https://www.bullguard.com/press/press-releases/2018/dojo-by-bullguard-introduces-first-of-its-kind-int.aspx>

2.9 Checkpoint



2.9.1 Technology

- Zero Trust - Network segmenting
- Traffic scanner for known exploits
- Runtime-protection installed on units (Linux?)
- Firmware hardening during build process.

2.9.2 Quotes

Prevent IoT cyber attacks with multi-layer threat prevention

- Minimize the IoT attack surface with zero-trust policy utilizing device attributes and risk profile
- Shield devices from known vulnerabilities before they can be exploited with IoT virtual patching, using 1000s of protections, including over 300 unique IoT protections across intrusion prevention system (IPS), anti-bot and application control (APCL) signatures
- Prevent known and unknown attacks with Check Point Infinity, powered by 60 security service, and continuously updated threat intelligence from Check Point ThreatCloud, which aggregates threat intelligence from 100s of millions of sensors worldwide

Adapt IoT protections to any IoT and OT device

- Automatically identify and classify every IoT device and its risk profile using discovery engines
- Create perfectly suited policies with the industry's broadest application control, supporting over 1,600 IoT and OT applications, protocols and commands

- Apply real time enforcement to prevent IoT devices from compromising other assets or attempting communication with malicious sites
- Uncover firmware security risks – Get a full analysis of your IoT vulnerabilities within an hour

2.9.3 Links

<https://www.checkpoint.com/downloads/products/iot-protect-solution-brief.pdf>

<https://www.checkpoint.com/downloads/resources/absolute-zero-trust-security-wp.pdf>

<https://www.checkpoint.com/downloads/resources/iot-firmware-security-in-three-steps.pdf>

<https://blog.checkpoint.com/2020/02/05/the-dark-side-of-smart-lighting-check-point-research-shows-how-business-and-home-networks-can-be-hacked-from-a-lightbulb/>

2.10 Cisco

		Destination					
		✓	✗	✓	✓	✓	✓
		✗	✓	✓	✓	✓	✗
		✗	✗	✓	✓	✗	✗

2.10.1 Technology

- Network segmenting
- Traffic & behavior analysis (internal and internal↔external)

2.10.2 Quotes

Leverage ISE and Cisco DNA Center to automate end-to-end segmentation. Separate user, device, and application traffic without redesigning the network and align to the zero-trust framework in the workplace with simplified access and control.

The industrial cybersecurity market is at the high growth stage of its life cycle with rising awareness among end users and more ICS-based attacks globally. However, the shortage of security professionals further exacerbates the challenges above, requiring organizations to implement advanced, automated, and intelligent ICS cybersecurity technologies with pre-threat intelligence and anomaly detection being top priorities for organizations. ICS platforms equipped with artificial intelligence (AI) and machine learning (ML) capabilities will unburden security teams. Organizations need a comprehensive ICS cybersecurity solution that protects against malicious external attacks and insider threats and relieves security teams from conducting manual tasks that could be automated. Moreover, a vendor that can overcome these industry challenges and offer a vendor-agnostic platform to simplify and enhance ICS cybersecurity through a comprehensive platform will capture more market share and achieve market leadership

Cisco obtained the Cyber Vision technology through its acquisition of Sentryo SAS, a French ICS cybersecurity provider. The acquisition allows Cisco to offer a holistic approach to ICS cybersecurity through the Cyber Vision platform and Cisco's ICS cybersecurity services. Equipped with advanced AI and ML capabilities, Cyber Vision automatically detects asset inventory as OT endpoints communicate with the network, and uses behavioral analytics to monitor network, device, and user activities. The platform sends operators real-time "abnormal activity" alerts—including for zero-day attacks—sorted by priority level and provides actionable insights, enabling them to mitigate cyber risks rapidly before the environment incurs damage. OT cybersecurity solutions require organizations to deploy sensors across their industrial network to collect information and detect abnormal behaviors. Cisco has the unique capability of running this Cyber Vision feature within network switches, routers, and gateways. This makes the overall solution much simpler to deploy and dramatically reduces its total cost of ownership as the networking team doesn't have to deploy, maintain, and manage a fleet of security appliances or build a separate network to carry the additional traffic created by these appliances to the central analytics platform.

Software-based segmentation

Why segment IoT devices? Segmentation puts those devices out of the reach of attackers and prevents these devices from being used as pivot points to move through the network if they are compromised. Network segmentation is a well-established security best practice. VLANs have been in use for decades, and they still have an important place. However, when we consider securing 30 billion things, the sheer scale of the IoT makes creating enough VLANs impractical, if not impossible. Software-based segmentation uses factors such as location, device type, user role, and so on to create policy that is enforced throughout the network-anywhere

Visibility and analysis

Threats evolve as quickly as the new technologies that attackers strive to exploit. This means that there is limited time between threat detection and your response. You need to detect new devices, protocols, applications, and users as they attempt to get on your network-anywhere on your network. You also need to detect and block threats before they can affect your business. An automated, multilayered capability to analyze the network traffic throughout your network, as well as traffic entering and exiting your organization, to detect anomalies, block threats, identify compromised hosts, and even help prevent user error is required to defend against a variety of threat vectors. Rule-based detections will ferret out the latest known threats; protocol analysis helps prevent human error; anomaly detection uncovers new threats and will identify "patient

0.” Malware command and control traffic is blocked for your in-house and mobile users, and web traffic is continuously inspected for suspicious behavior.

Bringing it all together

The threats you face are dynamic, and your defenses should be, too. Imagine that a contractor connects a laptop infected with a worm to your network. The worm immediately attempts to propagate itself, and an automated response kicks in where:

1. The malicious traffic is detected and blocked.
2. The laptop is quarantined from the network.
3. The user account is disabled.
4. Your user console can visually display that your critical systems were never in danger.

You manage the entire process without it affecting the business because you were prepared and executed your prepared incident response plan.

2.10.3 Links

<https://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/network-access-net-segmentation-aag.pdf>

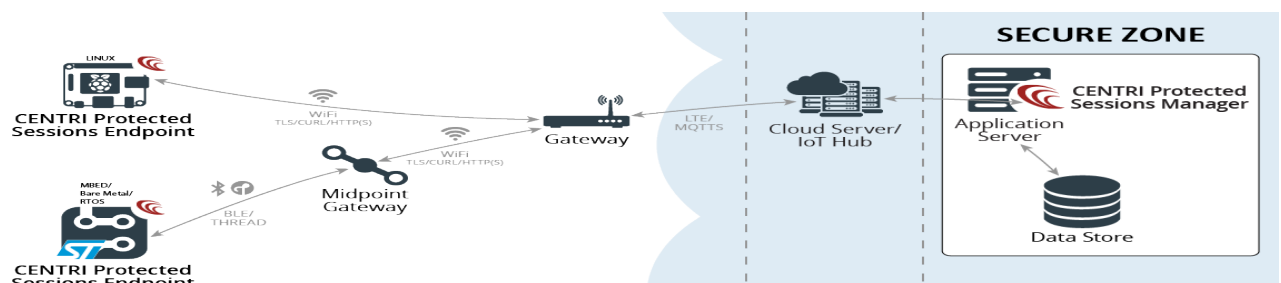
<https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html#~case-studies>

https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/2407595/Cisco_ETL_Award_Write-Up.pdf

<https://www.cisco.com/c/dam/assets/offers/pdfs/protecting-promise-of-internet.pdf>

<https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/nb-06-ai-endpoint-analytics-wp-cte-en.html>

2.11 Centri



2.11.1 Technology

- End-to-end encryption library for embedded devices
- Completely independent from network protocol
- Unlimited session lengths (months?)

- Intended for small MCUs

2.11.2 Quotes

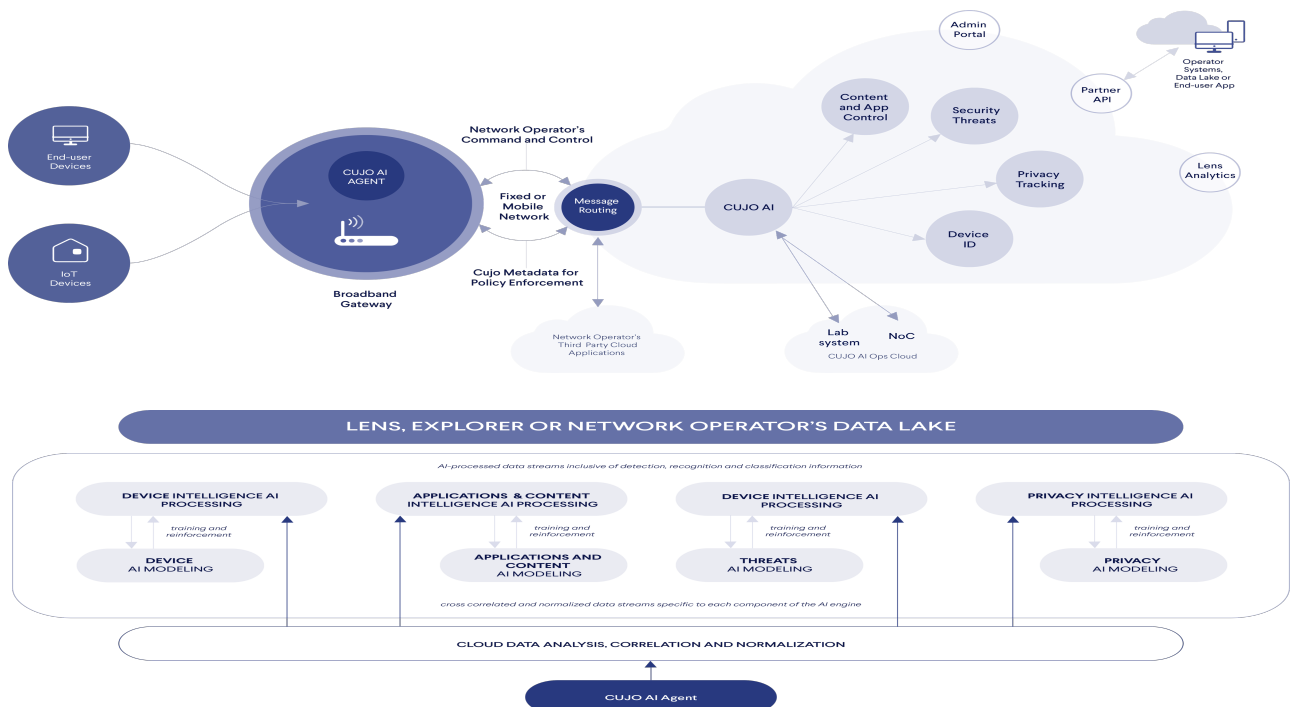
Secure your IoT data from creation to consumption, through every mile along the way. Protected Sessions changes the game by giving you data security for bi-directional communications while freeing you from the limitations of multiple network protocols and a mixed IoT topology. Session lifecycles are IoT-friendly by design – by working within the constraints of low-power MCU devices using low-power networks that may have intermittent network access, Protected Sessions can maintain the security of your communications channel through lifespans from seconds to months! Using heavyweight industry standard encryption, CENTRI Protected Sessions is optimized for lightweight devices with data compression and a tiny footprint, providing both security and efficiency between the endpoint device and the back of the cloud.

2.11.3 Links

<https://www.centritechnology.com/>

https://www.centritechnology.com/wp-content/documents/Datasheet_CENTRI-Protected-Sessions.pdf

2.12 Cujo AI



2.12.1 Technology

- Two markets, first is for Internet Service Providers, second is for enterprises/consumers with device networks
- Give operators ability to "develop insights on operational issues and marketing opportunities"
- Agent software placed in gateway, metadata sent to cloud for processing

2.12.2 Quotes

Our AI models can safely detect data security threats, problematic content or privacy breaking concerns that affect consumer and business networks, and block them before they can cause harm.

CUJO AI Agent is a high-performance, small and low overhead software module deployed within consumer and business broadband gateways, 5G cloud cores or as part of a software-defined network architecture to capture and process critical data from the network flow, and act upon it to block threats, content or network access.

CUJO AI Engine processes packet level data to extract salient features to identify, classify and inventory connected devices and their associated operating systems, accessed content, used applications, security threats and vulnerabilities, privacy. It primarily utilizes supervised learning and reinforcement training algorithms.

CUJO AI Engine utilizes unsupervised learning and reinforcement training techniques to identify patterns in correlated data to proactive develop insights on operational issues and marketing opportunities.

CUJO AI Engine builds threat knowledge by ingesting multiple threat and security feeds and models them into a single set of ML algorithms. It also monitors and models IoT devices to understand normal behavior, enabling it to flag zero day threats.

"So, CUJO AI is fundamentally an AI company that uses artificial intelligence and machine learning, specifically with deep learning algorithms, to address the challenge of providing network operators, and only network operators, with unified digital life protection solutions," Peiro said.

Peiro defined digital life protection solutions as a combination of network security, content control and digital control by parents as well as privacy and tracking protection. Peiro said CUJO AI has a two-pronged approach to its AI-based strategy.

"The first is empowering operators to provide their customers with value-added services that they can monetize directly in the domain of digital life protection, and the second part of our business is to provide insight and analytics and protection to the network operator itself," he said.

Contrary to traditional deep packet inspection (DPI) methods, CUJO AI is able to monitor the traffic flow of every device in a home by installing its private stack on gateways using open source frameworks. Peiro said DPI is becoming obsolete because of the encryption that it uses, and DPI slows down the speed of a connection.

"We combine our ability to look at data and how it flows in and out of the home and small business gateways that operators place in their customers' premises," Peiro said. "We can identify what devices generate this traffic, or what devices received the traffic and create AI-based maps, AI based networks, that map behavior exclusively looking at technical aspects of the network traffic, not the content itself," Peiro explained

2.12.3 Links

<https://cujo.com/>

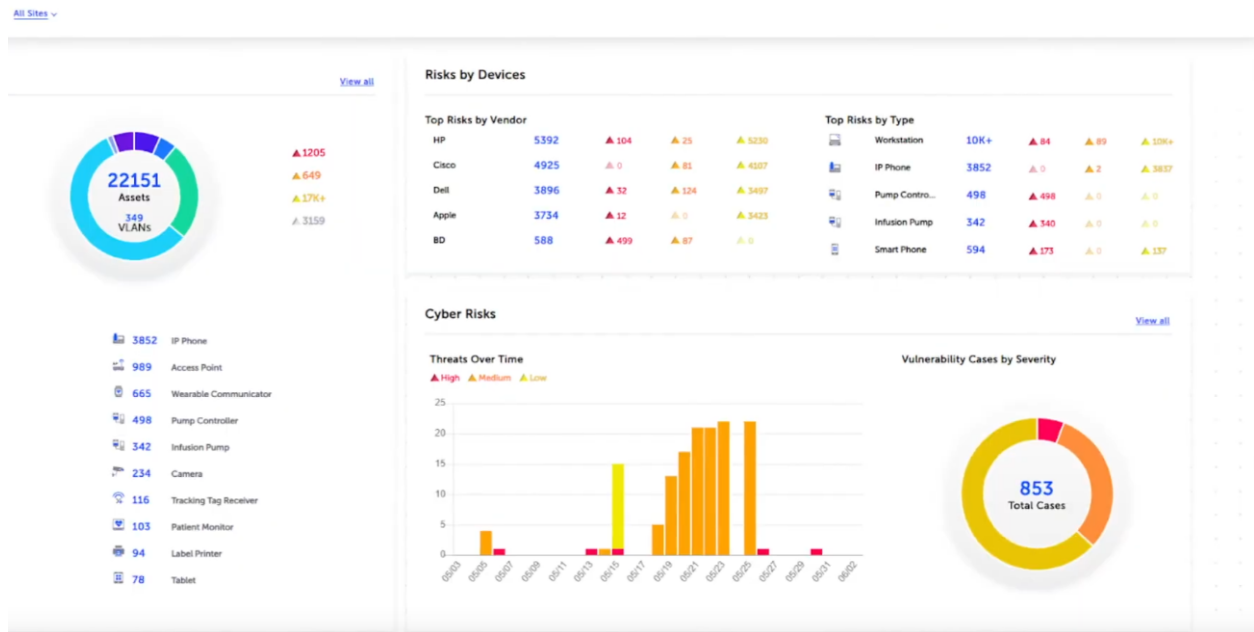
<https://cujo.com/agent/>

<https://cujo.com/engine/>

<https://cujo.com/ai-driven-network-security/>

<https://www.fiercetelecom.com/ai/cujo-ai-has-home-security-covered-for-both-service-providers-and-their-customers>

2.13 CyberMDX



2.13.1 Technology

- Focuses on protecting medical devices in hospitals
- Automatically discovers and tracks asset on network by analyzing 100+ proprietary protocols
- Alerts you of devices on network that are vulnerable
- Zero-trust micro segmentation of networks

2.13.2 Quotes

With so many connected devices and diverse motives driving bad actors, hospitals have become a cyber battleground. Medical devices introduce a wide range of operating systems and communication protocols that traditional cyber security solutions cannot adequately protect. Leveraging our expertise in medical device vulnerabilities, CyberMDX delivers zero-touch threat prevention through an easy-to-deploy solution. We provide unmatched visibility and protection for medical and IoT devices, ensuring operational continuity as well as patient and data safety.

Ransomware like Ryuk or WannaCry continues to have a significant impact on hospital operations. Standard security tools simply do not provide the context-aware visibility needed to understand and protect medical environments. CyberMDX illuminates your digital domain - offering concise and prioritized context-aware risk assessment, as well as continuous network vulnerability patrolling and protection.

Zero-trust security model enables micro-segmentation based on asset visibility and trusted relationships.

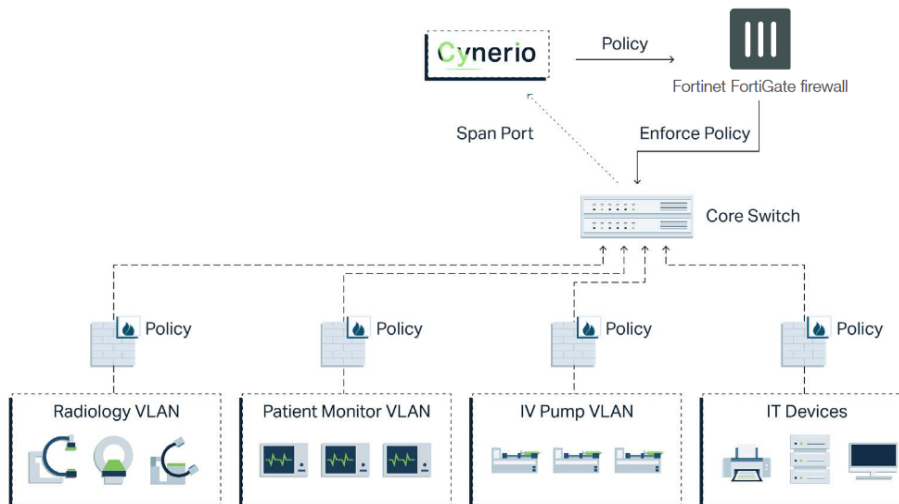
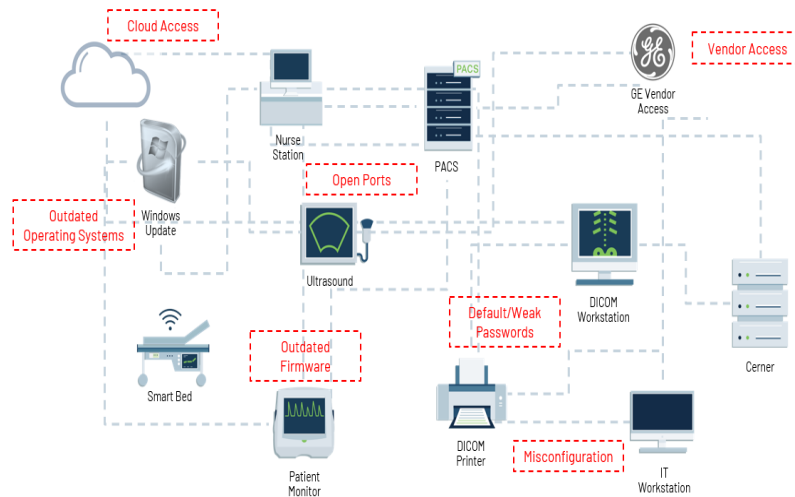
2.13.3 Links

<https://www.cybermdx.com/>

<https://www.cybermdx.com/solution-overview/it-security/>

2.14 Cynerio

What Puts Devices at Risk?



2.14.1 Technology

- Focuses on protecting medical devices in hospitals
- Automated device discovery on network
- Flags vulnerabilities and identifies malicious behavior with some sort of AI
- Zero-trust network microsegmentation

2.14.2 Quotes

Millions of Healthcare IoT devices are used to care for patients and streamline clinical workflows, but their inherent vulnerabilities to malware and cyber attacks put hospitals and

patients at risk. They can't be disconnected because of their critical roles in patient care and IT network infrastructures, and standard IT solutions can't secure them. This leaves hospitals exposed and jeopardizes patient safety, data confidentiality, and service availability.

The Cynerio platform promotes proactive and preemptive cybersecurity with automated risk reduction, threat mitigation, attack prevention tools, and step-by-step remediation programs built on a Zero Trust framework infused with clinical context to get hospitals secure - fast.

Take control and cover all your threat vectors: From Vendor Access to Cloud Access, Forensics, and Virtual Segmentation, our unique set of solutions automates risk reduction by offering the optimal remediation path. Starting from the most critical risks that have the highest impact on your organization, achieve quick and sustainable security posture.

2.14.3 Links

<https://www.cynerio.com/>

https://assets-global.website-files.com/5d2dbce8358ee9004d1c7eb6/5f9ac484afa194278effa14a_Cynerio%20Healthcare%20IoT%20Cybersecurity%20Platform.pdf

2.15 Darktrace

ENTERPRISE IMMUNE SYSTEM
Self-learning Detection

CYBER AI ANALYST
Automated Investigation

DARKTRACE ANTIGENA
Autonomous Response

DARKTRACE IMMUNE SYSTEM
World-leading Cyber AI

EMAIL Microsoft 365 Google Workspace	SaaS Salesforce box T	CLIENTS ((o))	CLOUD aws Microsoft Azure	NETWORK ((o))	OT Factory icon	IoT ((o))
Workforce			Infrastructure		Industrial	

2.15.1 Technology

- AI that learns behavior of devices and users

- Highlights threats in online dashboard
- Automated response through their "Antigena" product
- Allows for automated investigation of attacks that have occurred

2.15.2 Quotes

The Darktrace Immune System is the world's leading autonomous cyber defense platform. Its award-winning Cyber AI protects your workforce and data from sophisticated attackers, by detecting, investigating and responding to cyber-threats in real time — wherever they strike.

Darktrace's Enterprise Immune System learns normal 'patterns of life' to discover unpredictable cyber-threats, while delivering visibility across your dynamic workforce — from cloud and SaaS to endpoints and the corporate network.

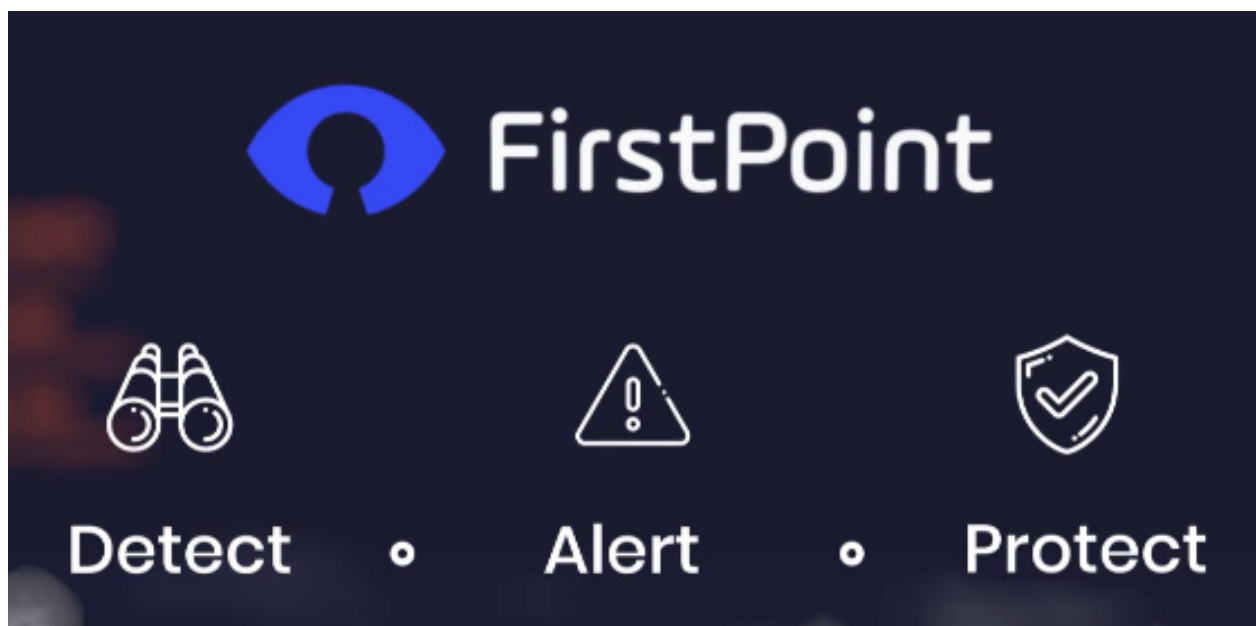
Darktrace's core detection engine, uses unsupervised machine learning to build a dynamic understanding of 'normal' for each organization it safeguards. Rather than rely on rules, signatures, fixed baselines, or training data, the immune system learns from your constantly changing digital environment — forming a bespoke and multi-dimensional understanding of every user, device, and all the complex relationships between them. This unique self-learning approach enables Darktrace to detect advanced attacks at an early stage, and well before they have time to escalate into a crisis — from a novel strain of ransomware or an insider attack, to a coordinated spear phishing campaign or critical cloud misconfiguration.

2.15.3 Links

<https://www.darktrace.com/en/>

<https://www.darktrace.com/en/resources/wp-platform.pdf>

2.16 FirstPoint



2.16.1 Technology

- Intended for SIM/eSIM devices.
 - Protects with software primarily in cellular gateway
-

2.16.2 Quotes

Protect any connected device

Secure all SIM-based or eSIM-based devices, 2G-5G including NB-IoT, LTE-M, eMBB, mMTC, URLLC and integrated with network slicing, for static or roaming devices, with or without an operating system, via the device or a central mobile gateway.

How Does it Work?

FirstPoint’s security solution protects without hardware installation, software updates or any impact on your devices, A truly invisible solution, the platform acts behind the scenes to identify, alert and mitigate any cellular network risk to connected devices. Simply define a list of devices to protect, and decide whether to provision the SIM applet OTA, or use new SIMs altogether. Your users will continue to interact with their devices as usual, with no impact on their performance or use. It really is as straightforward as that.

Out of sight, FirstPoint protects from three directions:

- *At the core: A secured, overlay core network that operates side by side with the MNOs network, without any impact on operations.*
- *On the SIM: A dedicated applet on the SIM itself, providing an added layer of protection to the device, and guaranteeing full anonymity.*
- *Across all communication: Any signalling and data traffic is routed via the protected network, adding security at the earliest possible stage.*

2.16.3 Links

<https://www.firstpoint-mg.com/cellular-iot-cybersecurity/>

2.17 Forescout



2.17.1 Technology

- Discover and profile IoT devices on network

- Checks risk profile of each unit with online database of 12 million devices
- Automates network segmentation to reduce risks
- Continuously monitors for changed behavior, spoofing, vulnerabilities, etc.

2.17.2 Quotes

Forescout applies Zero Trust principles to identify and secure IoT devices.

- Forescout provides **complete visibility** – a critical component for identifying and classifying IoT and other devices on the network
- By designing **trust zones** for IoT devices, you can define appropriate communication to and from those devices
- With **passive detection** capabilities, Forescout will monitor IoT devices, reducing the potential for business disruptions and managing the remediation workflow should an IoT-related incident occur

It's essential to obtain complete visibility and device context of all IoT, OT and critical infrastructure endpoints across your heterogeneous environment. The Forescout platform:

- Continuously discovers all IP-connected devices, physical and virtual, the instant they enter your network– no software agents required
- Provides in-depth visibility into all devices using 20+ active and passive discovery, profiling and classification techniques
- Leverages the Forescout Device Cloud, the world's largest data lake of crowdsourced device intelligence, providing a cross-industry single source of truth on the fingerprints, behavior and risk profiles of more than 12 million devices

In today's heterogeneous EoT environments, an enterprise that adopts the Zero Trust model must be capable of network segmentation and orchestrated incident response across all EoT domains. With Forescout, you can:

- Correlate access with user identities (who is doing what, where, when and why)
- Provision devices to dynamic network segments based on policies and real-time context
- Map data flows to design segmentation policies and simulate them for non-disruptive deployment
- Automate segmentation to reduce cyber and operational risk

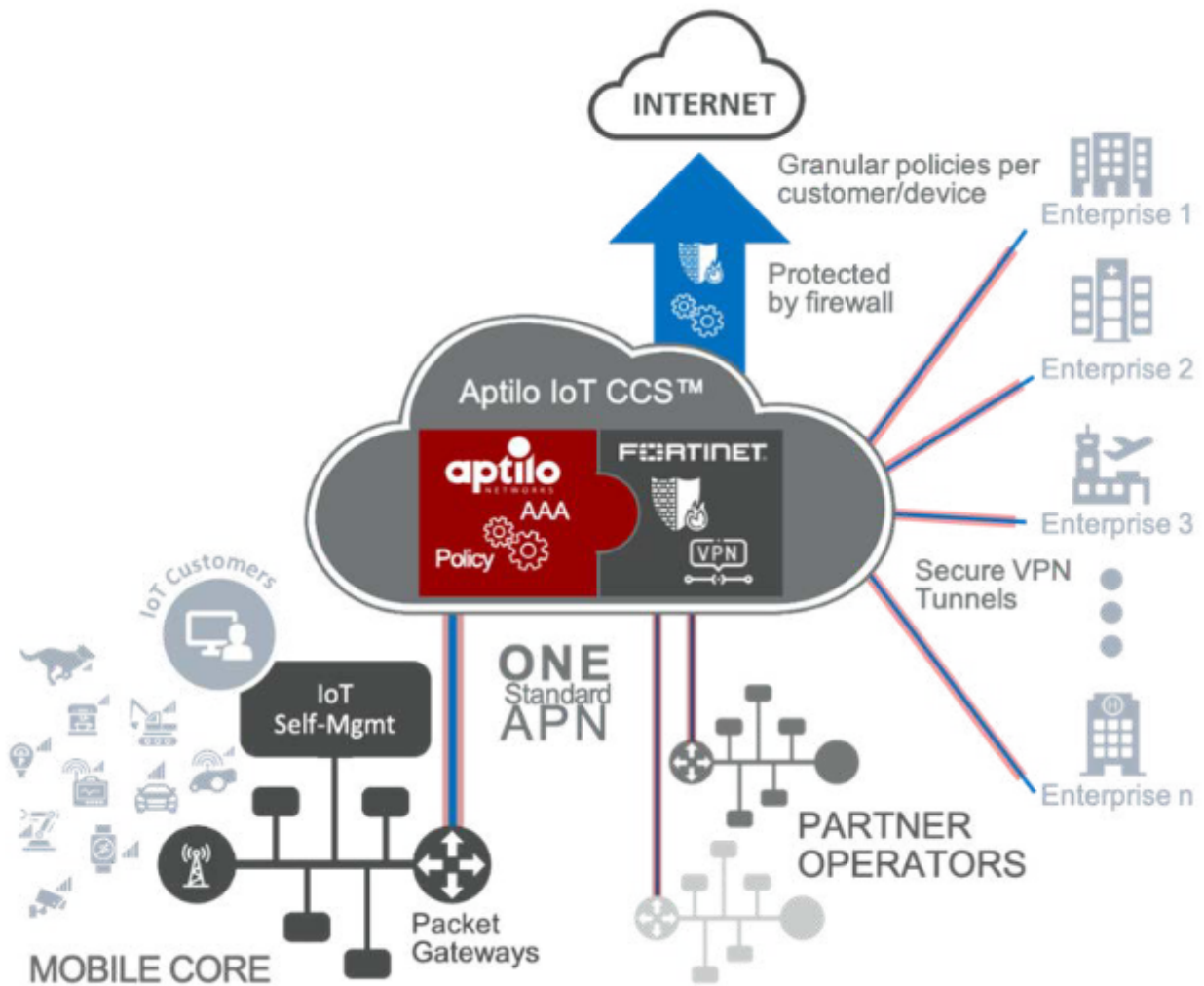
2.17.3 Links

<https://www.forescout.com/>

<https://www.forescout.com/company/resources/internet-things-solution-brief/>

<https://www.forescout.com/company/resources/how-the-iot-is-transforming-cybersecurity-strategy/>

2.18 Fortinet



2.18.1 Technology

- Large product portfolio, overall security and firewall provider
- Automatic discovery of devices on network
- Network segmenting with NAC VLANs, controlling what IoT devices can get access to on the network
- Monitor devices for compromise and takes action automatically

2.18.2 Quotes

Providing protection for IoT devices and the networks they connect to should include Zero-Trust principles, including the tight management of access control. Whether in enterprise, medical, industrial, or other settings where IoT devices proliferate, it's critical to ensure IT administrators can:

1. *Understand what IoT devices are being deployed by seeing and profiling every device connecting to the network*
2. *Manage access to the network, including not only what devices are connecting to the network, but also what areas of the network IoT devices can access*
3. *Monitor the IoT devices once on the network, to ensure access stays consistent and the devices don't become compromised*
4. *Automatically take immediate action in the event of a device compromise or other security issue*

FortiNAC enables three key capabilities to secure IoT devices:

- Network visibility to see every device and user as they join the network
- Network control to limit where devices can go on the network
- Automated response to speed reaction time to events from days to seconds

The FortiGate next-generation firewalls (NGFWs) and the FortiWeb web application firewalls provide a powerful platform to deliver security for the MNO IoT services and ecosystem.

FortiGate capabilities include:

- Stateful firewalling to block non-authorized destinations and anomalous behavior
- IPS to detect and block a wide range of IoT attacks such as:
 - Exploit attacks
 - Scanning attacks
 - Fuzzing attacks
- IoT rate-based behavior rules and enforcement
- TLS inspection for attack detection over secure IoT links
- Application and protocol control authorized for IoT use
- Antivirus to protect the IoT platform devices
- Anti-botnet to stop malicious bots

FortiWeb capabilities add:

- API protection within the IoT ecosystem (devices, platform, applications)
- Automation framework to link events and trigger actions for rapid risk mitigation

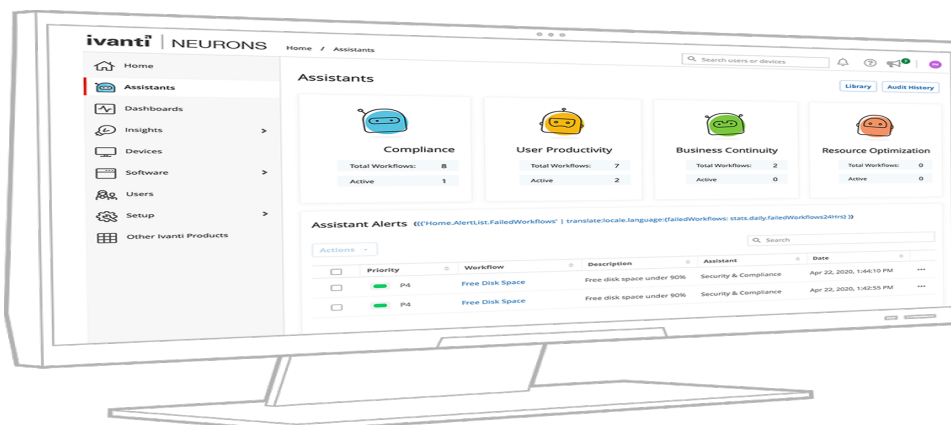
2.18.3 Links

<https://www.fortinet.com/>

<https://www.fortinet.com/products/network-access-control>

<https://www.fortinet.com/solutions/mobile-carrier/iot-ecosystem>

2.19 Ivanti



2.19.1 Technology

- "Discover, Service, Manage and Secure endpoints"

- "Neurons" is an automation platform based on MQTT for different network tasks.
- Discovers devices, issues relating to configuration or security, and self-heals them automatically.
- Online dashboard to see devices in network and automatically secure them

2.19.2 Quotes

The demands on IT are growing exponentially as remote working becomes the next normal with employees working anywhere, anytime and expecting fast, personalized, consumer-like experiences. With the explosive growth of endpoints, edge devices, and the data they generate, cyber-security threats are reaching catastrophic new heights. With hyper-automation powered by advanced artificial intelligence, the Ivanti Neurons platform uses machine and deep learning to self-heal, self-secure, and self-service devices.

Ivanti Neurons for Discovery delivers accurate and actionable asset information in minutes. This provides visibility in real-time using active and passive scanning and third-party connectors. These provide normalized hardware and software inventory data, software usage information and actionable insights to efficiently feed configuration management and asset management databases.

Ivanti Neurons for Edge Intelligence gives IT the ability to query all edge devices using natural language processing (NLP) and get real-time intelligence across the enterprise in seconds. It provides quick operational awareness, real-time inventory, and security configurations across the edge leveraging sensor-based architecture.

Ivanti Neurons for Healing offers an army of automation bots to proactively detect, diagnose, and auto-remediate configuration drift, performance, and security issues, and maintain compliance for endpoints. Automation of routine tasks paves the way to creating a truly self-healing environment, reducing time, costs, and improving the employee experience.

2.19.3 Links

<https://www.ivanti.com/>

<https://www.ivanti.com/solutions/ivanti-neurons>

2.20 IoTsploit

<h3>VULNERABILITY SCANNER</h3> <p>Automates detection and identification of device model and maker based on a new algorithm. Powered by our R&D lab, it targets weak configurations, hidden back doors and other exploits.</p>	<p>20/20 visibility of network connections Shifts control from vendor back to operator;</p> <p>Night vision ability Hunts down hidden weaknesses such as back doors and hidden exploits;</p> <p>Monitoring 24/7 Prioritises asset availability;</p>
<h3>FIRMWARE ANALYZER</h3> <p>Allows manufacturers and vendors of networked software and sensors to detect hardcoded passwords and keys, back doors and hidden services and interfaces in device firmware BEFORE putting products on the shopfloor, thus safeguarding customer security and assuring own compliance and service integrity.</p>	<p>Compliance with increasingly comprehensive legal requirements to ensure user and customer security service providers will need to take ownership of security for customers</p> <p>Real-time detection and patching mechanism automated and scalable firmware bug fixing as a QA/AC measure</p> <p>Transparent cataloging of resources visibility of connected inventory</p>

2.20.1 Technology

- Detects devices on network
- Scans devices for vulnerabilities
- Very few details of implementation

2.20.2 Quotes

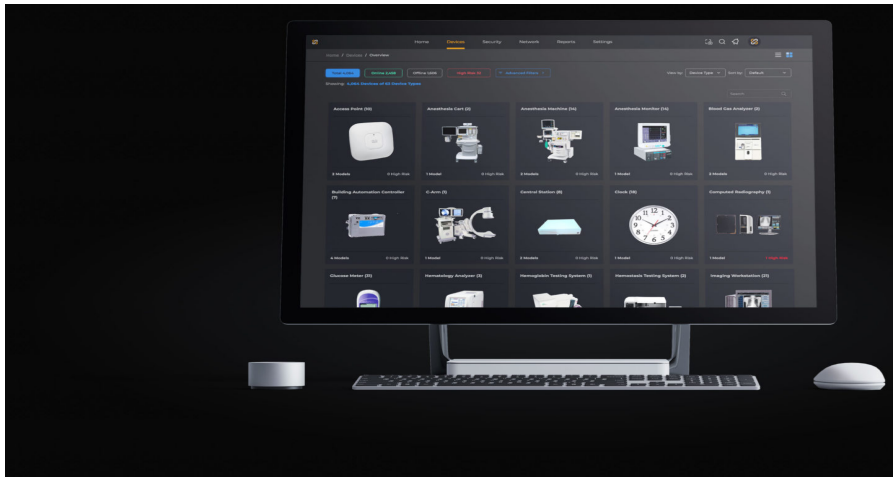
Vulnerability Scanner: Automates detection and identification of device model and maker based on a new algorithm. Powered by our R&D lab, it targets weak configurations, hidden back doors and other exploits.

Firmware analyzer: Allows manufacturers and vendors of networked software and sensors to detect hardcoded passwords and keys, back doors and hidden services and interfaces in device firmware BEFORE putting products on the shopfloor, thus safeguarding customer security and assuring own compliance and service integrity.

2.20.3 Links

<https://iotsplloit.co/>

2.21 Medigate



2.21.1 Technology

- Focuses on protecting medical devices in hospitals
- Automated device discovery on network
- Flags vulnerabilities and unpatched devices
- Identifies malicious behavior on network through Deep Packet Inspection

2.21.2 Quotes

Medigate puts “clinical intelligence” into its security platform so IT, IS, and biomed can truly understand what’s on the network, where it’s coming from, and what’s it’s doing. Clinical context gives you an advantage, enabling the accurate identification of anomalous behavior, communications and traffic patterns and the development of effective policies. Comprehensive device profiles enable you to establish additional security filters to quickly shut down segments of the network when needed and manage device lifecycles more effectively.

The Medigate platform is the only solution that has cataloged thousands of IoT and IoMT devices, enabling it to discover and precisely identify 100% of connected devices on a provider’s clinical network. Medigate uses deep packet inspection (DPI) techniques on passively-collected network traffic to obtain granular identifications for each device, including manufacturer, model, OS, app and hardware versions, and location, allowing dynamic medical device inventory management. Data gathered from DPI is also used to calculate a device’s risk score, incorporating device parameters, network topology, and published CVEs, among other parameters to inform the risk assessment.

Only Medigate has the contextual understanding to accurately detect credible threats. The platform understands IoT and IoMT protocols and manufacturer-intended protocols to detect malicious or out-of-order behavior. It meticulously analyses device and network communications, categorizes them by protocol and destination, and marks any suspicious activity, in real-time, with minimal false positives.

The Medigate platform integrates with existing NAC and firewall solutions to enforce clinically-driven policies and prevent malicious communications, in real time, without affecting the operation of the medical device under attack. Intelligence gathered through the platform’s visibility and detection capabilities is used to build rule-based policies tailored for each type or group of connected devices. Medigate also identifies all current VLANs and virtual security groups and collaborates with the hospital to build a safer segmentation plan. Medigate allows

the healthcare provider to make their existing policy enforcement infrastructure much more effective in the clinical setting.

2.21.3 Links

<https://www.medigate.io/>

https://medigate.pathfactory.com/c/clinical-network-cybersecurity-requires-clinical-expertise?x=yqXts5&lb_email=

2.22 NanoLock

2.22.1 Technology

- Firmware library protecting intruders from modifying flash memory
- Changes to flash need to be authenticated by remote server

2.22.2 Quotes

NanoLock introduces a new approach for tackling persistent attacks: An embedded gatekeeper that allows persistent changes to critical code only if authenticated and signed by an external authorized server. The patented solution prevents manipulation and erasure of critical code through establishing a root-of-trust in the device's Flash memory (Non-Volatile Memory) and moving the control from a vulnerable remote device to a trusted entity in the customer's cloud or data center. Every attempt for a persistent change to the device's critical code in the Flash, such as calibration, configuration, applications, is verified by the root-of-trust that acts as a gatekeeper. Only update requests that were authenticated by an external server will be approved. Unauthorized change attempts are rejected and alerted, blocking cyber-attacks by insiders, outsiders and even supply chain attackers.

2.22.3 Links

<https://www.nanolocksecurity.com/>

2.23 Outpost 24 (acquired Pwnie Express)



2.23.1 Technology

- Pwn Pulse is a hardware device running analysis (1.8GHz Intel i3, 4GB RAM, OS based on Kali Linux)
- Discover and fingerprint devices on the network
- Monitor devices for suspicious behavior

2.23.2 Quotes

Discover and categorize every device on your network automatically, and fingerprint them for tracking and monitoring.

Identify any wired, wireless (WiFi) and Bluetooth connected devices lurking in your network so you will never miss a rogue device again.

Continuously monitor your assets and network for unusual device behavior or unauthorized network access to prevent intrusion attempts.

Get instant alerts for potential threats so you can quickly isolate and neutralize unwanted devices, or remove unknown access points.

2.23.2.1 DISCOVER & INVENTORY ALL DEVICES

Real time discovery of all IT and IoT devices — wired, wireless, and Bluetooth — on the network and in the surrounding airspace.

2.23.2.2 CAPTURE DEVICE SNAPSHOTS

Automatically create comprehensive fingerprints of devices consisting of manufacturer, OS, ports, running services, and IP/MAC address.

2.23.2.3 ESTABLISH DEVICE IDENTITIES

Correlate interfaces, analyze snapshots, and evaluate device relationships to create individual device identities and track their behavior and changes.

2.23.3 Links

<https://outpost24.com/products/wireless-security>

<https://outpost24.com/products/wireless-security/pulse>

https://outpost24.com/sites/default/files/2020-03/Wireless-Security-The-Internet-of-Evil-Things-2020.pdf?utm_campaign=Download-Internet-of-Evil-Things-2020&utm_medium=email&_hsmi=85353970&_hsenc=p2ANqtz-U2Mfd-wtFqXGFpMpK2xcq8UQD4bv32vGYJE-Vq8yk3YB44QyUsPqzT753SzCJD1uWdKDAL-UgqER4ycVgn7jROJmXnvdIBpNhC0mkRICO7wKt5j8&utm_content=85353970&utm_source=hs_automation

<https://kb.outpost24.com/kb/how-to-s>

2.24 Overwatch

The screenshot displays the Overwatch security interface. At the top, there are filters for 'THREATS', 'TIME DETECTED', and 'ACTION'. The main area shows a list of threats:

- Unusual inbound traffic**: Traffic Source: 192.168.1.13, TRAFFIC ORIGIN: Beijing, China.
- Unusual high inbound traffic spike**: 265 connections.
- Unusual high inbound traffic spike**: 265 connections, 5 minutes ago, Traffic Blocked.
- Device has moved**: TRAFFIC ORIGIN: Beijing, China, 8 minutes ago, Lock Device.
- Config changed**: 3 hours ago, Lock Device.

A modal dialog titled 'Traffic Blocked' is open, asking 'Do you want to apply this as a policy rule?'. It has two radio buttons: 'Only this device' (selected) and 'All devices'. There are 'Yes' and 'Not this time' buttons.

2.24.1 Technology

- Edge-deployed firewall with cloud monitoring and configuration interface
- Primarily intended for IoT devices with OS
- Installable agent application reports monitoring data up to cloud-hosted web interface

2.24.2 Quotes

Overwatch is a security platform designed to secure network connected devices. Its purpose is to help device owners, fleet operators, server admins, DevOps engineers, and more, track and

monitor their devices and servers, preventing nefarious actors from unauthorized access and detecting irregular behavior that might otherwise go unnoticed. You can think of Overwatch as a edge-deployed firewall and security monitoring solution.

Overwatch Devices

Overwatch uses an installable device agent to monitor your devices, analyzing and logging their regular behavior and enforcing security rules that you configure in the Overwatch web interface. The term Device refers to any platform or physical hardware on which our agent can be installed.

The Overwatch Agent

Our agent runs as a service on your device and its purpose is two-fold: it enforces any Security Policy rules that you've defined in the Overwatch web interface, and it sends regular status updates to the Overwatch platform for analysis.

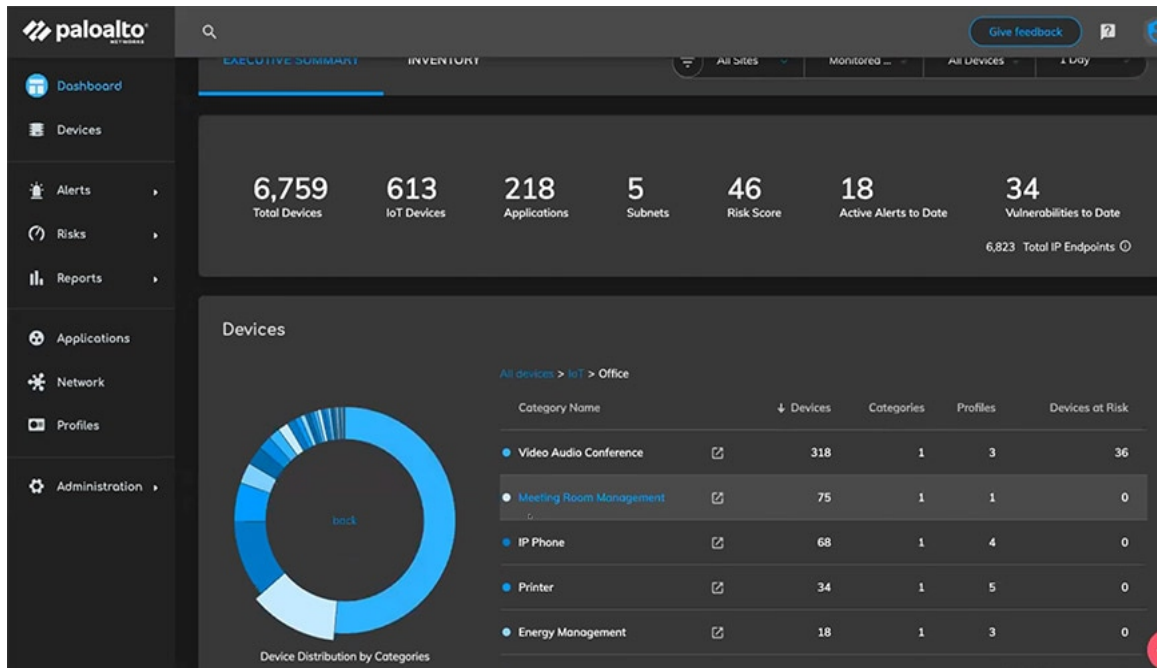
The information sent out by the agent include plain keepalives, inbound and outbound traffic data, open connections and general details such as the device's IP. The privacy of our user's data is very important to us, as such all communication between the agent and the Overwatch server is encrypted, and while we do analyze the behaviour of the device — such as the amount of traffic exchanged between the device and the network — the data itself is never sent to Overwatch. If you have any concerns about privacy, please get in touch and we'll be happy to discuss our security measures in more detail.

2.24.3 Links

<https://overwatchsec.com>

<https://overwatchsec.com/documentation.html>

2.25 Palo Alto Networks (acquired Zingbox)



2.25.1 Technology

- Firewall with ML and cloud integration to protect (including IoT) networks
- Discovers and identifies IoT devices, scans them for vulnerabilities
- Learns traffic patterns, proactively guards against new threats

2.25.2 Quotes

Leveraging a machine learning-based approach, our cloud-delivered IoT Security service quickly and accurately discovers and identifies all unmanaged IoT, IoMT, and OT devices in real time, including those never seen before. IoT Security uses crowdsourced data to identify anomalous activity, continually assess risk, and offer trust-based policy recommendations to improve your security posture. Combined with our industry-leading ML-Powered Next-Generation Firewall (NGFW) platform, IoT Security can prevent threats, block vulnerabilities, and automatically enforce policies either directly or through integrations, reducing the strain on your operations team and keeping devices safe. IoT Security deploys effortlessly from the cloud and requires no additional infrastructure.

Perform vulnerability analysis, detect anomalies in abnormal device behavior, calculate and assess risk to prioritize action.

Use collective threat intelligence to deliver real-time protections for unknown threats, and investigate behavioral anomalies or other never-heard-before threats unique to your IoT environment.

2.25.3 Links

<https://www.paloaltonetworks.com/>

<https://www.paloaltonetworks.com/network-security/iot-security>

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/iot-security.pdf

2.26 SecuriThings



Risk Detection

Endpoint protection capabilities



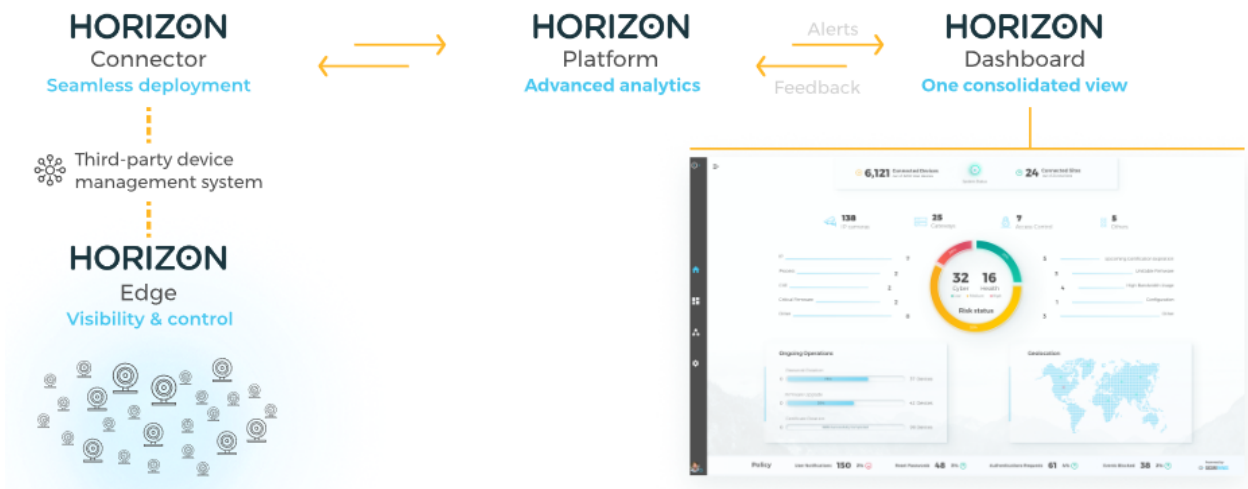
Predictive Maintenance

Real-time health monitoring & analysis



Automated Operations

Mitigation & maintenance



2.26.1 Technology

- Management interface for IoT devices
- Automate operations (e.g. password switch) over whole fleet of devices
- Collects metadata from devices and analyzes it with AI and ML

2.26.2 Quotes

SecuriThings Horizon detects and mitigates IoT-specific cyber-attacks by monitoring the cyber security posture of each device. Horizon deploys agents or agentless modules to pull data from each edge device and leverages advanced analytical capabilities to detect abnormal behaviors. Organizational policies are then applied to mitigate threats in real-time.

SecuriThings Horizon detects the most common and known IoT-specific cyber-threats such as:

- *Brute force attack (successful / attempt)*
- *Port scan attack*
- *Backdoor activity / passive backdoor*
- *Identification of suspicious process*
- *And more*

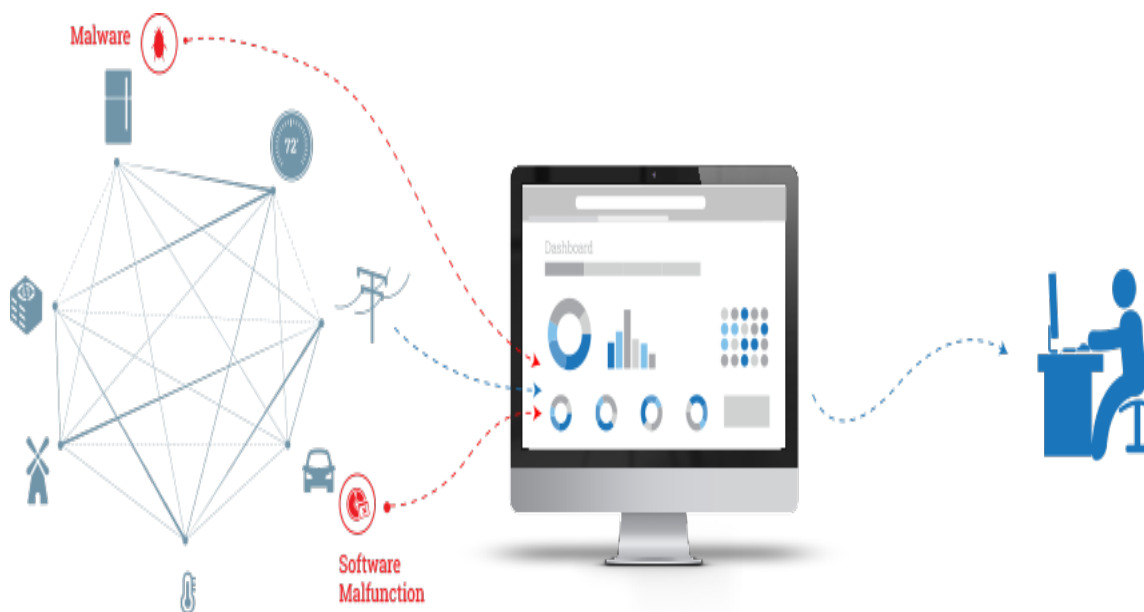
IoTOps start with the collection of tremendous amounts of data from each and every managed device. This metadata is analyzed and translated into alerts which should be then prioritized, leveraging AI and Machine Learning capabilities.

2.26.3 Links

<https://securithings.com/>

<https://securithings.com/wp-content/uploads/2020/04/SecuriThings-Horizon-Brochure.pdf>

2.27 SensorHound



2.27.1 Technology

- Monitoring interface for IoT devices
- Not released yet, very few details
- "Real-time detection of software failures and intrusions"

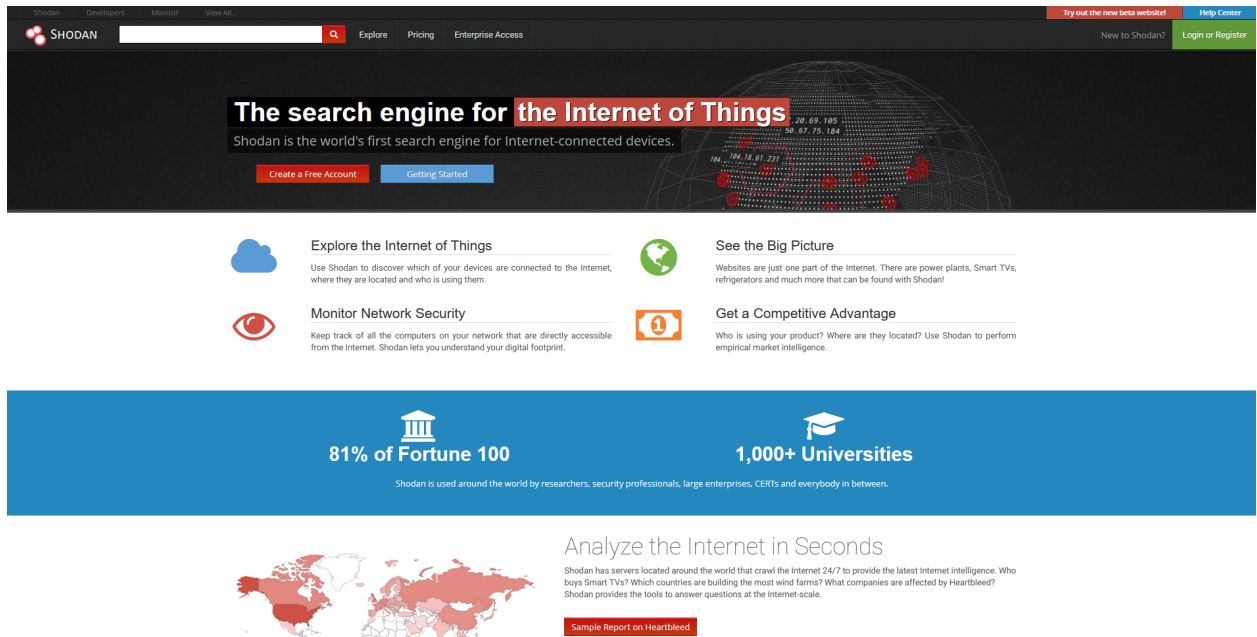
2.27.2 Quotes

SensorHound's mission is to improve the security and reliability of the Internet of Things (IoT). Our suite of software products provides continuous in situ deployment monitoring you can count on, and sends immediate alerts with detailed diagnostic information when software failures or security intrusions are detected. Based on patent-pending technology developed by leading IoT researchers, our award-winning solutions are proactive, automated, and easy to integrate - all with an unbelievably small footprint.

2.27.3 Links

<http://www.sensorhound.com/>

2.28 Shodan



The screenshot shows the Shodan website homepage. At the top, there is a navigation bar with links for 'Search', 'Developers', 'Monitor', and 'View All'. The main header features the Shodan logo and a search bar. Below the header, a large banner reads 'The search engine for the Internet of Things' and 'Shodan is the world's first search engine for Internet-connected devices.' There are two buttons: 'Create a Free Account' and 'Getting Started'. The main content area is divided into four sections: 'Explore the Internet of Things', 'Monitor Network Security', 'See the Big Picture', and 'Get a Competitive Advantage'. Each section has a small icon and a brief description. Below this, a blue banner highlights '81% of Fortune 100' and '1,000+ Universities'. The bottom section features a world map and the text 'Analyze the Internet in Seconds' with a 'Sample Report on Heartbleed' button.

2.28.1 Technology

- Google for exposed devices on the internet.
- Search results based on "banner grabbing" from open ports

2.28.2 Quotes

"Shodan is a search engine that lets the user find specific types of computers (webcams, routers, servers, etc.) connected to the internet using a variety of filters. Some have also described it as a search engine of service banners, which are metadata that the server sends back to the client. This can be information about the server software, what options the service supports, a welcome message or anything else that the client can find out before interacting with the server."

Unfortunately, there are no state secrets here and cyber criminals also make use of [Shodan.io](https://www.shodan.io) and CVE to find devices that are online and discover the vulnerabilities they can exploit by connecting to the device. Indeed, plans for a US Air Force drone were reportedly put up for sale on the dark web after hackers found vulnerabilities in the routers used by the military on [Shodan.io](https://www.shodan.io).

2.28.3 Links

<https://www.shodan.io/>

2.29 Snort



2.29.1 Technology

- Open source IDS/IPS developed by Cisco Talos
- Sniffs and logs network traffic
- Analyzes traffic and compares against ruleset (based on known vulnerabilities and exploits)
- Configurable actions based on what has been discovered

2.29.2 Quotes

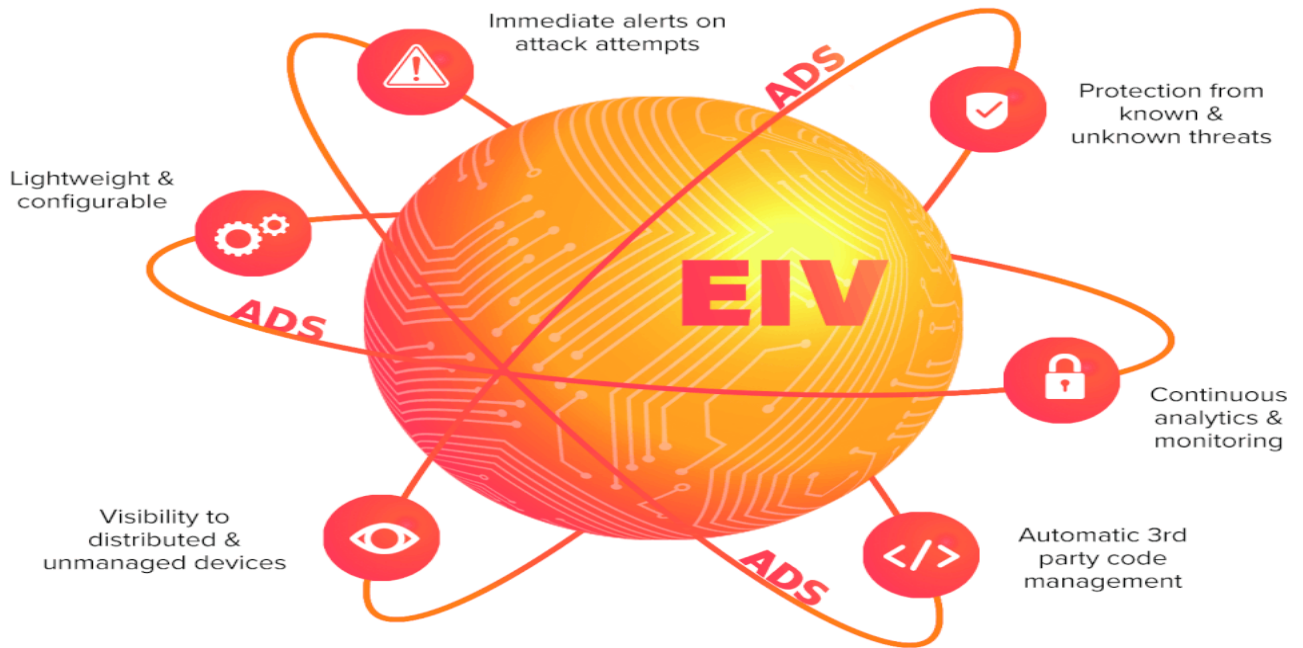
Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.

2.29.3 Links

<https://www.snort.org/>

2.30 Sternum



2.30.1 Technology

- Checks for security vulnerabilities during development/build
- On-device agent which monitors for exploitation attempts
- Online dashboard displays monitoring data from devices

2.30.2 Quotes

Sternum seamlessly embeds security into your embedded devices. With a new approach to IoT security, Sternum has built a holistic, highly scalable IoT endpoint security solution that prevents attacks in real time and provides ongoing visibility and monitoring of the device.

*Our innovative approach offers **agentless on-device protection** acceptable by any IoT device. Now the entire IoT value chain can benefit from scalable security and visibility from within the device with under 3% overhead and transparent integration. With the Sternum Suite **enterprises** can be immediately alerted of any cyber-attack attempt on their networks involving IoT devices, and manufacturers can offer managed and monitored IoT devices to their customers with built-in **real-time** security.*

Full support of linux-based devices as well as real-time operating systems, including FreeRTOS, SAFERTOS, ThreadX, Micrium, VxWorks & home-grown OS.

EIV is communication-protocol agnostic, supporting Wi-Fi, BT/BLE, Cellular and more.

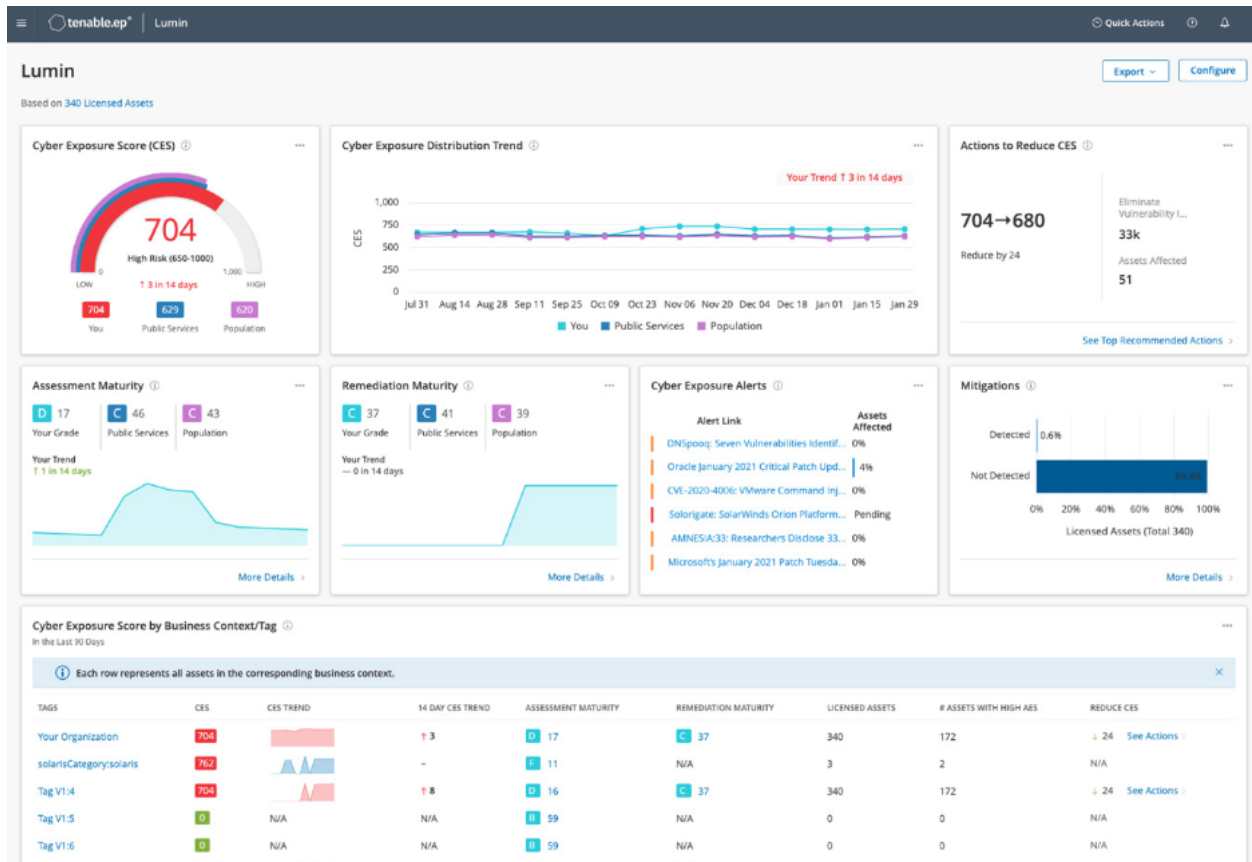
Supporting ARM-Thumb based micro-controllers (Cortex-M, Cortex-A, Cortex-R and more).

2.30.3 Links

<https://www.sternumiot.com/>

<https://www.sternumiot.com/sternum-suite>

2.31 Tenable (Nessus)



2.31.1 Technology

- Automatically discovers all assets on the network across different communication stacks
- Vulnerability scanner for all the whole network
- Comprehensive dashboard presents vulnerabilities and ranks them based on most likely to be exploited by an attacker

2.31.2 Quotes

Tenable.ep is a comprehensive risk-based vulnerability management solution that enables you to determine the cyber exposure of all of your assets, everywhere, on every platform, at all times. With Tenable.ep, you can see every asset and vulnerability across your entire attack surface, predict which vulnerabilities attackers are most likely to exploit in the near future and act on what matters most. It enables you to reduce the greatest amount of risk with the least amount of effort.

Tenable.ep is built on Nessus technology and leverages active scanners, web application scanners, agents, passive network monitoring, and cloud connectors to help maximize scan coverage across your infrastructure and reduce vulnerability blind spots. This mix of data sensor types helps you track and assess both known and unknown assets and their vulnerabilities, including hard-to-scan assets like laptops and sensitive systems like industrial control systems.

Tenable.ep prioritizes vulnerabilities based on the probability that they will be leveraged in an attack by combining over 150 data sources, including Tenable and third-party vulnerability and threat data. A proprietary machine learning algorithm is used to identify vulnerabilities with the highest likelihood of exploitability to help you focus first on the security issues that matter most to your organization.

Tenable.ot's automated asset discovery and visualization capabilities provide a comprehensive, up-to-date inventory of all assets, including workstations, servers, human machine interfaces (HMIs), historians, programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices (IEDs) and network devices. Tenable's patented active querying capabilities discover dormant devices that do not communicate over your network. The inventory contains unparalleled asset information depth—tracking firmware and OS versions, internal configurations, patch levels and users, as well as serial numbers and backplane configuration for both IT and OT assets.

2.31.3 Links

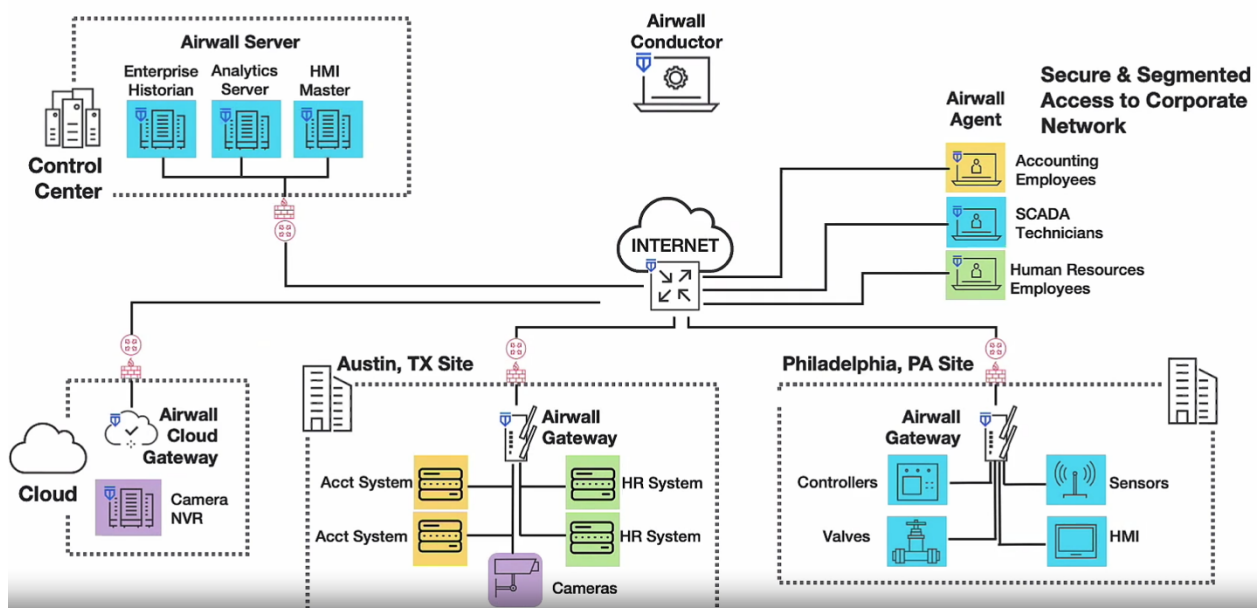
<https://www.tenable.com/>

<https://www.tenable.com/solutions/it-ot>

<https://static.tenable.com/marketing/datasheets/Datasheet-Tenable-ep.pdf>

2.32 Tempered Airwall

after deployment



2.32.1 Technology

- Software defined networks, control which devices can communicate with a simple GUI
- Zero Trust Networking

- Network Micro Segmentation
- Remote access to devices - not whole networks
- Devices need either agent program installed, or hardware gateway in network (masquerading as default gateway)

2.32.2 Quotes

Tempered Airwall restores a logical air gap by making networks invisible. So what does that actually mean? Well, it means Airwall:

- *is a zero trust network access solution that securely connects things at Layer Three.*
- *creates an overlay network over your existing underlay network with minor, if any, modifications to the underlay.*
- *handles communications with remote trusted devices through authenticated encrypted tunnels.*
- *can segment zones of devices behind Airwall Gateways in different isolated port groups.*

How does Airwall Teams differ from Airwall?

Airwall Teams implements only the basics of Airwall's secure networking technologies. The Airwall Zero-Trust solution is designed to meet the needs of the largest enterprise and industrial customers as they move to more secure, connected architectures. Key additional features include:

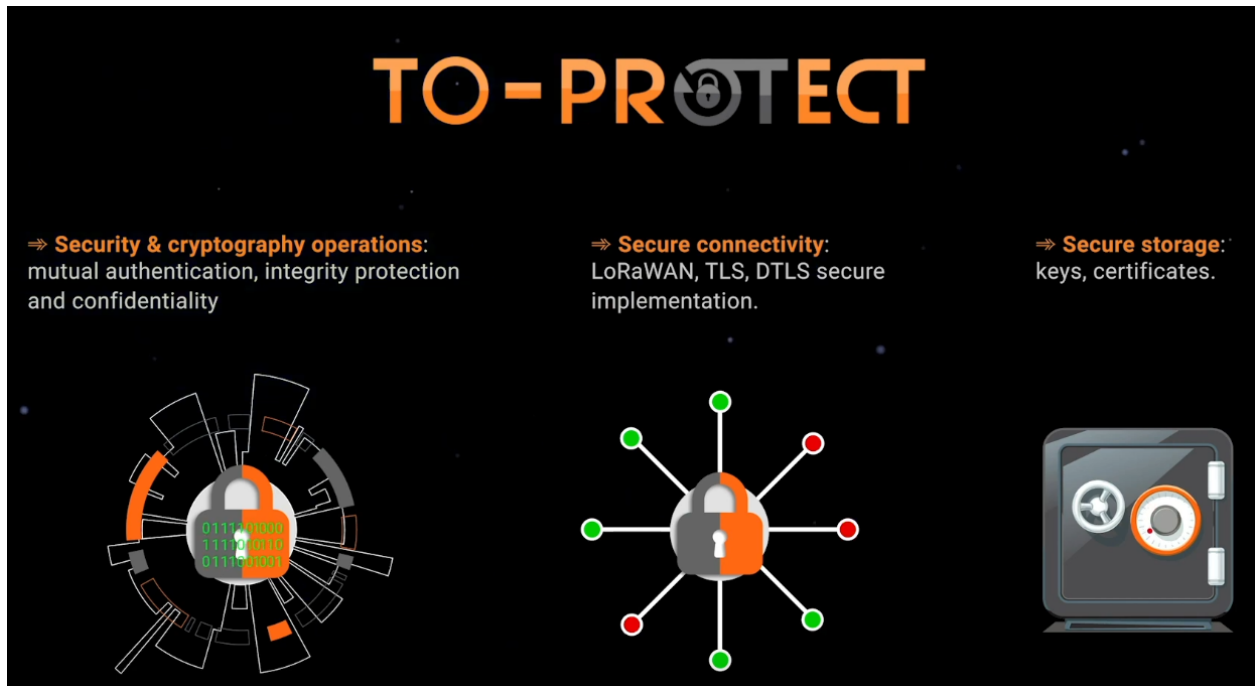
- **Add networks, not just devices, to the private network with virtual or physical gateways. This lets you protect IoT devices and other dedicated systems that can't have agents installed on them.**
- *Strong user authentication of all users via AD and OpenID, in addition to Airwall Teams device identification technology*
- *Easy segmentation of users and devices – realize least privileged access quickly to reduce your attack surface and increase information security*
- *"Cloaking" technology makes devices invisible to hackers*
- *A full-featured API for provisioning and deployment of all aspects of the solution*
- *Enterprise-grade configuration and management features*

2.32.3 Links

<https://www.tempered.io/>

<https://discover.tempered.io/webinars/what-is-airwall>

2.33 TrustedObjects



2.33.1 Technology

- Library for root-of-trust, side channel attack protection, etc.
- Support for SecureElement-chips to secure important assets (cryptographic keys, financial data, etc).

2.33.2 Quotes

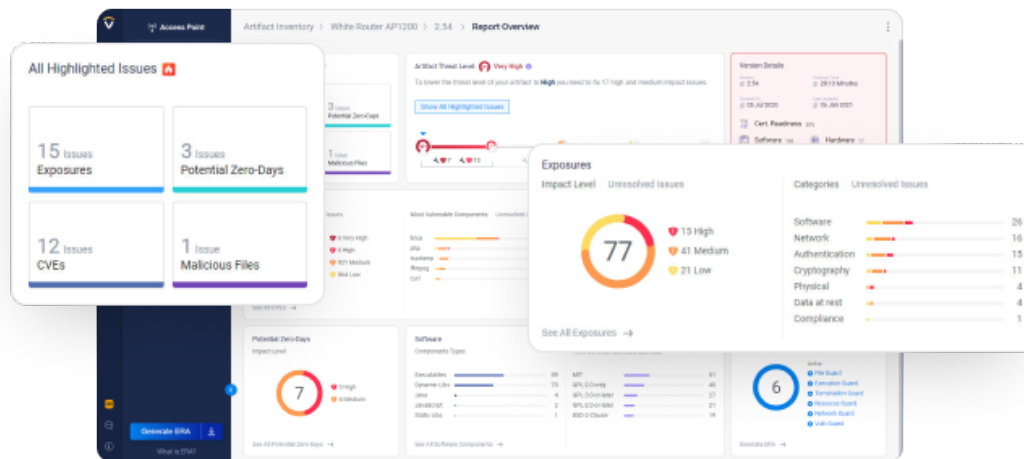
to-protect offers many benefits:

- *Easy to integrate on-device Root-of-Trust*
- *Prevention against logical and physical security attacks on IoT devices exposed to threats*
- *Fully integrated in several IoT chains to achieve a Chain of Trust*
- *Reference design already qualified*
- *Compatible with existing hardware (no redesign / no impact on the BOM)*
- *Easy security retrofit for devices already in the field with MCU FUOTA (Firmware-Update-Over-The-Air).*

2.33.3 Links

<https://www.trusted-objects.com/>

2.34 Vdoo



2.34.1 Technology

- Security tools for embedded product developers
- Image scanner to look for vulnerabilities just by analyzing binaries
- Runtime threat-protection agent which is generated for product

2.34.2 Quotes

Get all the information you need to quickly and efficiently achieve optimal security for the connected products you bring to market. Vdoo’s automated platform combines software composition analysis, deep static and dynamic security analysis, and device-aware vulnerability assessment in a single solution. It inspects your devices’ binary images to deliver comprehensive insights based on the entire device context – including CVEs and other known vulnerabilities, hardening and configuration issues, and potential zero-days in internally developed or third-party software – without requiring access to their source code.

Vdoo’s device security focused expertise and tools enable everyone to resolve security gaps, even developers who are not security experts.

- Simple-to-understand background information on issues including their potential impact and how attackers may exploit them
- Clear step-by-step vulnerability remediation instructions
- Contextual information including specific references to relevant findings in the code

Implement an efficient solution to quickly address a range of known and unknown threats.

- Easily integrate an independent and easy-to-deploy agent to mitigate new threats, postponing complex patches or upgrades and achieving long-term protection even on legacy devices
- Quickly detect and respond to attack attempts with real-time security alerts and active exploit prevention mechanisms
- Generate the agent in one click, based on full analysis of the device’s attributes and configuration, with easily configurable security policies

2.34.3 Links

<https://www.vdoo.com/>

<https://www.vdoo.com/security-analysis>

2.35 Zeek (formerly Bro)



2.35.1 Technology

- Open source network analysis framework
- Captures packets and runs them through an event engine, creating compact transaction logs
- Output is intended for later review in other tools

2.35.2 Quotes

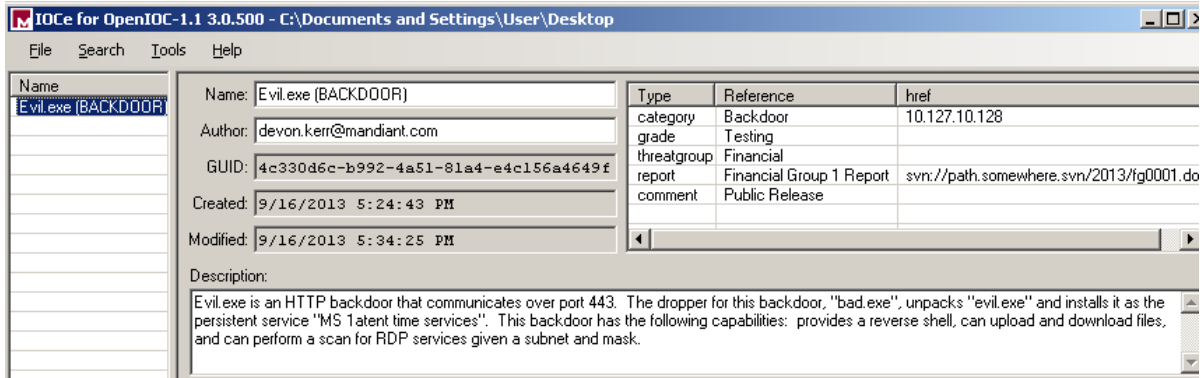
Zeek is not an active security device, like a firewall or intrusion prevention system. Rather, Zeek sits on a “sensor,” a hardware, software, virtual, or cloud platform that quietly and unobtrusively observes network traffic. Zeek interprets what it sees and creates compact, high-fidelity transaction logs, file content, and fully customized output, suitable for manual review on disk or in a more analyst-friendly tool like a security and information event management (SIEM) system.

2.35.3 Links

<https://zeek.org/>

3 OTHER INTERESTING PROJECTS

3.1 OpenIOC



3.1.1 Technology

- Format for tagging IOC.

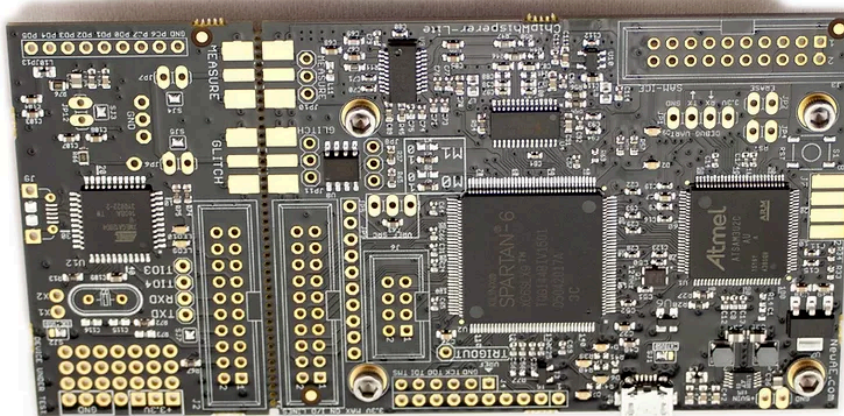
3.1.2 Quotes

One challenge investigators face during incident response is finding a way to organize information about an attackers' activity, utilities, malware and other indicators of compromise, called IOCs. The OpenIOC format addresses this challenge head-on. OpenIOC provides a standard format and terms for describing the artifacts encountered during the course of an investigation.

3.1.3 Links

<https://www.fireeye.com/blog/threat-research/2013/10/openioc-basics.html>

3.2 ChipWhisperer



3.2.1 Technology

- Open-source toolkit to perform side-channel attacks.

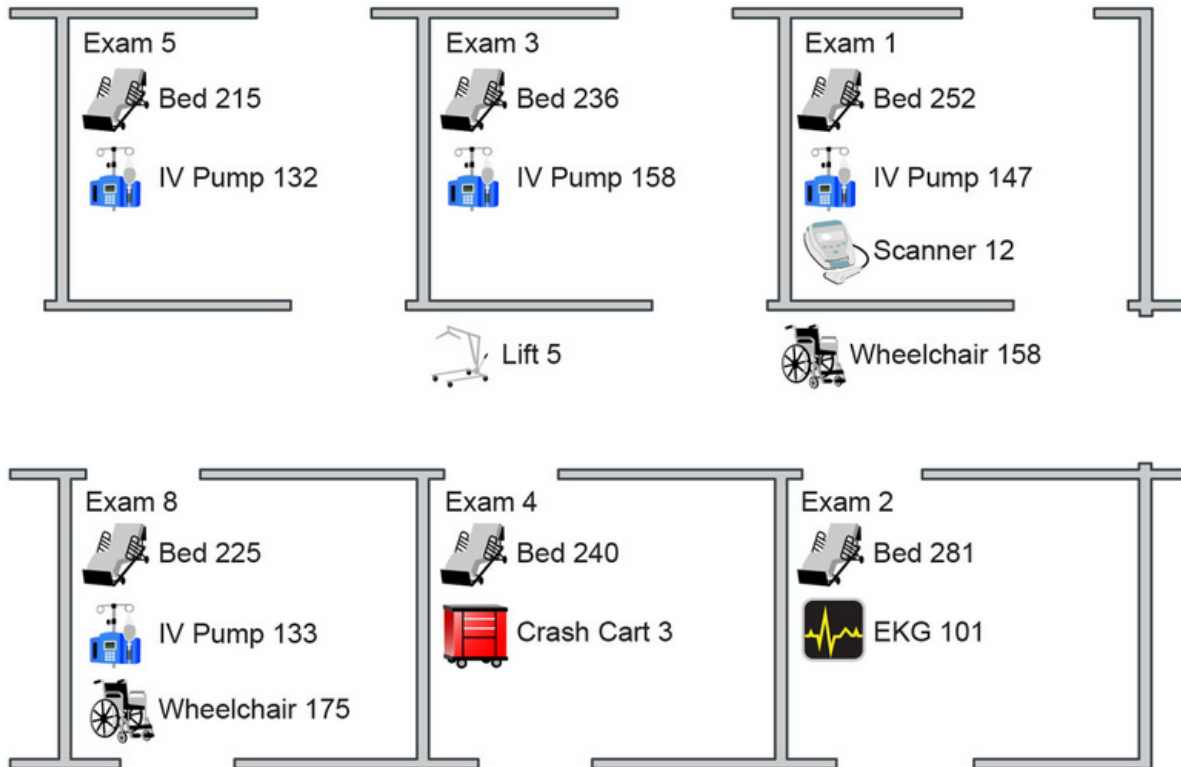
3.2.2 Quotes

The ChipWhisperer® ecosystem presents the first open-source, low-cost solution to expose weaknesses that exist in embedded systems all around us.

3.2.3 Links

<https://www.newae.com/chipwhisperer>

3.3 Midmark RTLS



3.3.1 Technology

- Asset and people tracking (for hospitals) by putting one small sensor in each room
- Every tracked object/person has a battery powered tag (18-24 months battery life)
- Three options on infrastructure; wired, ANT, WiFi

3.3.2 Quotes

With RTLS, staff no longer spend time searching for equipment - instead, they use that time to provide direct patient care, to efficiently maintain assets for safer patient care, or to perform other value added tasks.

In areas where the precise location of equipment is necessary (e.g., patient rooms or supply closets for PAR-level alerting), install infrared (IR) sensors, available in both wired or battery-powered options.

3.3.3 Links

<https://www.midmark.com/medical/products/rtls>

<https://www.midmark.com/medical/products/rtls/rtls-detail/sensory-network>

<https://centrak.com/2021-gartner-magic-quadrant/> ← More actors in this market
