portnox®

WHITE PAPER

The State of
IoT Security

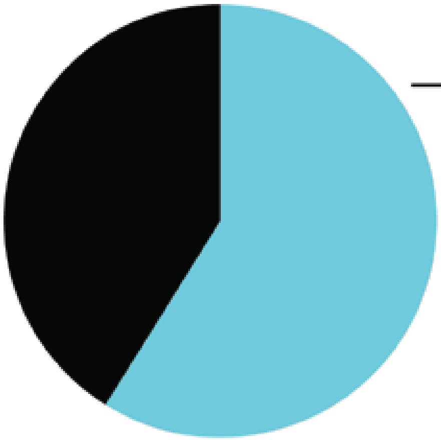
www.portnox.com

Table of Contents

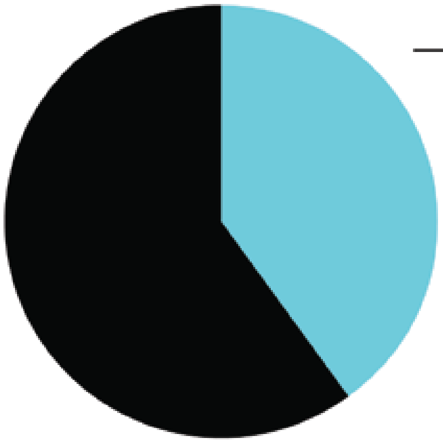
The State of IoT Security Today

Our world is becoming increasingly connected, and the Internet of Things (IoT) is at the forefront of this revolution. For example, the latest "Emerging Technology Trends Survey" from GlobalData, which surveyed 1,700 senior executives worldwide, reveals that 59% of respondents have already begun investing in IoT, with an additional 40% expected to ramp up their IoT investments in the coming 12 months[1].

This increased connectivity, however, comes with a heightened risk to our security. Many IoT devices lack the necessary built-in security controls to defend against threats, leaving them vulnerable to attack. The limited computational capacity and constrained environment of these devices mean that security controls often come up short.



59% have already begun investing in IoT



40% plan to ramp up IoT investment

[1] https://www.globaldata.com/store/report/iot-market-analysis/

We're Still Plagued by IoT Security Vulnerabilities

Weak Passwords

Weak passwords are one of the most pervasive and egregious security vulnerabilities plaguing IoT. Many devices come with default passwords that are easily guessable or hardcoded, making them easy targets for attackers. And in many cases, off-the-shelf IoT devices have their default passwords posted online, a simple Google search away. Even when users are prompted to create their own passwords, they often choose weak ones that are easily cracked.

Insecure Network Services

Another common issue is unneeded or insecure network services running on the device itself, especially those exposed to the internet. For example, a smart home security camera may have an unsecured remote access service that allows unauthorized parties to view or control the camera feed, putting the privacy and security of the homeowner at risk. These services can compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control.

Insecure Ecosystem Interfaces

Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device can also allow device compromise. Common issues include a lack of authentication/authorization, weak encryption, and a lack of input and output filtering. For example, if a mobile app used to manage an IoT device neglects to properly authenticate users or encrypt communication, it opens the doors for a man-in-the-middle attack.

Lack of Secure Update Mechanisms

Once a device is released, it's up to the manufacturer to provide updates to address new security risks. However, many IoT manufacturers do not release regular updates, leaving IoT devices vulnerable to attack from known security flaws.

Use of Insecure or Outdated Components

Many manufacturers use off-the-shelf components that may contain vulnerabilities, or they use outdated components that are no longer supported.

Insufficient Privacy Protection

Many IoT devices also lack sufficient privacy protections, such as encryption or data minimization. This can leave users' personal information exposed to unauthorized access or disclosure.

Insecure Data Transfer and Storage

Data transmissions between IoT devices can also be vulnerable to interception by third parties. This could allow threat actors to gain access to sensitive information, like user passwords or credit card numbers. Data storage on IoT devices can also be vulnerable to attack, exposing sensitive information.

Lack of Device Management

Finally, many IoT devices lack robust device management capabilities, making it challenging to track

[1] https://www.verdict.co.uk/verkada-security-breach/

There's a Lack of Coherent IoT Security Policies & Strategies

Despite the prevalence of IoT vulnerabilities, there is still a lack of coherent IoT security policies and strategies to mitigate these vulnerabilities. Furthermore, IoT security is still in its relative infancy, and the industry lacks stringent regulations or guidelines.

As a result, many organizations struggle to identify and address risks associated with IoT devices. And there is often a lack of understanding of how to manage these devices securely. Without a comprehensive strategy for securing IoT devices, IoT security risks will continue to grow.

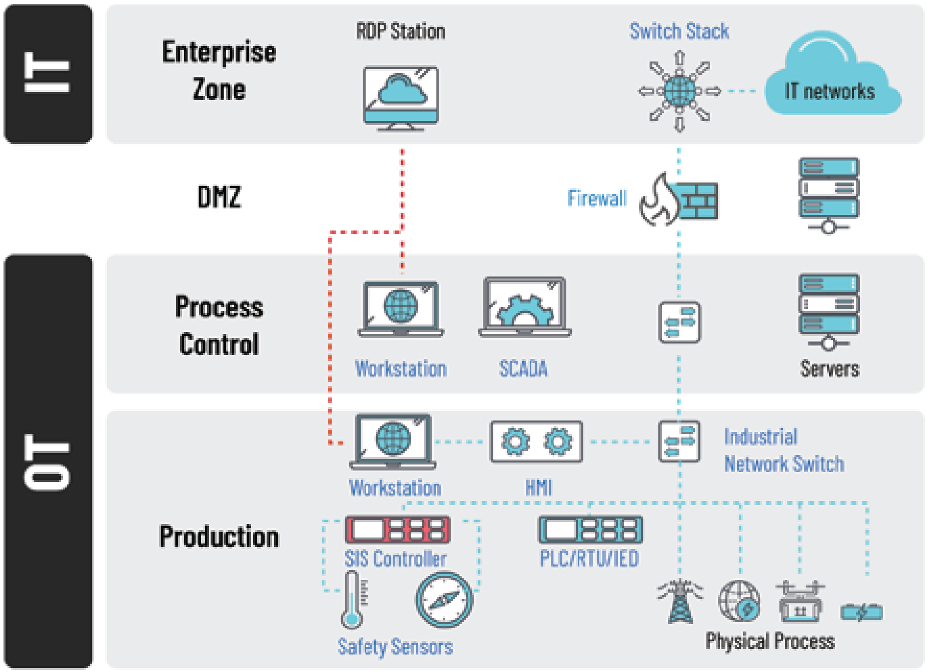
No One is Safe from an IoT-Focused Cyberattack

Recent high-profile attacks involving IoT devices highlight the urgent need for immediate and robust security solutions.

Triton: The World's Most Murderous Malware

Triton, dubbed "the world's most murderous malware," is a notorious malware discovered in 2017 that targets critical infrastructure safety systems, including those used in industrial environments. It aims to disable safety instrumented systems, which can lead to catastrophic accidents. The malware exploits a vulnerability in computers running Microsoft Windows and is believed to have been used in state-sponsored attacks.

In December 2017, Triton was responsible for an attack on a petrochemical plant in Saudi Arabia, which resulted in the shutdown of Schneider Electric's Triconex safety instrumentation system. The malware went undetected for almost a year and has been linked to a group called XENOTIME, affiliated with the Russian government.



Triton has since been used in attacks on critical infrastructure facilities in North America and other parts of the world. The attackers use custom tools designed for credential harvesting, remote command execution, backdoors, and widely available tools like Mimikatz. Additionally, the group frequently develops custom tools with a focus on evading anti-virus software.

Triton's ability to target safety systems highlights the potential for cyber-physical attacks to cause severe physical damage and loss of life[2345].

Ripple20: 19 Vulnerabilities in 2020

In 2020, JSOF, an Israeli cybersecurity firm, identified a group of 19 vulnerabilities called Ripple20 that could affect millions of IoT devices across different industries. These vulnerabilities were discovered in software developed by Treck Inc. in the late 90s, which enables companies to connect their devices to the internet via TCP/IP connections. JSOF warned that these Ripple20 vulnerabilities could impact vital machines in industries such as medical, power, transportation, oil and gas, and manufacturing.

[2] https://www.securityweek.com/triton-hackers-focus-maintaining-access-compromised-systems-fireeye/

[3] https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/new-critical-infrastructure-facility-hit-by-group-behind-triton

[4] https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/#:~:text=The%20rogue%20code%20can%20disable, parts%20of%20the%20world%2C%20too.

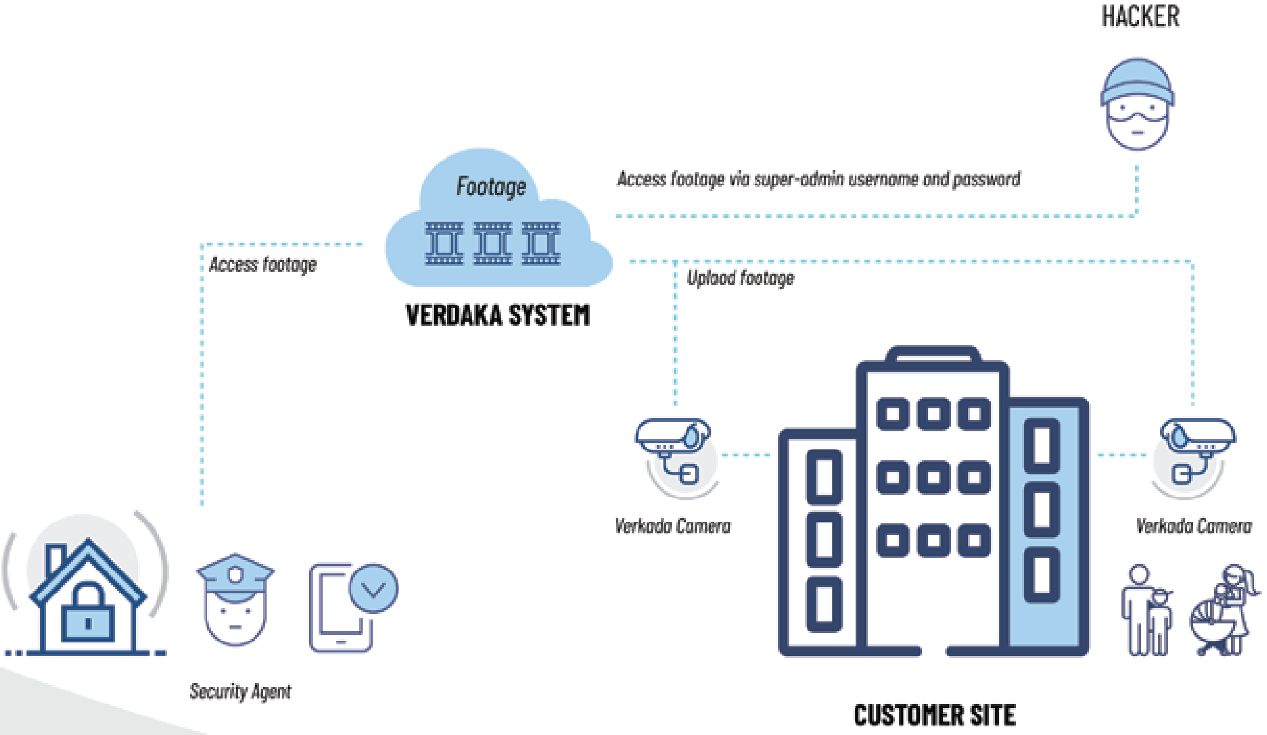
[5] https://techcrunch.com/2019/04/09/triton-malware-strike/

Experts estimated that hundreds of millions of IoT devices, including smart home devices, routers, printers, power grid equipment, and healthcare systems, are at risk of being impacted by Ripple20. Moreover, in addition to its direct use by equipment vendors, other software suites integrated the vulnerable library, making it challenging for companies to track its usage.

Some Ripple20 vulnerabilities pose significant threats, with four vulnerabilities receiving a CVSSv3 score of 9.8 or 10, indicating that they could allow attackers to take over vulnerable systems remotely. Attackers could exploit these vulnerabilities through the internet or local networks by accessing an internal network through a compromised router [6,7,8,9].

Verkada: It Could be Watching You

In March 2021, Verkada, a video security start-up, suffered a cyber attack that resulted in unauthorized access to customer data. The attackers gained access to a misconfigured customer support server, where they obtained customer support administrator credentials and accessed customer devices using internal support functionality. In addition, they viewed video or image data for a subset of Verkada customers, including footage from over 149,000 security cameras from office buildings, schools, and consumer homes.



[6] https://www.trendmicro.com/vinfo/de/security/news/internet-of-things/millions-of-iot-devices-affected-by-ripple20-vulnerabilities

[7] https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come/

[8] https://www.jsof-tech.com/disclosures/ripple20/

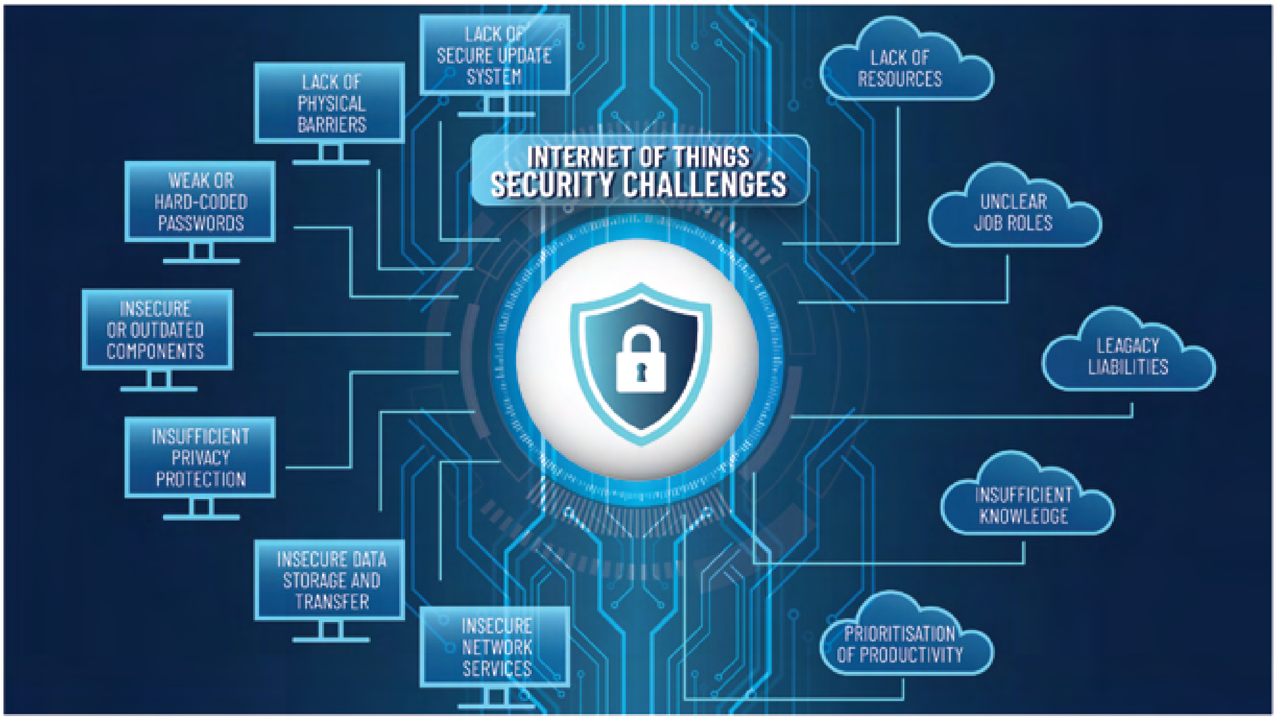
[9] https://www.wired.com/story/ripple20-iot-vulnerabilities/

Notable victims included Tesla, Nissan, and security firm Cloudflare, as well as jails, schools, and hospitals. In total, 97 customers had their cameras accessed, eight of which had Access Control product data accessed, including badge credentials.
The attackers also obtained a list of Command users and Verkada sales orders.

Tillie Kottman, a Swiss hacker accused of hacking dozens of companies and government agencies and leaking internal files and records of more than 100 entities, was behind the attack. Verkada acted swiftly, cutting off the attackers' access within two hours and notifying affected customers within six hours [10] [11] [12] [13].

The State of IoT Security Strategies Today

While IoT devices are becoming increasingly ubiquitous, IoT security strategies have been slow to catch up, leaving them vulnerable to various security threats. One key area where IoT security strategies fall short is in their failure to prioritize security from the outset of device development, often leading to security vulnerabilities being baked into the very foundation of IoT systems.


INTERNET OF THINGS
SECURITY CHALLENGES
LACK OF SECURE UPDATE SYSTEM
LACK OF PHYSICAL BARRIERS
WEAK OR HARD-CODED PASSWORDS
INSECURE OR OUTDATED COMPONENTS
INSUFFICIENT PRIVACY PROTECTION
INSECURE DATA STORAGE AND TRANSFER
INSECURE NETWORK SERVICES
LACK OF RESOURCES
UNCLEAR JOB ROLES
LEAGACY LIABILITIES
INSUFFICIENT KNOWLEDGE
PRIORITISATION OF PRODUCTIVITY

One reason for this is the lack of standardization in IoT security. Without universally accepted security standards, each device or system may have its own unique vulnerabilities and security requirements. This makes it difficult to implement consistent security measures across an entire IoT ecosystem.

These shortcomings leave IoT devices and their users at risk of cyber-attacks, data breaches, and other security threats.

[10] *https://securityboulevard.com/2021/03/verkada-surveillance-hack-breach-highlights-iot-risks/*

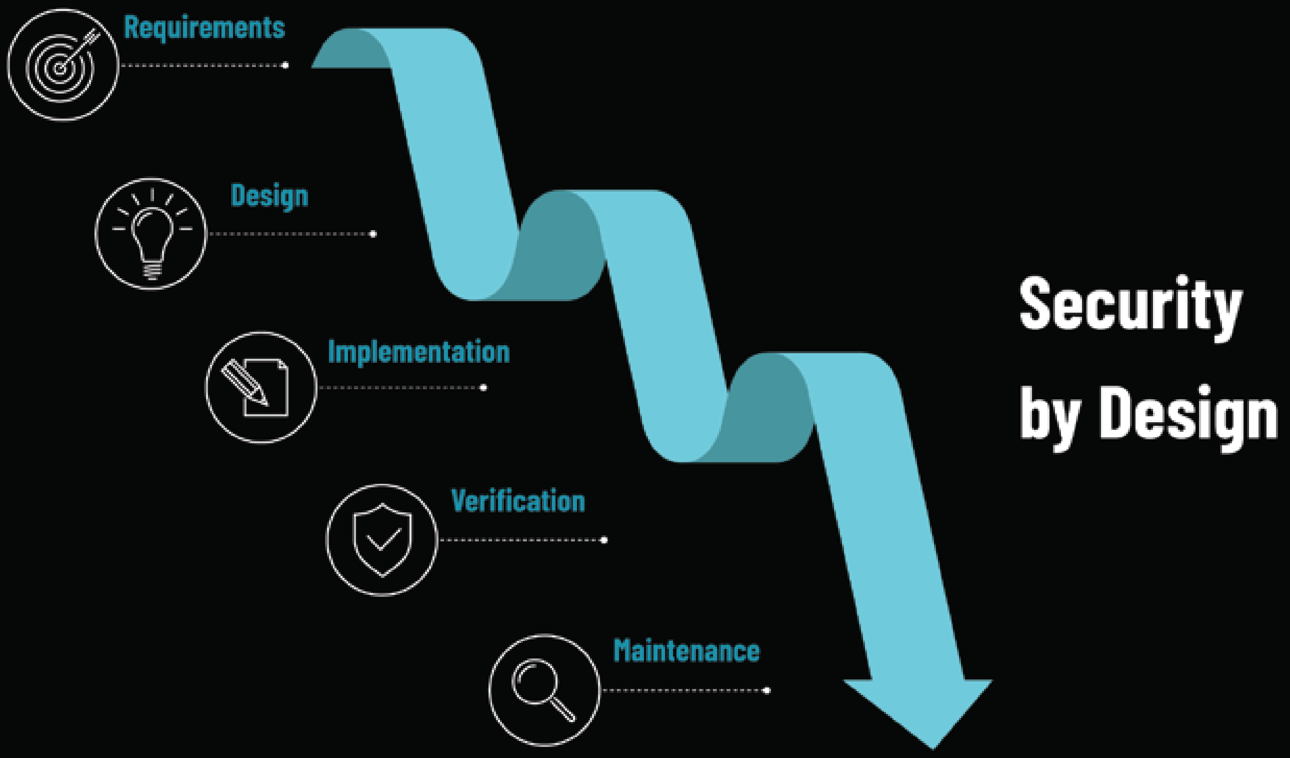
[11] *https://www.zscaler.com/blogs/product-insights/bringing-zero-trust-focus?_bt=649585368934&_bk=&_bm=&_bn=g&_bg=148078537322&utm_source=google&utm_medium=cpc&utm_campaign=google-ads-na&gclid=Cj0KCQjwu-KiBhCsARIsAPztUF2KQjecS4bmPHR7IGHMYLrZTDjovFURGtpqwyetW9krAVWkcy9HDusaAoPqEALw_wcB*

[12] *https://www.nozominetworks.com/blog/defending-against-iot-security-camera-hacks-like-verkada/*

[13] *https://www.verkada.com/uk/security-update/report/*

Where Do We See Success?

Successful IoT security strategies begin with Security by Design. This methodology prioritizes security at all stages of product creation and deployment to avoid retrofitting security requirements later down the line. But, of course, this isn't always possible. As the Verkada attack highlights, many millions of insecure IoT devices are already in existence, and recalling them and starting from the ground up isn't always feasible. For these devices, retrofitting IoT security measures like robust authentication, encryption, and stringent access controls is paramount.



IoT ecosystems are complex and diverse, which makes it challenging to develop a one-size-fits-all cybersecurity solution. This is why organizations with the most successful IoT security strategies take a deliberate and personalized approach to implementing security solutions. One key element of this is security risk assessment. A thorough security risk assessment is critical to mitigating risks throughout the IoT lifecycle, especially as it scales and expands.

We'll dive into specific IoT security technologies in the next section.

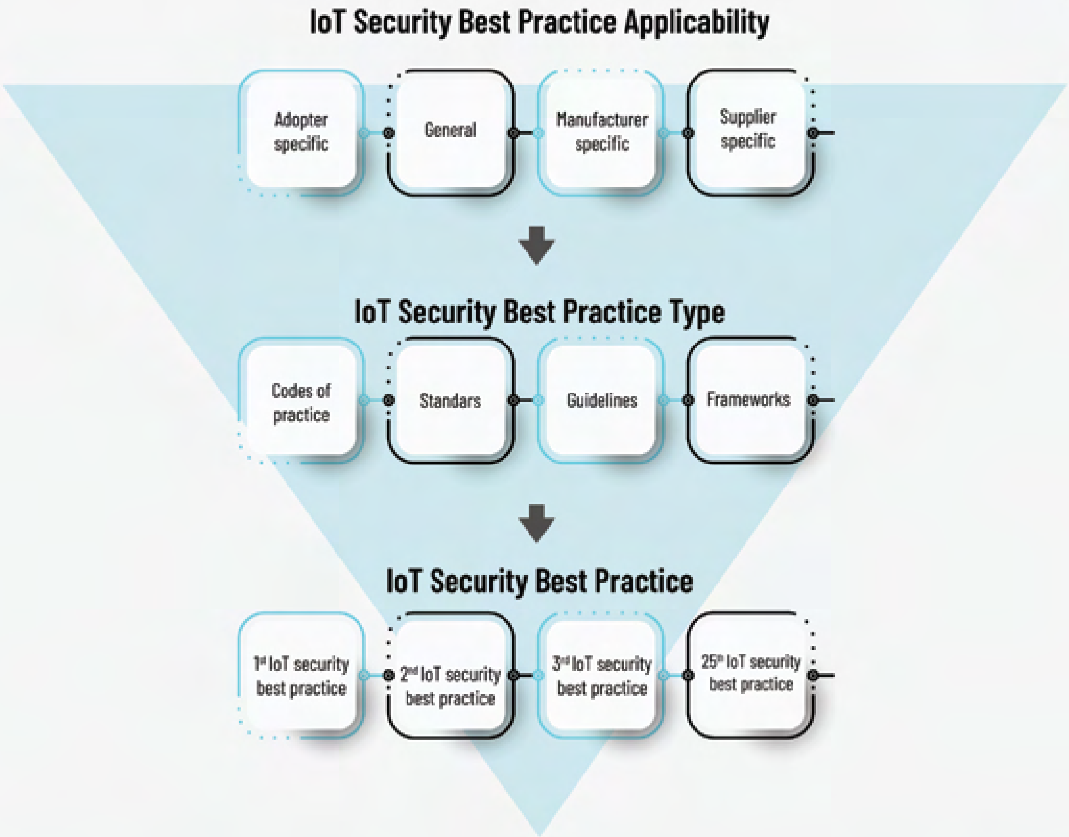
What Obstacles Remain?

Several obstacles still need to be overcome to ensure effective IoT security strategies. One major obstacle is the lack of buy-in from senior executives. Many organizations do not consider IoT security a top priority, leading to a lack of investment in security measures and a reluctance to allocate resources to address security concerns.

Another obstacle is the lack of expertise surrounding IoT security. Many organizations lack the necessary skills and knowledge to assess and mitigate IoT security risks properly. The IT industry at large is experiencing a skills gap, which only exacerbates the precarious nature of IoT security.

Additionally, the rapid pace of technological change and innovation in the IoT space can make it challenging to keep up with the latest security threats and vulnerabilities. As new technologies and devices are developed, new security risks and challenges may arise that organizations are not prepared to address.

Another ongoing challenge is the lack of standardization in IoT security. While there has been progress in this area, with reputable security bodies like the National Institute of Standards (NIST) releasing best practice guidelines, there's still some way to go. Without universally accepted security standards, companies often end up with a patchwork of security solutions that may not be effective in protecting against all types of security threats.



IoT Security Best Practice Applicability

Adopter specific — General — Manufacturer specific — Supplier specific

IoT Security Best Practice Type

Codes of practice — Standars — Guidelines — Frameworks

IoT Security Best Practice

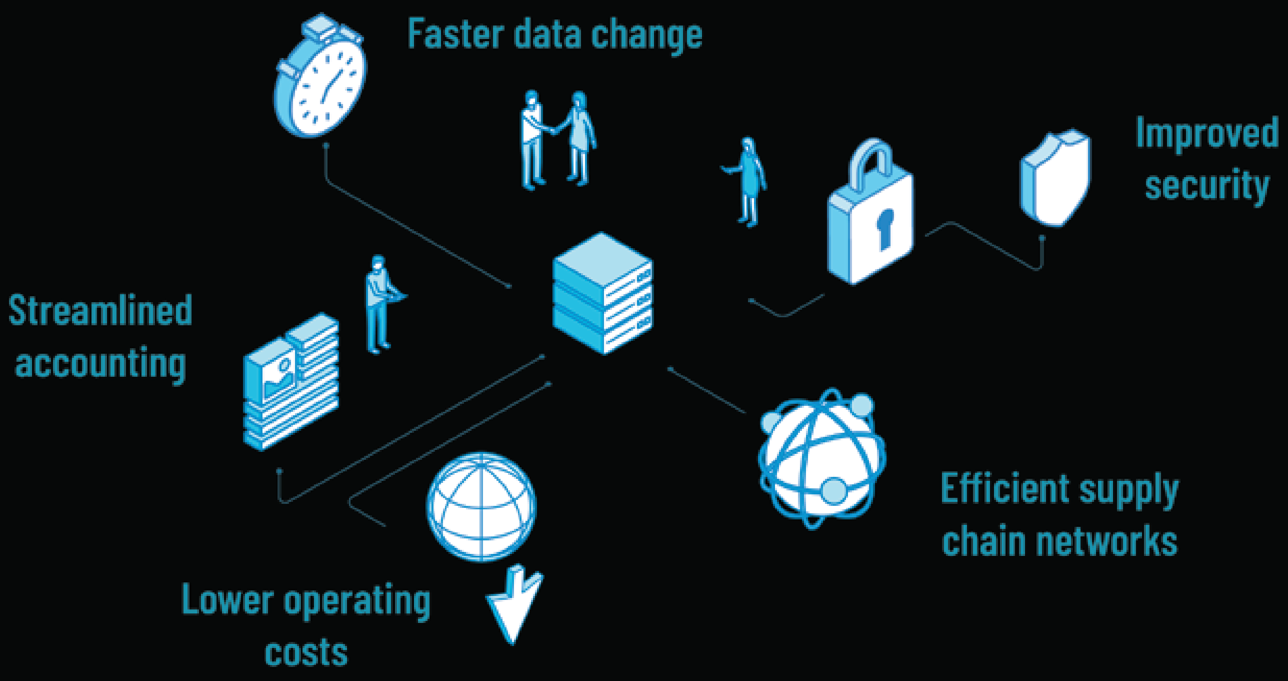
1st IoT security best practice — 2nd IoT security best practice — 3rd IoT security best practice — 25th IoT security best practice

Finally, the cost of implementing robust IoT security strategies can be high, especially for smaller organizations with limited resources. This can lead to a reluctance to invest in security measures, leaving devices and systems vulnerable to attacks and breaches.

IoT Security Technologies that Can Close the Gap

Blockchain: Over-Marketed, but Nonetheless Effective

Blockchain is a digital ledger that records all transactions in a secure and unalterable way. Each transaction is verified and then added to a block linked to previous blocks, creating a chain of blocks - hence the name "blockchain.



One significant benefit of using blockchain with IoT is that it can help build trust in IoT data. By storing IoT data on a private blockchain network, all transactions are recorded and added to a secure, immutable data chain that cannot be changed, only added to. This makes IoT data virtually theft and tamper-proof. And there are many other benefits to blockchain for IoT, including:

- Decentralization: Decentralization is a crucial feature of blockchain technology that can enhance transparency and security in IoT applications. By eliminating the need for a central authority, blockchain creates a distributed network of nodes that work together to verify and validate transactions.

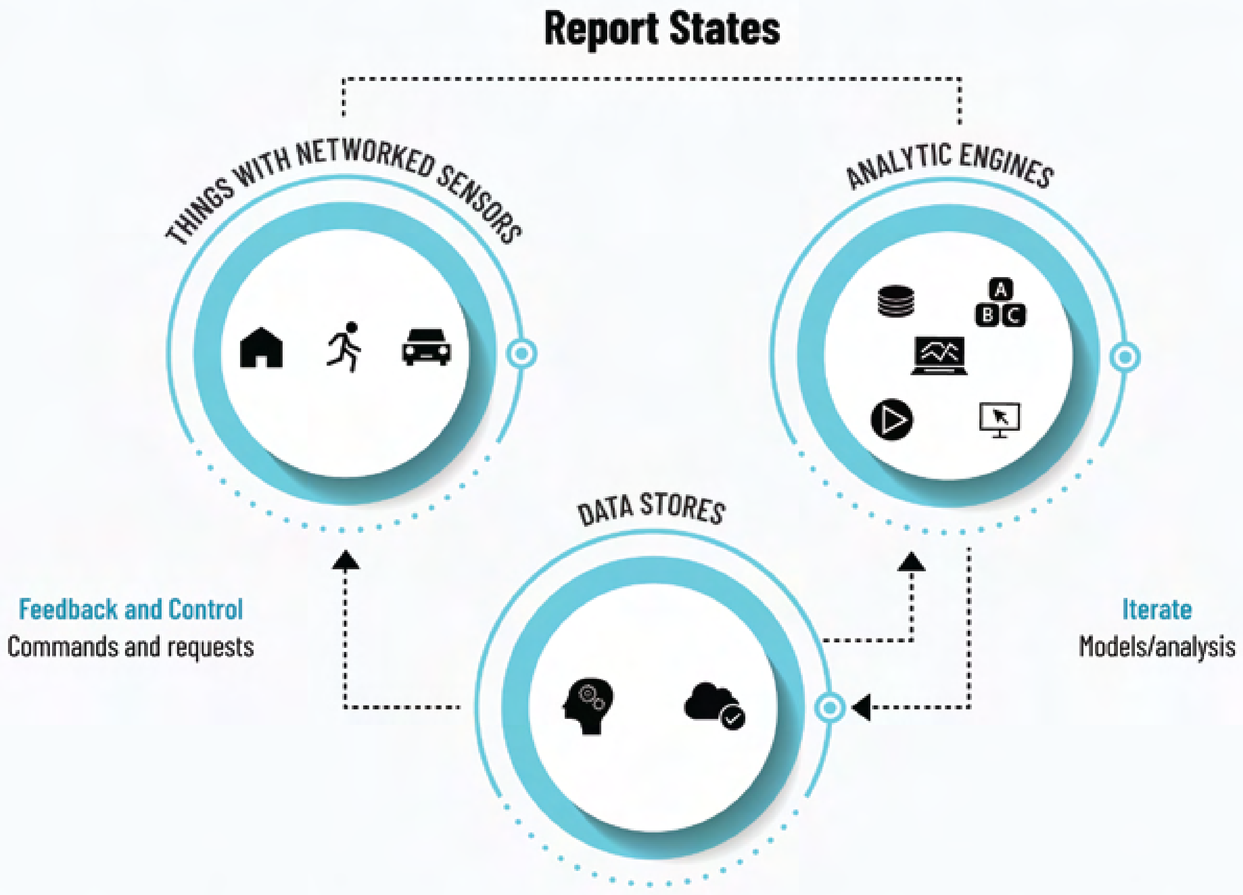
- Smart Contracts: Smart contracts are self-executing contracts with terms written directly into code, enabling automation of processes like payments and data sharing in IoT. Using smart contracts can streamline operations and ensure compliance with regulations.

- Privacy: Private blockchain networks can improve privacy and data protection in IoT by limiting access to authorized parties. This is especially important in industries that handle sensitive data, like healthcare.

The applications of blockchain and IoT are wide-ranging, from tracking components for regulatory compliance to logging operational maintenance data. One specific use case is in freight transportation, where blockchain can store the temperatures, position, arrival times, and status of shipping containers as they move, ensuring that all parties can trust the data and take action to move products quickly
and efficiently.

AI & Machine Learning:

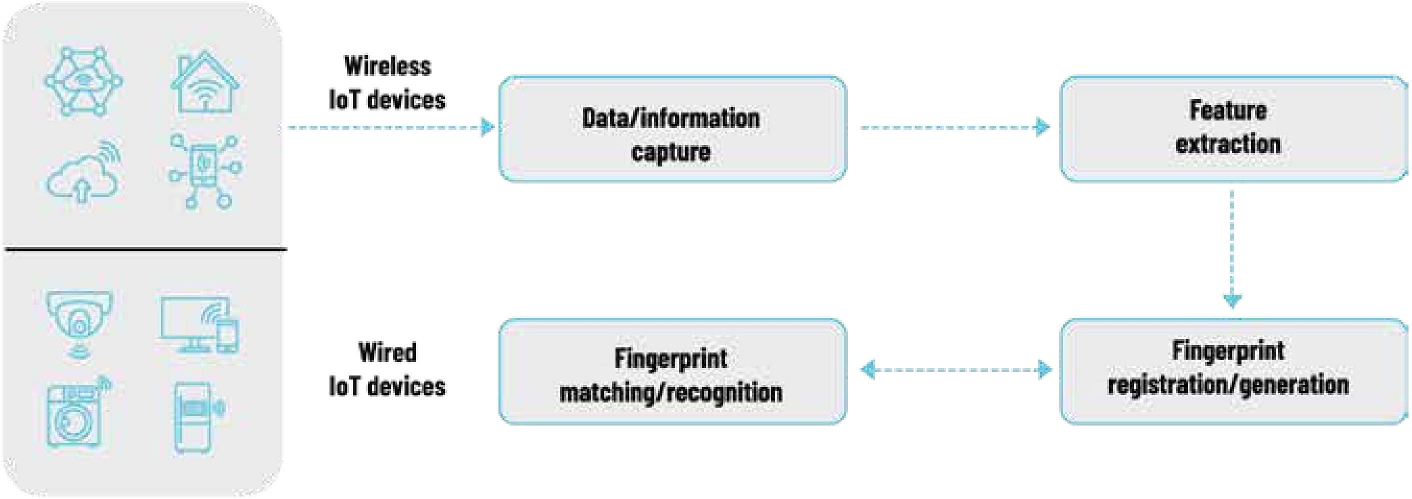
AI and ML provide a powerful defense against security threats by enabling real-time monitoring, identification, and response to anomalous behavior. By analyzing vast amounts of data generated by IoT devices, AI and ML can detect patterns and anomalies that might indicate malicious activity, such as DDoS attacks, ransomware, and botnet infections. AI and ML can also assist in identifying vulnerabilities in IoT devices and systems, allowing for swift remediation. And by learning from past attacks and incidents, AI and ML can improve security posture and enable predictive and proactive measures against future threats.



In addition, AI and ML can help with device authentication by analyzing usage patterns, behavioral data, and biometric identifiers. They can aid in anomaly detection by detecting deviations from normal patterns of behavior, allowing for early detection and response to potential security breaches. AI and ML can also predict potential failures of IoT devices and schedule maintenance to prevent security breaches caused by malfunctioning devices. Lastly, they can analyze data from multiple sources to provide insights into emerging threats and attack patterns.

IoT Fingerprinting & Profiling

IoT fingerprinting involves identifying IoT devices' unique characteristics, such as their manufacturer, model, and firmware version, by analyzing their network traffic. And IoT profiling involves creating a behavioral profile of each IoT device, such as the type of data it sends and receives, its communication patterns, and its typical usage patterns.



By implementing IoT fingerprinting and profiling, organizations can better understand their IoT devices and detect any abnormal behavior quickly. This technology enables organizations to monitor their IoT devices in real time and identify any malicious activity, such as data exfiltration, unauthorized access, or malware infections. IoT fingerprinting and profiling can also help organizations identify and manage vulnerabilities in their IoT infrastructure. By analyzing IoT device traffic and behavior, organizations can identify potential attack vectors and prioritize patching and remediation efforts accordingly.

Moreover, it can also help organizations comply with regulatory requirements and industry standards, like the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS).

Enhancing IoT Security with the Portnox Cloud

Closing the IoT Gap for Zero Trust

Portnox firmly believes the key to zero trust security is to control access and thus control risk, but IoT devices present unique challenges when applying basic network monitoring and security practices like fingerprinting.

Since these devices typically do not have the mechanism to support a network authentication protocol like 802.1x - that means you have to either use a Wi-Fi network protected only by a password or MAB (MAC address Bypass) which is basically just a deny/allow list of MAC addresses. Neither of these methods is among the best practices for network security and potentially increases the possibility that one of your IoT devices will be compromised.

In Search of a Better Method for IoT Visibility & Control

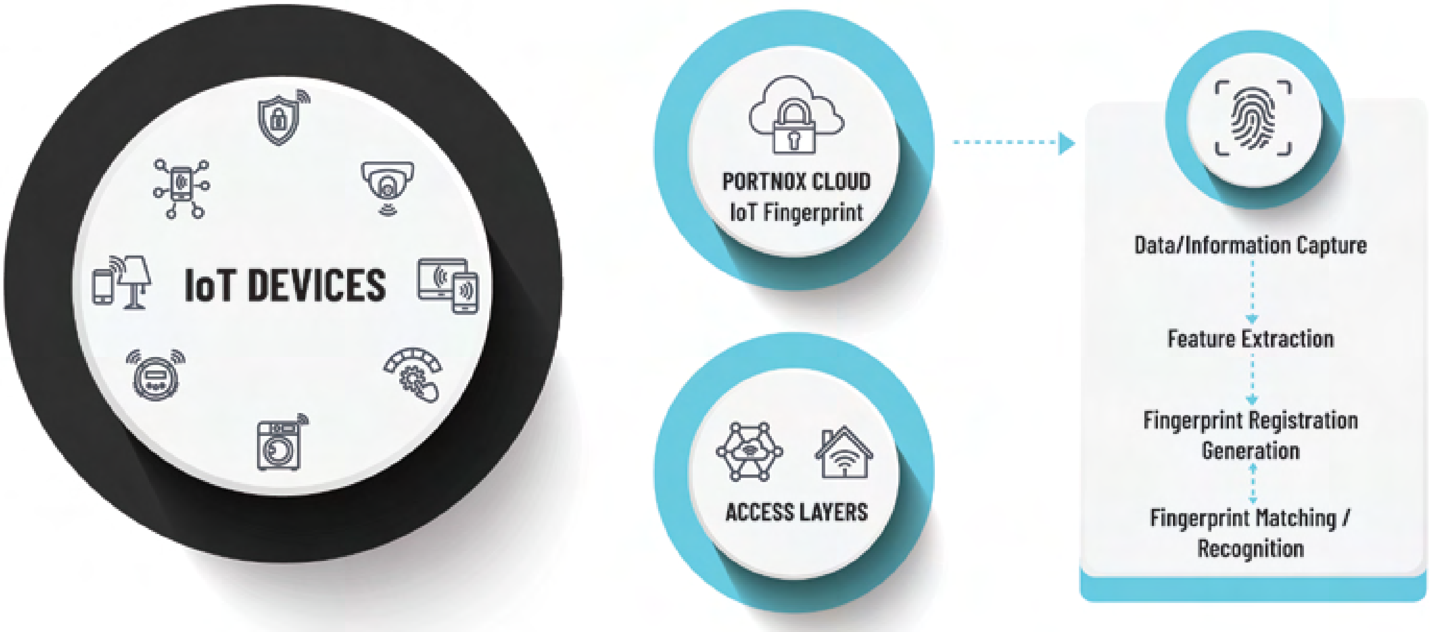
Traditional network monitoring is done via an active protocol - for example, SNMP, WMI, CDP/LLDP, or an Nmap scan. Unfortunately, IoT devices generally do not respond to these active methods, nor can you install extra software like an agent that would communicate back to a network monitoring system. At most, you might be able to get an ICMP response, but even that is often disabled - and of course, it does not tell you anything about the device itself, just that something exists.

That leaves you to look at more passive methods of IoT profiling. One of the most common ones is MAC address clustering. When a device is manufactured, the production run typically has a range of MAC addresses assigned to them - so the first device is 00:11:22:aa:bb:cc and the next device is 00:11:22:aa:bb:cd and then 00:11:22:aa:bb:ce - and so on. The first 6 letters of a MAC address, called the OUI (Organizationally Unique Identifier), identifies the manufacturer, and you can use the remaining values of the cluster to identify the device. There are several free, publicly available websites that will identify a device based on the MAC address that you can test.

Another passive method that yields highly accurate fingerprinting results is called DCHP Gleaning. When a device connects to your network, it contacts a DHCP server to get an IP address. The way in which it makes this request, along with the information it provides, can be used to identify the device. Many manufacturers of enterprise switches support a feature called DCHP gleaning, where they will listen for DHCP requests and forward the information on to, say, a RADIUS server as part of the accounting traffic to be used in fingerprinting.

Cloud-Native IoT Fingerprinting & Device Profiling

Portnox uses both DHCP gleaning and MAC address clustering to give customers the ability to fingerprint over 260,000 distinct types of IoT devices across 27,000 brands. Our IoT solution goes beyond just fingerprinting – we use DHCP gleaning and behavior analysis to detect changes in device behavior to protect against MAC address spoofing. So, if a security camera suddenly starts behaving like a laptop, administrators will be alerted, and the device can be automatically kicked off the network.



Combining this with 802.1x authentication for network access control, Portnox is an essential component of a zero trust security strategy. The cloud-native architecture simplifies deployment and maintenance, removing much of the overhead that comes with on-premises NAC solutions.

What Lies Ahead for IoT Security

Here are some emerging technologies poised to shape the future of IoT security.

Secure Hardware

One of the primary challenges of IoT security is the difficulty in securing a vast number of devices, each with their unique hardware configurations. However, secure hardware offers a potential solution to this problem. Secure hardware refers to the use of dedicated security chips embedded within IoT devices, enabling them to perform cryptographic operations, securely store sensitive data, and establish secure communication channels.

In addition, these security chips also protect against hardware-level attacks, such as side-channel attacks, which can extract sensitive data by exploiting the physical properties of the device. Finally, and critically, implementing secure hardware can also ensure that IoT devices remain secure even if other layers of security are compromised, such as software or network-level security measures.

Software-Defined Perimeter

Another approach to securing IoT devices is to employ a software-defined perimeter (SDP). An SDP is a security model that establishes secure communication channels between devices within a network while limiting their exposure to the internet. The SDP model replaces the traditional perimeter-based security model, which relies on firewalls and other security measures to protect against external threats. Instead, SDP creates a virtual boundary around infrastructure, effectively concealing it from external parties and attackers. Authorized users can still access the infrastructure by providing the necessary credentials.

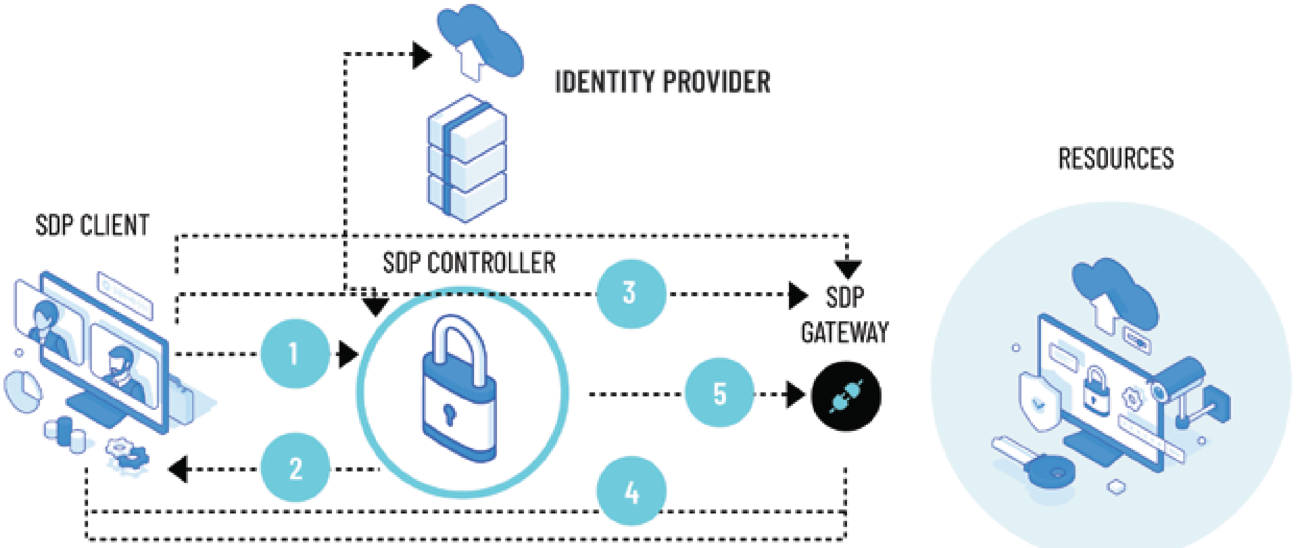


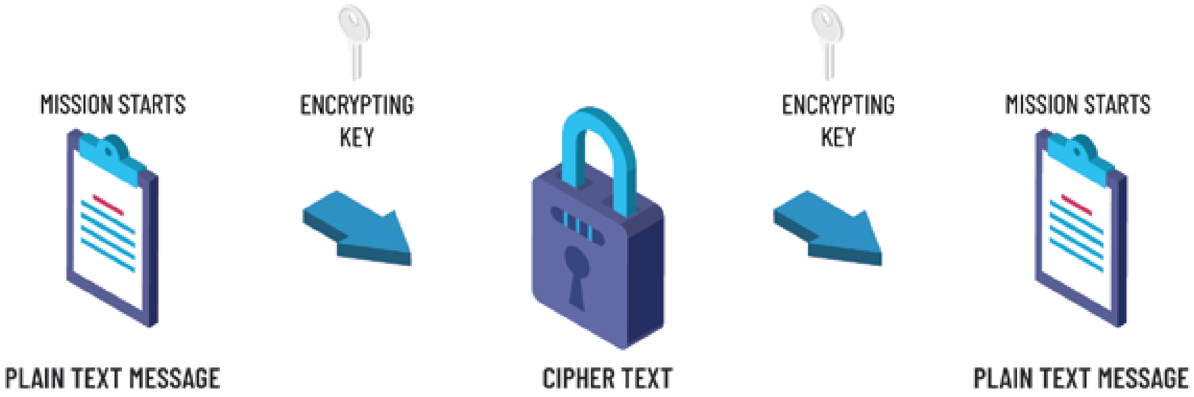
DIAGRAM - SDP REFERENCE ARCHITECTURE

An SDP approach also offers dynamic access control, which means access to the IoT device is only granted for a limited time or under specific circumstances, adding an extra layer of security. Additionally, SDP can encrypt all traffic between the IoT device and the authorized user, protecting against eavesdropping and other attacks.

Post-Quantum Cryptography

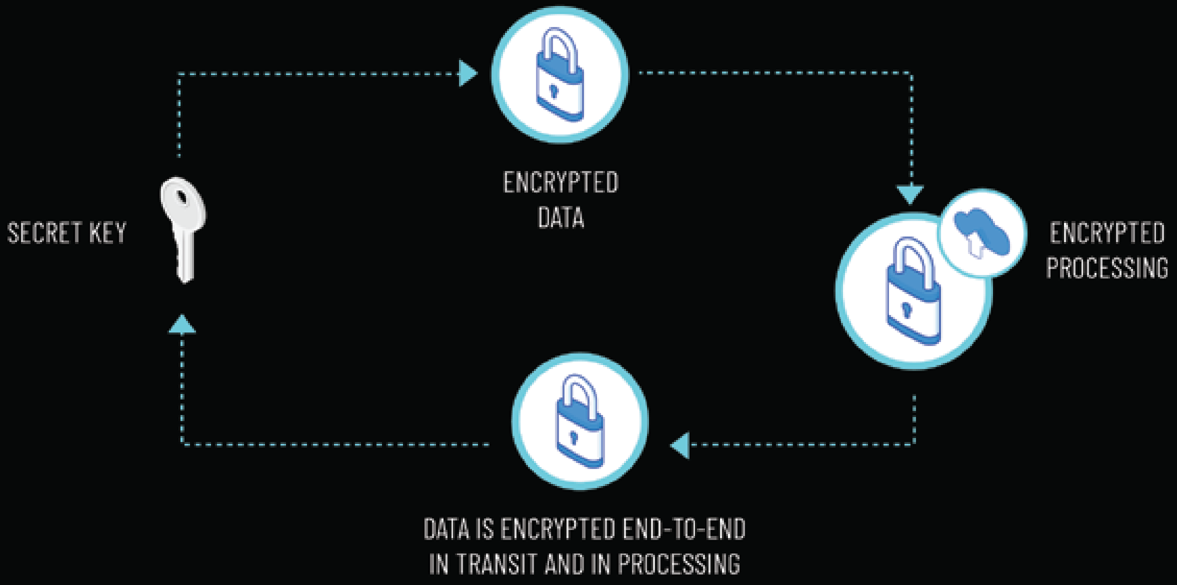
Cryptography is an essential tool for securing IoT devices and data. However, quantum computing threatens to render many of the existing cryptographic algorithms obsolete. Post-quantum cryptography offers a solution to this problem by providing cryptographic algorithms resistant to both conventional and quantum attacks.

These algorithms typically use mathematical problems that are challenging even for quantum computers to solve, such as the learning with errors (LWE) problem or the shortest vector problem (SVP).



Homomorphic Encryption

Homomorphic encryption enables computations to be performed on encrypted data without first decrypting it. This technology offers significant benefits for IoT security, allowing sensitive data to be processed and analyzed without ever being exposed to potential attackers.



Homomorphic encryption also enables secure data sharing and collaboration among different entities without requiring them to trust each other. This can be particularly important in industries such as healthcare, where IoT devices may collect and transmit sensitive patient data. By using homomorphic encryption, healthcare providers can perform data analysis and machine learning on patient data without putting that data at risk of being compromised.

Conclusion

IoT devices provide numerous benefits in efficiency, productivity, and cost-savings, with even more exciting new avenues coming in the future, but these benefits often come at the price of increased risk. Mitigating that risk via a comprehensive zero trust security strategy is essential to prevent a data breach, which can have disastrous consequences for your organization. Portnox can partner with you to make sure you are thoroughly protected without increasing the burden on your IT staff to maintain yet another tool.