aeris

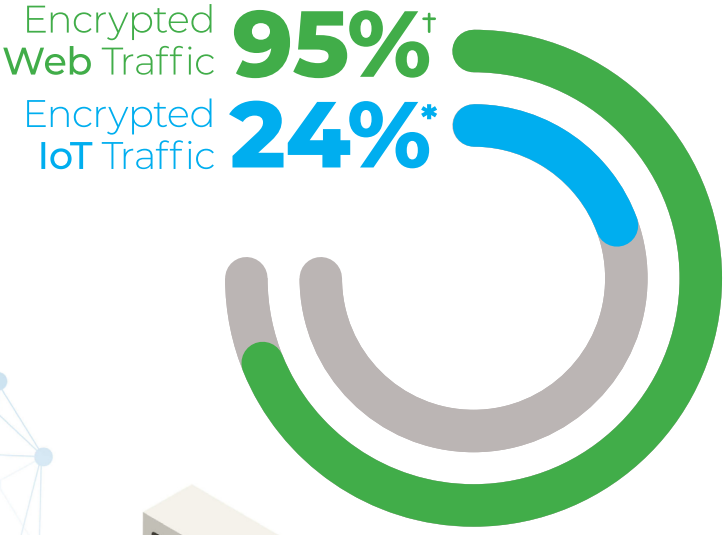
Solving Cellular IoT Security Challenges with an Intelligent Network

IoT Security Guide

It is a hyperconnected world we live in today. From homes to the office, from indoors to outdoors, on land, in air and sea, there is a growing number of internet of things (IoT) devices that are connected through wired or wireless technologies. Whether they are personal devices like smart phones, stationary devices like smart street lights, or mobile units like automotive vehicles or freight trucks, the growing adoption of IoT devices is rapidly changing how we live. They have broad capabilities with real-world benefits to make our lives better, more enjoyable, safer, or more productive.

The power of IoT is reflected in our economic realities. A 2021 McKinsey and Company study[1] found that by 2030, IoT devices could enable $5.5 trillion to $12.6 trillion in value globally, including the value captured by consumers and customers of IoT products and services. Moreover, according to IoT Analytics,[2] IoT spending is projected to grow at 26.7% annually beyond 2021.

Yet these growing potentials carry hidden risks. Alongside the economic and social advancements is a brewing storm of security threats that must not be overlooked. While businesses are racing to incorporate IoT devices and developing their own products/solutions, extra care and an equal investment in time and resources must be made to ensure the benefits are not encumbered by potential security threats.



What Make IoT Devices Vulnerable?

Simply put, if something can be attacked, it will be—especially if it is accessible over the internet. The escalating frequency and severity of security threats have undoubtedly increased the market awareness of this sobering reality. With IoT devices in particular, there are unique characteristics that make them even more vulnerable than IT end devices like computers, tablets, or smartphones.

Scale

The sheer volume of devices in an IoT network makes them an attractive target. According to IoT Analytics[3] the total number of connected IoT devices is estimated to grow from 12.3 billion today to 27 billion by 2025. As the idiom goes, a chain is only as strong as its weakest link; from an attacker's point-of-view, it only takes one compromised IoT device to get into the IT/OT network and wreak havoc.

Resource-constraints

A vast majority of IoT devices are typically resource constrained, which makes it hard to implement traditional security countermeasures like agents, or conduct regular vulnerability assessments. Sometimes even a scan of open ports may "brick" a device and render it unusable.

Accessibility

By definition, IoT devices are internet accessible, which could make them easy to reach if there is no robust security in place. These devices are typically not behind corporate firewalls like IT/OT equipment. In other cases, IoT devices are deployed in remote locations with very little oversight, which makes them easier to be physically compromised (e.g., SIM card theft).

Longevity

The lifecycle of some of IoT devices can be surprisingly long, depending on their applications. Attila Security found that some devices may last as long as two decades or more in the field. As these deployments age, security maintenance becomes increasingly complex. When security firmware updates come out for newer devices, these older devices may not be supported. As an example, Cisco reported that 60% of medical IoT devices today are already at their end-of-life stage.

Variety

Given the strong appeal of IoT devices and their benefits—more customer insights, better efficiencies, reduced OPEX—business interests are taking priority over the heightened security risks that businesses are willing to assume. Proliferation of IoT devices that businesses have adopted to serve the needs of their employees, as well as those they developed to serve the needs of their customers, leads to a greater attack surface because of the wide variety of these devices. To protect them all from malicious actors can be daunting.

Why Are IoT Devices Under Attack

Regardless of the types of cyberattacks—malware, ransomware, distributed denial of service (DDoS), zero-day, or SQL injection, just to name a few—malicious actors typically have one or more of the following in mind:

Data

This can be financial data, intellectual property, strategic plans, customer information, etc. IoT devices can be used to breach the victim's network, pivot to data sources that hold sensitive information, and then leak or exfiltrate this data to malicious actors.

Money

Ransomware, where the victim's devices are locked/encrypted unless they pay a ransom to the attacker, has become one of the most common security threats because of the immediate financial gains. Another variant to this attack vector is Doxware, where the attacker threatens to publish release confidential/sensitive data to the public if the victim does not pay the ransom. IoT devices can hold important, sensitive data that businesses do not want to lose or expose to the public.

Resources

While IoT devices are typically resource-constrained, the sheer scale of IoT deployments makes them attractive to bad actors, because a compromised IoT deployment can be repurposed (or "hijacked") to launch coordinated attacks on other entities. Unlike typical attacks that have one or few sources, an IoT attack will involve hundreds or even thousands of devices. This sheer volume makes it extremely hard to stop the attack (sometimes referred to as Distributed Denial of Service or DDoS). These IoT devices, once coopted by a hacker to become part of a botnet of networked things, are sometimes referred to as a ThingBot.

Sabotage

As many mission critical systems become internet enabled (e.g., smart grids, industrial control systems, weather monitoring stations, to name a few), a compromise in these systems can have a very disruptive impact. This is especially attractive to sophisticated bad actors, typically nation-states looking to cripple their intended target(s) via cyberwarfare. The 2016 attack on Ukraine's power grid showed just how real and devastating this attack vector can be.

For 2021, there are alarming data points that make a compelling case to designate securing IoT deployments a top priority:

Kaspersky[4]

A well-respected cybersecurity vendor with deep experience in threat intelligence, saw 1.5 billion attacks against IoT devices in the first half of 2021, up from 639 million during the last 6 months of 2020. This is an astonishing increase of 240%. It may not come as a surprise that Kaspersky also found that an IoT device could be probed for exposed services in as little as 5 minutes[5], after it comes online for the first time.

1.5 Billion Attacks

700% increase

ZScaler[6]

A cloud security company with customers worldwide, detected a 700% year-over-year increase in IoT malware on corporate networks. Just as alarmingly they found that 76% of IoT communications were occurring on unencrypted, plain-text channels.

$4.24 million

IBM[7]

They have found that the average cost of a data breach in 2021 has risen to $4.24 million. For the United States, this number actually is more than $9 million.

The sobering reality is that any IoT device will get discovered and targeted by malicious actors eventually. And the resulting financial impact of a successful attack is in millions of dollars.

Issues with Current IoT Cybersecurity Approach

Given the unique characteristics of IoT devices that make them vulnerable, traditional security approaches, which are more IT-centric, are not enough. For IoT devices that rely on cellular connectivity in particular, having an up-to-date and effective security posture can be daunting. Even the often touted "secure by design" principle, which requires security to be baked into the IoT device at inception, may require considerable logistical planning and human resources. Let's examine specific scenarios where traditional security approaches are not well-suited for cellular IoT devices.

Scale & Accessibility

The sheer number of IoT devices, and the locations where they are deployed, make it extremely difficult for traditional security approaches to be as successful. For example, in some cases it may be challenging to reach all IoT devices due to connectivity issues. When the number of devices is in the hundreds and thousands, and if they are not in the same cellular network, the challenge to synchronize security patch management can be even more daunting.

Resources

Even if a customer can reliably get to all of their IoT devices, the limited computing power on these devices can make it impractical to run traditional security countermeasures like agents or penetration tests. As such, continuous, on-device security maybe infeasible.

Device lifetimes

The majority of IT network applications and endpoint devices are easily reached and have well-defined patch and maintenance schedules. In contrast, IoT devices can be widely dispersed around the world and have very long lifetimes. In the event of an unforeseen vulnerability discovered after the IoT devices have left the factory, sometimes referred to as a "zero-day" attack, it is extremely difficult to patch the hardware or firmware long after IoT devices have been deployed.

Heterogeneity

IoT deployments may consist of many types of devices from different vendors. Rather than treating all devices the same way as a traditional IT security strategy is designed to do, it is safer to adopt a different approach where IoT networks are segmented from other networks. Even with a single type of IoT device, the hardware, firmware, and application may originate from different vendors, which makes identifying threats and vulnerabilities across all three very challenging.

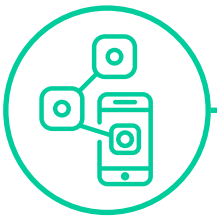
Based on these scenarios, it is clear there are challenges when it comes to securing IoT devices. Spotting a breach in the security posture is like trying to find the proverbial needle-in-a-haystack. It can be a daunting process when businesses have to assimilate and correlate security signals across multiple devices. Equally important is the speed at which a security incident can be identified and mitigated.

Four Aspects of Cybersecurity

Given the challenges and complexities of securing cellular IoT devices, it is important to take a holistic approach to ensure a robust security posture end-to-end. There are four aspects of protection that businesses should consider implementing—device, application, data, network. Each plays a key role in the Defense in Depth strategy advocated by security practitioners, and they must work together seamlessly.

DEVICE

For IoT devices, the most common methods utilized for increasing security at the device level are non-removable SIMs, limited physical connections (via USB port for example) to external devices, and controlled access through the use of cards, keys, or biometrics (e.g., fingerprint readers). Tamper-resistant packaging is another way to limit unauthorized device access. Finally, the root of trust is another key security measure. A hardware-based root of trust permits cryptographic functions and allows booting only with code from a trusted source.



APPLICATION

For application security, there are measures to prevent data or code within the app from being stolen or hijacked. In addition to considerations that occur during application development and design, application security also involves approaches to protect applications after they are deployed. For instance, hardened configuration, including ports for inbound and outbound communications, as well as limiting privileged access can be implemented to ensure secure over-the-air (OTA) updates.

DATA

While device and application security account for the endpoints in an IoT network, it is ultimately the data that is being generated, transferred, and processed that vendors, operators, customers, and even malicious actors are primarily focused on protecting or attacking. Given the wide range of applicability of IoT systems today, from healthcare to fleet management and mission critical utilities, it stands to reason that there is a lot of scrutiny on how sensitive data is secured.

For tightly regulated market segments like healthcare (e.g., Health Insurance Portability and Accountability Act or HIPAA) and financial services (e.g., Payment Card Industry Data Security Standard or PCI/DSS), the impact of a data breach can be enormous. It is paramount to ensure data stays encrypted – both at rest and in motion. In addition, data sovereignty is also a concern; data generated in one region should not be accessible from other regions. This becomes a challenge in the context of mobile IoT devices. Strong security controls are needed to ensure that data can only be accessed by authorized entities in authorized domains.

NETWORK

While network security has traditionally been considered an important component of a Defense in Depth strategy, it is mostly an afterthought for businesses that rely on cellular connectivity for their IoT devices. This is because cellular networks are typically considered a "black box" for many.

What they are missing out on are the unique advantages that network security has to offer—continuous non-intrusive monitoring, behavioral analysis, and the ability to detect offline devices or rogue actors. While a virtual private network (VPN) and access point name (APN) help to improve cellular IoT security, relying on them alone is not enough. Also, encryption of IoT communications is typically implemented at the application layer. While encryption of IoT communications is typically implemented at the application layer, network-based monitoring can verify that communications are actually happening over encrypted channels.

Governments Around the World Are Taking Action to Safeguard Cybersecurity

Given the alarming growth in frequency of ransomware attacks and security breaches, and the disruptive impact it can have on our financial, healthcare, and utility systems, governments around the world have stepped up their efforts to establish regulatory frameworks to safeguard the public interest. In the United States, the IoT Cybersecurity Improvement Act is a legislation that directs the U.S. National Institute of Standards and Technology (NIST) to create minimum cybersecurity standards for IoT devices owned or controlled by the U.S. government. While regulations are slowly emerging as the IoT industry matures, there is still a need for established security practices like the national vulnerability database (NVD) for common vulnerabilities and exposures (CVEs).

In Europe, the European Telecommunications Standards Institute (ETSI) is the standards organization that sets the regional standards for telecommunications, broadcasting and other electronic communications networks and services. Its IoT security standard lists 13 provisions for device security and five for data protection. The United Kingdom has also introduced the Product Security and Telecommunications Infrastructure (PSTI) bill which promises to protect IoT device stakeholders.

In Asia, South Korea has the National Security Council (NSC) that reports directly to the president. It helps coordinate cybersecurity at the national level to ensure stable operations of the state and build a strong cybersecurity foundation.

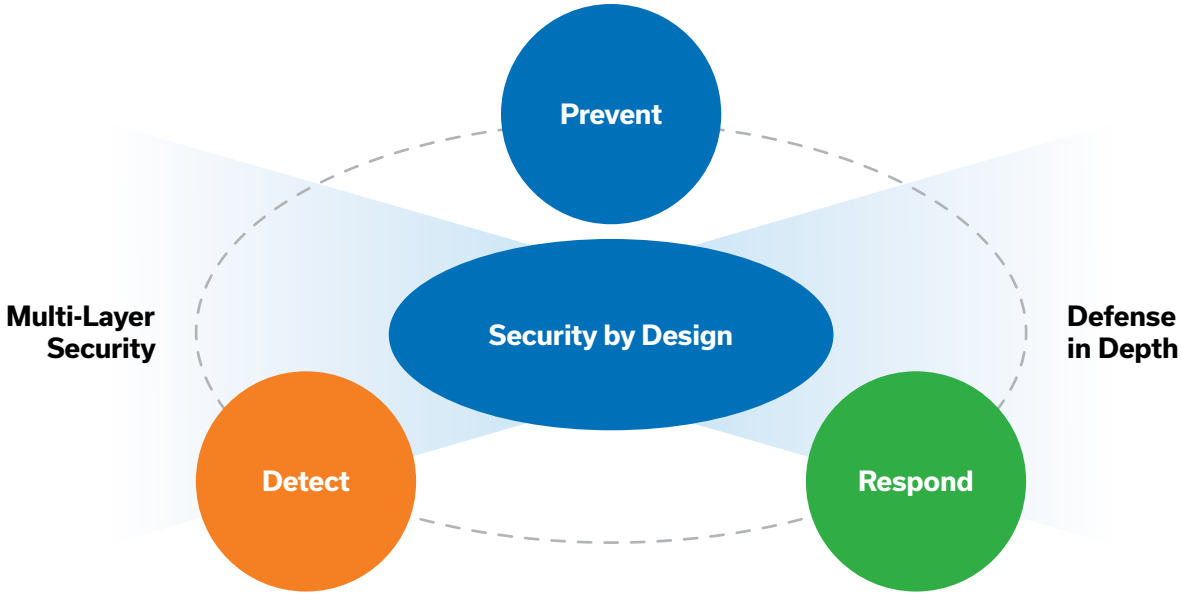
Secure by Design for IoT Through Prevent, Detect, Respond

In spite of these government-led legislations and agencies, cybersecurity attacks and ransomware continue to become headline news. Secure by Design is a cybersecurity approach that can help to lessen these threats. The idea is to start with a robust architecture design at the onset and incorporate security measures at the device, application, data, and especially network level. This approach complements the Defense in Depth strategy in which multiple layers of security measures are used throughout the security architecture to provide redundancy. The end-goal is to ensure that when one of the security measures fails or a vulnerability is exploited, it is quickly discovered and addressed with minimal service disruption or customer impact.

Through Aeris, Security by Design for IoT devices can be achieved using our new features that are designed to prevent, detect, and respond to vulnerabilities and cybersecurity threats.

"Prevention, detection, and response are essential. Prevent by making sure you have implemented security by design. Detect by working with companies like ours, who have all of the tools and the monitoring functions needed to track these devices and help you determine what devices might have been breached. Then respond to them by blocking the bad devices and the bad data."

— Syed "Z" Hosain
Chief Technology Officer, Aeris



Prevent

Aeris Intelligent Security Features	Objectives	Outcome
1. Private Domain Name Server (DNS) 2. Aeris ConnectionLock 3. Access point name (APN) 4. Non-dialable numbers 5. SMS & AccountLock 6. Cloud Connect 7. Dynamic/static IP address 8. Virtual Private Network (VPN)	1. Prevent unauthorized actors or services from accessing the network (while also detecting shadow IoT). 2. Encrypt data on the network, both in-transit and at-rest, to ensure integrity and prevent theft or leakage. 3. Minimize risk posed by exposure to public DNS servers.	1. Devices are only allowed to interact with authorized servers and endpoints on the network. 2. Devices are properly segmented and isolated to their designated networks. 3. Devices can adhere to best practices like secure by design.

Detect

Aeris Intelligent Security Features	Objectives	Outcome
1. Indicators of Compromise (IOCs) 2. Security Risk Score (SRS)	1. Minimize manual efforts, time, and resources to identify issues. 2. Highlight potential security vulnerabilities and incidents at IoT scale and speed of deployment. 3. Expand security awareness, inform on best practices, and make key security indicators more accessible.	1. Detects traffic anomalies and security threats immediately. 2. Strengthens the overall security level. 3. Lowers the amount of internal security resources and allocates resources to address other business needs.

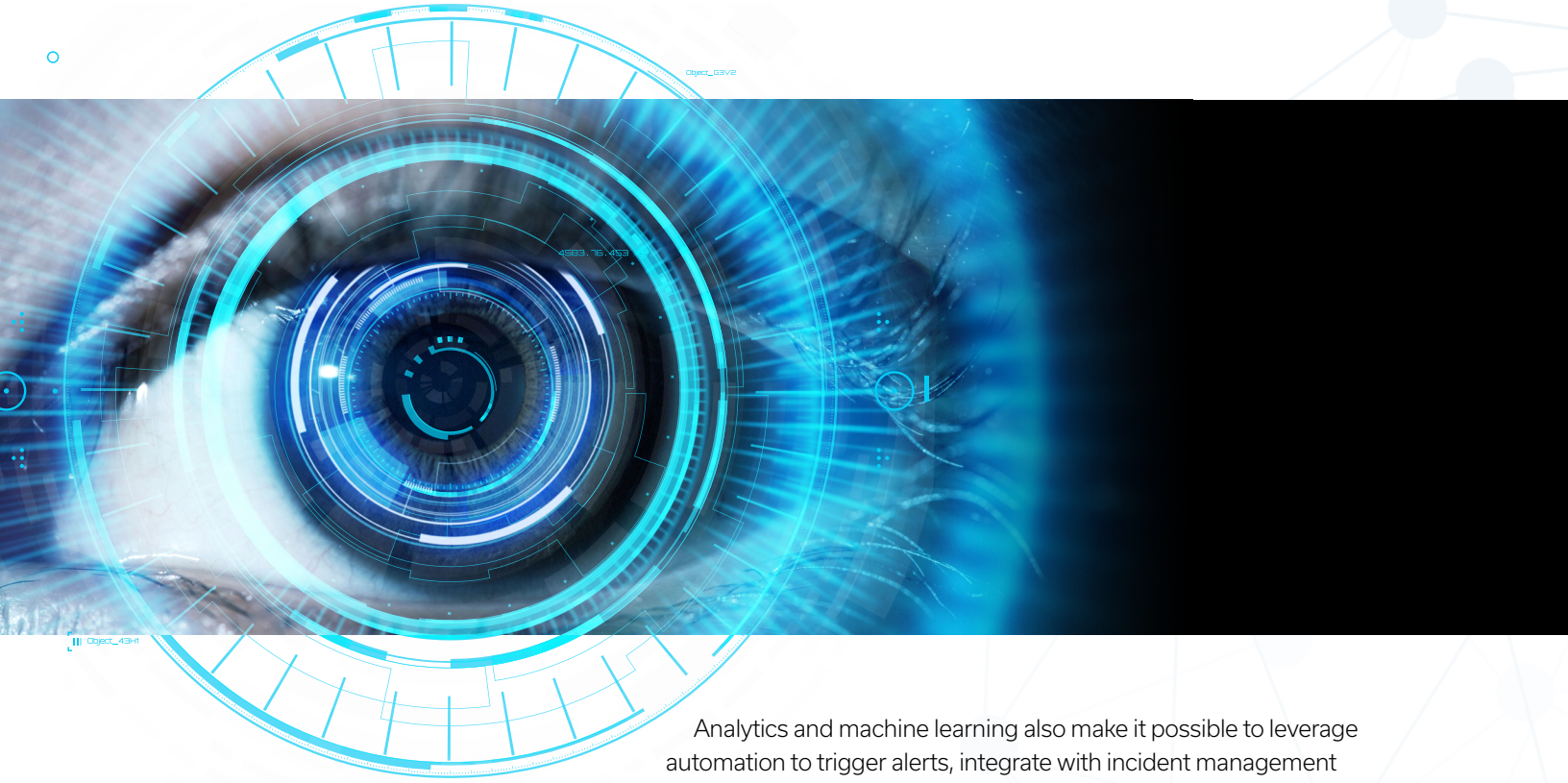
Respond

Aeris Intelligent Security Features	Objectives	Outcome
1. Deep forensics 2. Block traffic to/from compromised devices	1. Triage and validate potential anomalies and security issues. 2. Alert on confirmed incidents or threats. 3. Block or suspend traffic to impacted devices.	1. Detects SIM theft incidents. 2. Prevents data overage charges. 3. Responds rapidly to isolate vulnerable or compromised devices.

Aeris Delivers More Visibility & Insights

Attacks don't happen overnight. They come in waves. Some of the most sophisticated APTs (advanced persistent threats) have attackers covering their tracks, waiting patiently for months or even years, before launching a coordinated attack. With IoT, this is especially relevant because compromising a single device is sometimes not enough to get to what the attacker is after.

The Aeris Intelligent Security Center, or AISC, is a new class of IoT security solution that leverages network intelligence and machine-learning technology to improve the effectiveness of cybersecurity for IoT devices. By seamlessly combining near-real-time and historical data, we enable advanced, deep forensic analysis that customers can use in their investigative workflows to quickly identify and rapidly respond to potential security incidents. This is especially important for IoT deployments where the scale and distribution of devices render traditional techniques ineffective.



Analytics and machine learning also make it possible to leverage automation to trigger alerts, integrate with incident management systems, and expedite issue resolution. By pinpointing potential problems, offering guidance, and suggesting areas that need additional investigation, we make it easier for customers to detect, and potentially prevent, vulnerabilities and exploits.

What AISC provides is a set of metrics: Indicators of Compromise (IOCs), a Security Risk Score (SRS), and device-level forensics. They are key forensic evidence that can help businesses detect malicious activity at both the network level and the individual device level. It synthesizes various network traffic data by aggregating it and normalizing it over time. It also incorporates a dynamic scoring algorithm to evaluate IoT traffic against recommended security controls and best practices, thereby enabling your organization to stay ahead of the evolving threatscape. The application of machine learning, coupled with the highly sophisticated network intelligence of the Aeris IoT network, further enables your organization to quickly identify and take action on network anomalies and potential security risks.

Indicators of Compromise (IOCs)

The first line of defense for IoT security should be visibility. The IOCs from Aeris enable information security (InfoSec) and IT professionals to detect data breaches, malware infections, or other threat activity. Four specific metrics are chosen because they are highly useful early indicators of potential device compromise. They enable you to track activity, establish baselines, highlight anomalies, and conduct deep forensics.

Data Transactions

This is a traffic summary report on the average amount of data that is sent/received to/from each device per transaction. This is an important metric to track, as a spike could imply data overage charges and adversely impact the cost of operations. Additionally, it may also signal a potential data breach, where malicious actors are exfiltrating sensitive data out through IoT devices.

DNS Queries

Domain Name System (DNS) servers are used by IoT devices to route outbound communication to the appropriate destination endpoint. DNS traffic monitoring allows you to analyze how much of the IoT device traffic flows through open versus closed systems, to understand how IoT deployment has been configured, and to spot anomalies. A higher than expected query count could signal a DDoS attack, which can have bigger ramifications on your network.

Destination Endpoints

Endpoints are sources/destinations of transmission activity within your IoT networks. While many IoT networks adhere to a hub/spoke (sometimes referred to as a star) architecture, other models like a mesh network where IoT devices can talk to each other are also becoming prevalent. Monitoring the source/destination IPs contacted by an IoT network can be a powerful tool to detect malicious activity like pivoting attacks or device hijacking (for botnet attacks).

Data Volume

This is a security control that gives you early warnings about potential data breaches by monitoring outbound data transmission activity. It allows you to track the volume of data that gets sent out, drill down into the specifics of which devices are sending this data, and where the data is being sent.

Security Risk Score (SRS)

Aeris helps customers quantify their IoT risks proactively through a dynamic scoring algorithm to evaluate their deployment against recommended security controls and best practices, continually keeping up with the evolving threatscape.

The Aeris Security Risk Score (SRS) is the quantified output of a risk assessment model that accurately tracks the relative security of a customer's IoT deployment. The score is a percentile ranking that incorporates multiple threat vectors and provides security teams with an intuitive and interactive view into their IoT deployment's risk posture.

Device-Level Forensics

Once a potential compromise has been identified through one of these four IoCs, you can drill down further using a variety of options through ASIC:

- ***By Time (specific days)***
- ***By Source/Destination URLs (for where data is being transmitted)***
- ***By Device ID (to isolate specific devices for remediation)***

AISC enables the selection of each of the three options above to aid the triage and root-cause analysis of security incidents involving IoT devices. These incidents are typically large and distributed in nature, so it's important to gain network-level visibility to better detect any anomality or potential threat.

What Sets the Aeris Security Solution Apart

For businesses that have begun the internal assessment and are searching for effective tools to beef up their IoT security, consider the two unique AISC capabilities that set it apart from other IoT security options:

1. The ability to monitor traffic at the network layer and establish normal/baseline behavior.

Traditional approaches to detecting and remediating device issues require either an agent-based approach, which is hard to manage and expensive to implement, or an agentless approach which requires the ability to connect out to each device. Neither of these approaches work well, especially with the scale and distributed nature of IoT deployments. Even the "snap-and-tap" flow monitoring solutions that are modified for IoT networks add extra complexity and require significant integration efforts for deployment and maintenance.

In contrast, what makes AISC unique is that this approach is seamless and can be easily layered on top of a business' IoT network well after the initial deployment. Nor does it require labor intensive device reconfiguration, because all the security forensic tools are integrated with the Aeris intelligent IoT network management platform. This makes it easier and faster for businesses to implement their Defense in Depth for IoT deployment.

2. The ability to immediately respond to a security incident by blocking data transmission, at the device or to/from a network address.

Instead of flagging compromised IoT device(s), you can actually close the loop by taking the compromised device(s) out of the network. Not only does AISC enable you to take rapid, near real-time action in the event of a security incident, it also offers automation capabilities, which makes it easy to seamlessly integrate AISC with your organization's existing security workflows.

"Network detection and response must be considered a critical component of IoT security, especially because it can significantly reduce the time to detect breaches and respond to incidents — from months to minutes."

— Hari Nair

Senior Director of Product Management, Aeris

Ultimately, network-based detection and response capabilities should be considered as part of your organization's security toolchain. By combining key metrics on security threats, easy-to-understand metrics about the overall security risk, deep forensic capabilities, and cutting-edge machine learning technology, AISC improves the effectiveness of your security strategy. It can also be cost-effectively, seamlessly, and quickly integrated with other network security tools your organization has already deployed.

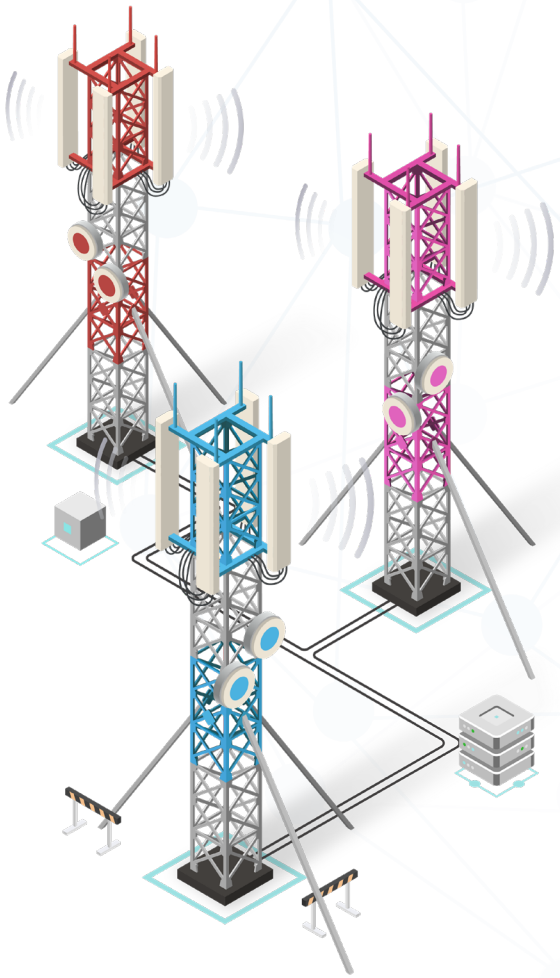
Why Choose Aeris as Your Cellular IoT Connectivity Provider

Given the growing scale and complexity of IoT deployments, basic visibility into network traffic is no longer sufficient. Being able to analyze and distill growing reams of data, and turning that into specific insights, is essential for businesses to focus more time and effort on value-creation activities that benefit their businesses and serve their customers.

For many years, Aeris has been recognized in the Gartner Magic Quadrant Report as a visionary for cellular IoT connectivity solutions. By leveraging nearly three decades of IoT knowledge and experience, we empower businesses by delivering intelligent IoT cellular connectivity, security, reliability, and support that simplifies and streamlines IoT programs at the best value, at scale.

To enhance IoT security, Aeris AISC is a new class of agentless security solution. It offers a comprehensive set of features that augment your current security strategy and can vastly improve your ability to identify and mitigate security threats. Key features such as IOCs and SRS provide your business with greater visibility and insight into your IoT network activity using threat intelligence. They also help businesses quantify security risks by continually evaluating IoT deployments against recommended security controls and best practices, which enables your business to stay ahead of the evolving threatscape.

Through the use of machine-learning technology, Aeris can help businesses greatly simplify and accelerate the detection of IoT traffic anomalies and emerging security threats. Adoption of this technology is essential for successful IoT programs, considering the challenges of manually identifying security threats, the expanding scale of deployments, and the amount of data that is generated. Machine learning coupled with network intelligence helps businesses develop a new baseline as their IoT use cases become more diverse and complex, and as they cover wider geographies.



For 30 years, Aeris has successfully positioned itself as a trusted business partner to organizations around the globe that launch and scale IoT programs. With the introduction of AISC, this new class of agentless IoT security solution can help businesses quickly and cost-effectively implement all facets of the prevent, detect, and respond framework. Please contact us for a demo of AISC, and see for yourself how it can help improve your business' IoT security posture.

Source Materials

* Gandhi, Viral. "IoT in the Enterprise Report: Empty Office Edition" [2021 Report]. Zscaler; ThreatLabZ. July 15, 2021. https://www.zscaler.com/press/zscaler-study-confirms-iot-devices-major-source-security-compromise-reinforces-need-zero

† Google Transparency Report. "HTTPS encryption on the web." Google.com. January 2022. https://transparencyreport.google.com/https/overview?hl=en)_

1. Chui, Michael; Collins, Mark; & Patel, Mark. "IoT value set to accelerate through 2030: Where and how to capture it." McKinsey Digital. November 9, 2021. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it

2. Wegner, P. "Global IoT spending to grow 24% in 2021, led by investments in IoT software and IoT security." IoT Analytics. June 16, 2021. https://iot-analytics.com/2021-global-iot-spending-grow-24-percent

3. Sinha, Satyajit. "State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion." IoT Analytics. September 22, 2021. https://iot-analytics.com/number-connected-iot-devices

4. Cyrus, Callum. "IoT Cyberattacks Escalate in 2021, According to Kaspersky." IoT World Today. September 17, 2021. https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/

5. Adams, R. Dallon. "IoT device attacks double in the first half of 2021, and remote work may shoulder some of the blame." TechRepublic. September 13, 2021. https://www.techrepublic.com/article/iot-device-attacks-double-in-the-first-half-of-2021-and-remote-work-may-shoulder-some-of-the-blame/

6. Gandhi, Viral. "IoT in the Enterprise Report: Empty Office Edition" [2021 Report]. Zscaler; ThreatLabZ. July 15, 2021. https://www.zscaler.com/press/zscaler-study-confirms-iot-devices-major-source-security-compromise-reinforces-need-zero

7. IBM Security. "How much does a data breach cost?" [2021 Report]. IBM.com. https://www.ibm.com/security/data-breach

United States Contact:
info@aeris.net or
+1 408 557 1993

Europe Contact:
EU_info@aeris.net or
+44 118 315 0614