CHECK POINT™

Modern Challenges for IoT Security

Tips for proactively preventing sophisticated IoT attacks

Introduction

While networked IoT devices can increase the productivity and efficiency of enterprise operations, they also bring significant security risks by expanding the cyber-attack surface. There are thousands of IoT devices deployed across every enterprise and many of them are unknown and unmanaged, so the security risk impacts everyone. Something as simple as the camera on a smart tv in a conference room can be breached and used to record conversations and steal intellectual property. Every enterprise is vulnerable to an IoT attack. There is a higher density of IoT devices in healthcare, manufacturing, distribution, transportation, energy, government, and utilities, so those industries have an even higher level of security risk.

IoT devices are not like PCs and mobile phones. They do not have security built in, don't usually have the ability to update the software, have default or weak passwords, and are based on older operating systems that are no longer supported. In regulated industries like healthcare and manufacturing, any change the software on a device could require recertification. This can be a long and costly process.

As businesses continue to incorporate IoT devices into their networks, they must have a security solution that balances the security risk with the operational benefits.

Why is IoT Security Important?

Networked IoT devices deployed on corporate networks have access to sensitive data and critical operational systems. Cyber threats target a range of IoT devices looking for an entry point into a network. These IoT devices include everything from simple printers, IP phones, smart TVs, and IP cameras to the more sophisticated medical devices and operational technology systems in manufacturing and other critical infrastructure.

Once in the network, they can move laterally to access more critical applications and sensitive data. They can then hold that information for ransom, shutting down the business network in the process.

A comprehensive IoT security solution needs to protect your business from all of these risks, and is a vital component of every company's cybersecurity strategy.

Industrial

Medical

Enterprise

Which Industries Need IoT Security?

All enterprises use IoT devices and are vulnerable to a cyber-attack and should pay special attention to IoT security best practices.

Enterprises

Organizations often have complex networks and limited visibility into the IoT devices connected to their networks. IoT security solutions are essential to discovering unmanaged IoT devices and managing their security risk.

Healthcare

The Medical Internet of Things (IoMT) is rapidly growing as healthcare providers take advantage of network connected scanners, monitoring tools, MRI machines, wearable devices and other network connected systems for patient care. The sensitive data that healthcare providers hold makes them prime targets for cyber threat actors.

Industrial

Operational Technology (OT) systems are increasingly connected to corporate networks and play a vital role in operational processes. Cyberattacks against these systems could degrade productivity, or even worse, have physical effects that harm an organization's infrastructure. For example, a cyber-attack on a water treatment facility exposed the drinking water of an entire city. The attackers could have made the water toxic and undrinkable.

IoT Security Best Practices

Securing devices requires securing both the devices themselves and their connections to the network.

Device Discovery & Risk Analysis

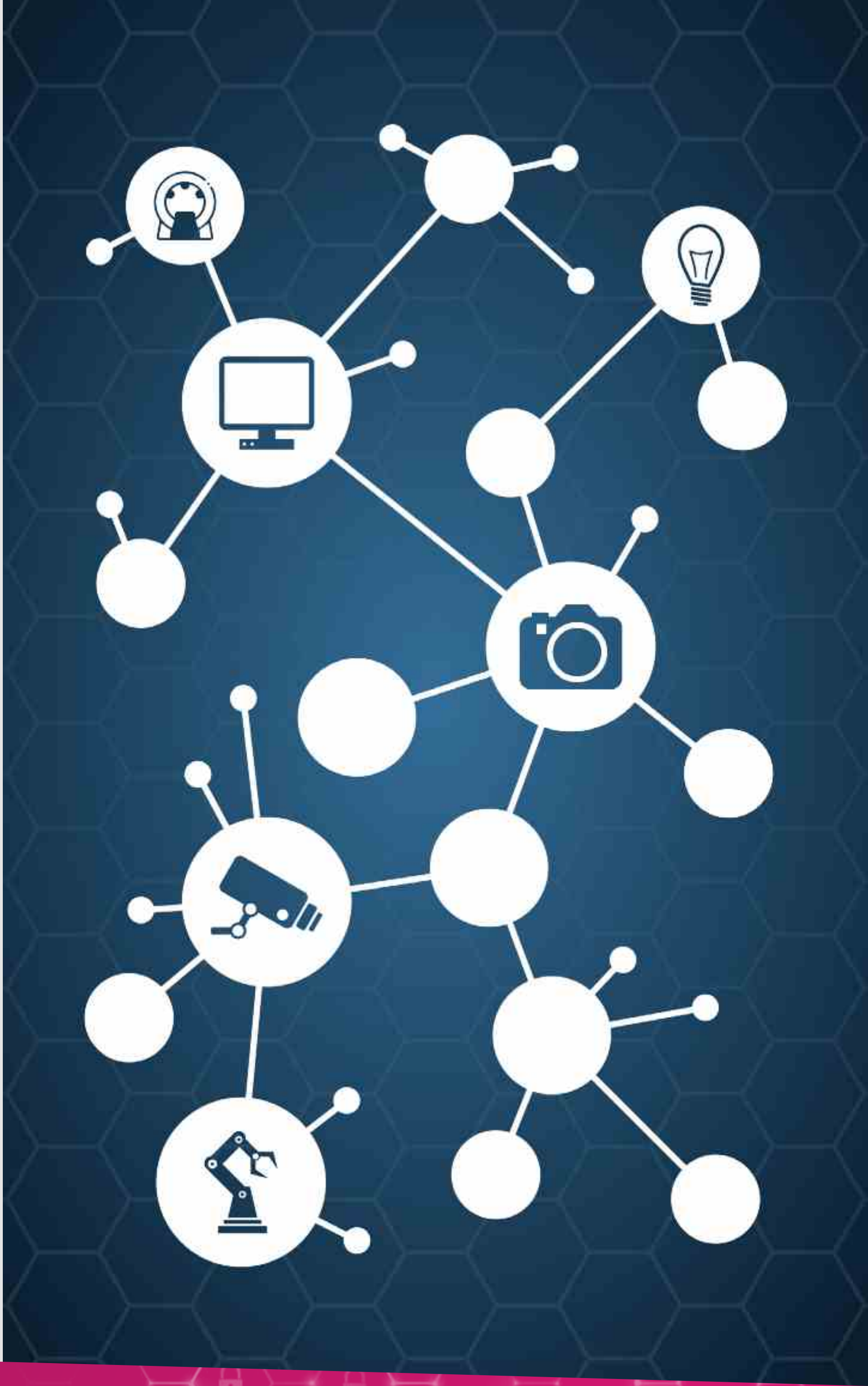
Organizations lack visibility into the IoT devices connected to their networks because employees may connect shadow unauthorized devices. Traditional endpoint solutions don't work on IoT devices, so they are vulnerable to attack. Completing a full inventory of networked devices is essential to securing IoT systems on the corporate network.

Zero-Trust Network Access

IoT devices deployed on the same network as other corporate systems, or are accessible from the Internet, are a potential access vector for attackers. Firstly, IoT devices should be segmented from the rest of the corporate network to minimize the risk that they pose to other corporate systems. Then, you can begin minimizing the attack surface even further with zero-trust policies that utilize device attributes and risk profiles. This allows for real-time enforcement to prevent IoT devices from ever compromising other assets or attempting communication with malicious sites.

Always up-to-date IoT Threat Prevention

Like PCs and phones, IoT devices can have vulnerable software and firmware. Most IoT and OT devices are closed systems, so they cannot be updated to protect against known vulnerabilities. Instead of changing the device software, enterprises block IoT attacks at the point the device is connected to the network using a network firewall. The Firewall Intrusion Prevention Systems (IPS) is constantly updated with the latest information on known and unknown IoT vulnerabilities and attacks across the globe.



Check Point Quantum IoT Protect

Autonomous threat prevention for both IoT devices themselves and their connections to the network.

1

Autonomous Zero Trust Protection

Quantum IoT Protect provides the ability to autonomously locate, analyze and determine the security risk of all IoT devices connected to the network; which is a key factor in securing IoT devices and networks. The devices are automatically categorized device type, category, and vendor and protected with zero trust IoT security policies, preventing unauthorized access all within minutes.

2

Advanced Threat Prevention

Security professionals need to have the ability to block known and unknown attacks. Quantum IoT Protect includes industry-leading IPS protection with break-through performance, containing over 10,000 protections for both IT and IoT devices and over 300 signatures and protections for Industrial Systems. These protections are applied via virtual patching and effectively protect the assets and devices in real time.

3

Preemptive On-Device Security

Quantum IoT Protect also offers revolutionary on-device runtime protection enabling customers to develop connected IoT devices with built-in firmware security, defending against the most sophisticated cyber attacks. Check Point's Nano Agent® is added to the IoT device with the assistance of the device manufacturer monitoring the current state of the device and taking action based on anomalies to identify and remediate zero-day attacks.

Additional Resources

Click on the following links to learn more about various aspects of IoT security and related topics and technologies.

Getting Started with IoT Security

- IDC IoT Security Guide 2022
- Video: IoT Embedded Security
- Industrial Control System Security
- IoT Security for Networks and Devices
- IoT Embedded Security

Related Topics

- What is SCADA?
- What is Nano Agent Security?
- What is OT Security?
- What is IoT
- Firmware Security

CHECK POINT™

Achieving IoT Security with Check Point

Internet of Things and networked OT devices have become a critical component of many organizations' operations and competitive advantage. However, as these devices become more embedded within a company, they pose a growing risk to the security of an organization's data and other devices on its network.

Check Point provides solutions for both network and on-device IoT security. For more information about Check Point's IoT Protect solutions, head to our **website** for more resources. Then, see its capabilities for yourself by requesting a **free demo**.

Worldwide Headquarters
5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753-4555
Fax: 972-3-624-1100

U.S. Headquarters
959 Skyway Road, Suite 300
San Carlos, CA 94070
Tel: 800-429-4391; 650-628-2000
Email: info@checkpoint.com