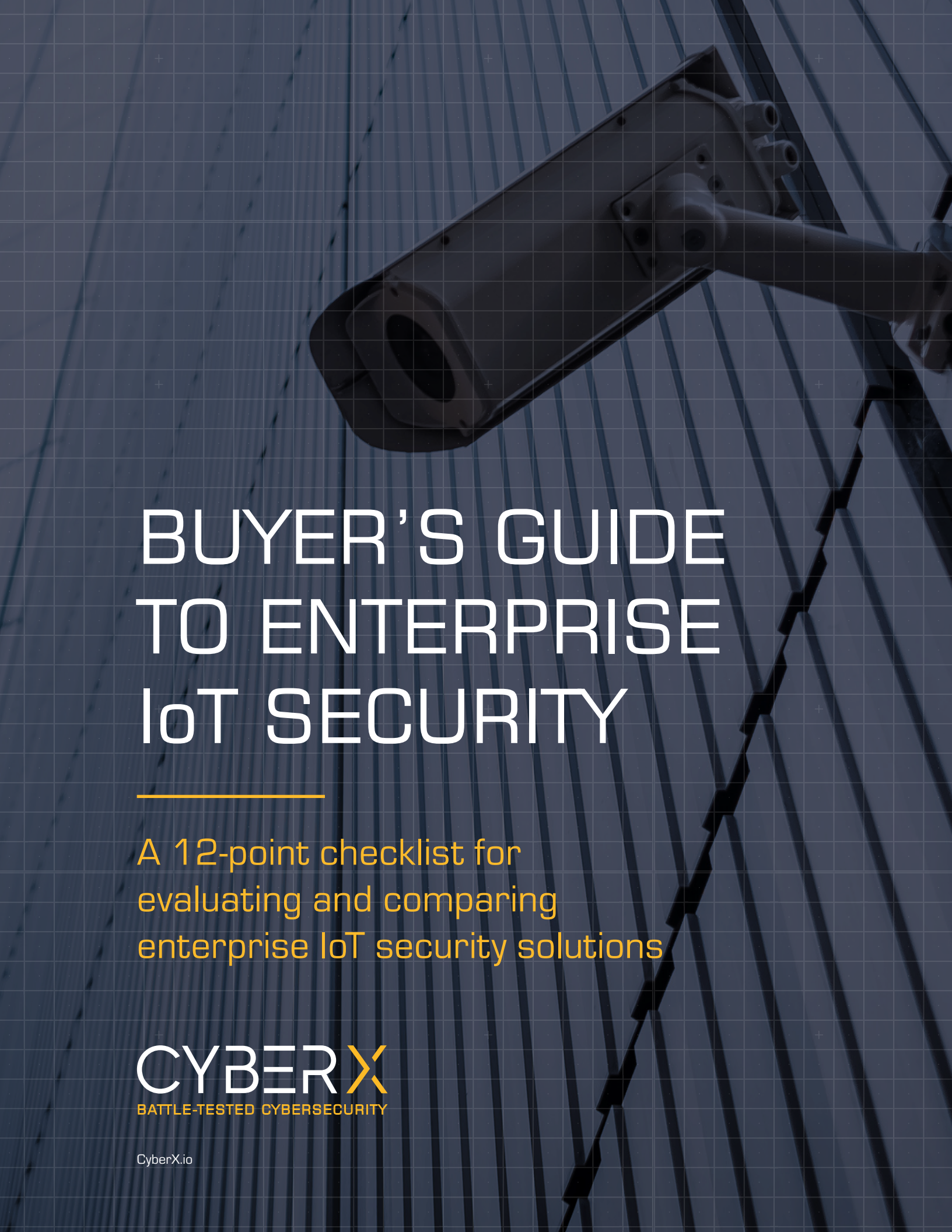


BUYER'S GUIDE TO ENTERPRISE IoT SECURITY

A 12-point checklist for evaluating and comparing enterprise IoT security solutions

CYBERX
BATTLE-TESTED CYBERSECURITY

CyberX.io

Table of Contents

1.0 WHAT'S AN IOT DEVICE? 3

2.0 THE RISK IS REAL 4

3.0 REAL-WORLD THREAT SCENARIOS 5

4.0 WHY TRADITIONAL SECURITY SOLUTIONS ARE INEFFECTIVE 7

5.0 12-POINT CHECKLIST FOR IOT SECURITY 8

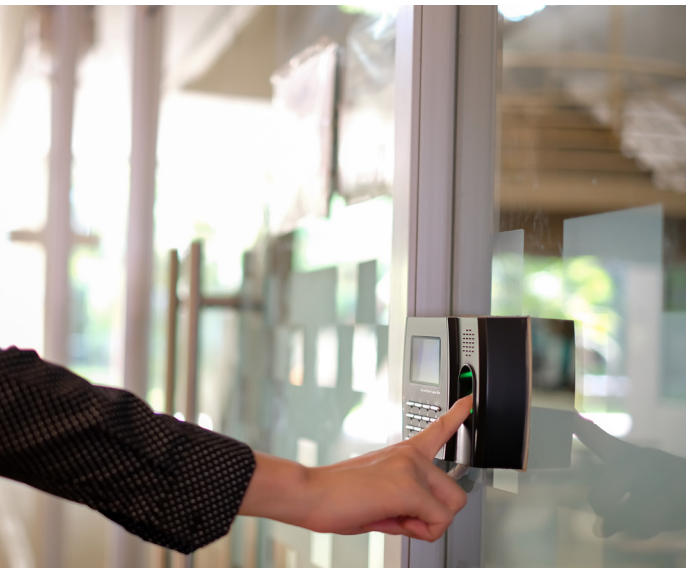
ABOUT CYBERX 16

1.0

What's an IoT Device?

Today's IoT devices come in many different shapes and sizes. They're used in almost every application in business and life. Examples include:

- **IT and office equipment** such as printers, routers, Smart TVs, VoIP phones, and wireless access points
- **Lab and clinical testing devices** such as temperature sensors and laboratory robotics (autosampling devices)



- **Smart Building and Building Management Systems (BMS)** for managing smart thermostats, security cameras, badge readers, building access control systems, heaters, ventilators, air conditioners, and elevators
- **Bring-Your-Own-Device (BYOD)** products connected to corporate or guest networks such as smart watches, Alexas, gaming consoles, mobile phones, tablets, and Raspberry Pis
- **Retail devices** such as price scanners, PoS terminals, and interactive kiosks
- **Logistics and warehousing systems** such as robotic stock pickers and automated guided vehicles
- **Industrial IoT** devices such as tracking devices and temperature or pressure sensors used for predictive maintenance and supply chain optimization
- **Smart Cities and Transportation** devices such as traffic control, smart lighting, and parking sensors
- **Medical devices** such as blood pressure monitors, infusion pumps, ECG units, and fitness devices

2.0

The Risk is Real

As organizations connect massive numbers of IoT devices to their networks to optimize operations, boards and management teams are increasingly concerned about the expanding attack surface and corporate liability they represent.

With good reason ...

IoT devices are truly everywhere. While they simplify our lives and streamline businesses in many ways, they're also soft targets that give adversaries a wide-open opportunity to penetrate corporate networks.

These connected devices are unmanaged, unseen, unpatched, and often misconfigured. What's more, they can't be protected by agent-based technologies — making them easily compromised by adversaries who use them to pivot deeper into corporate networks in order to:

- **Threaten safety**, exposing people to harm, the environment to pollutants, and firms to corporate liability and brand damage.
- **Steal intellectual property and trade secrets,** impacting competitive posture
- **Conduct ransomware attacks** that cause downtime, decreased customer satisfaction, and loss of revenue and shareholder value
- **Decrease operational efficiency** by siphoning resources for DDoS botnets and cryptojacking

A robust and comprehensive solution must not only be backed by a business case that is easily explained to executives and non technical decision-makers, it must, first and foremost, be effective.

3.0

Real-World Threat Scenarios

VoIP Phones and Office Printers Used to Gain Access to Corporate Networks

In August 2019, Microsoft reported it had discovered a campaign by Russian state-sponsored threat actors who were compromising "popular IoT devices across multiple customer locations."

The attackers exploited simple vulnerabilities to deploy their malware, including default administrative credentials on a phone and printer and a missing patch on a video decoder.

After establishing initial beachheads on compromised devices, the attackers scanned the network to look for other insecure devices. They were also seen enumerating administrative groups to search for higher-privileged accounts that would grant access to higher-value data. As the actor moved from one device to another, they would drop a shell script to establish persistence on the network for extended access.

Analysis of network traffic showed the devices were also communicating with an external command and control (C2) server.

3.0

RADIATION Malware Compromises CCTV Cameras for Botnet Attacks

Months before the Mirai IoT botnet attack brought down large portions of the internet, CyberX's Section 52 threat intelligence team discovered a campaign exploiting a known vulnerability in CCTV cameras in order to corral them into massive botnets. Dubbed RADIATION by the researchers, the campaign was promoted on the Dark Web as a DDoS-for-Hire service that could be rented on an hourly basis to attack victims.

Malware Exploits Vulnerabilities in Smart Building Access Systems

Researchers have recently uncovered a malware campaign that exploits critical vulnerabilities in smart building access systems, for which the manufacturer has never released a patch. These smart building systems are used to control what doors and rooms employees and visitors can access based on their access codes or smart cards. Attackers are actively targeting tens of thousands of devices every day in over 100 countries, with most attacks being observed in the U.S.

VPNfilter Malware Exposes Routers to Attacks

Infecting more than 500,000 devices in at least 54 countries, VPNfilter malware exploits known vulnerabilities and default credentials in internet-facing routers from a broad range of manufacturers (Linksys, MikroTik, NETGEAR, TP-Link) as well as in QNAP network-attached storage (NAS) devices.

The multi-stage malware consists of several modules that the adversary uses to: capture and analyze all traffic flowing through devices; perform man-in-the-middle (MITM) attacks to deliver exploits to traditional endpoints; intercept Modbus traffic used in industrial and BMS environments; and execute "kill" commands to disable devices — especially useful in ransomware attacks conducted by cybercriminals.

Hackers Access Casino's High-Roller Database Through Thermometer In Fish Tank

Yes, a fish tank. The fish tank had sensors connected to a PC that regulated the temperature, food and cleanliness of the tank. Once the sensor was compromised, the hackers were able to access other areas of the network, searching for sensitive customer and PII data, undoubtedly for ransom and/or blackmail.

4.0

Why Traditional Security Solutions are Ineffective

Endpoint protection

IoT devices don't support agents, so traditional antivirus programs can't be run on them, let alone modern Endpoint Detection and Response (EDR) solutions.

Network Access Control (NAC)

NAC systems are an important component of a multi-layered security strategy, but they were designed for access control rather than continuous network security monitoring, and lack the ability to detect vulnerabilities, anomalous behavior, or malware. What's more, they typically don't recognize a broad range of IoT/OT devices on their own, and can be complex to configure and maintain.

Vulnerability Scanners

Vulnerability scanners are also an important component of your overall security strategy, but they have a limited understanding of IoT vulnerabilities and they can't be used at all in OT environments because they require intrusive commands that can interfere with OT infrastructure. Additionally, they're only used periodically which means they can't detect rogue or unauthorized devices until the next scheduled scan. Finally, they lack behavioral anomaly detection capabilities to immediately identify compromised devices or networks.

Firewalls

Similar to NAC systems, firewalls serve an important role in controlling access to and from networks, but they have a limited understanding of IoT protocols, are blind to wireless protocols, and lack behavioral anomaly detection capabilities.

5.0

12-Point Checklist For IoT Security

When considering any technology platform, it's easy to get lost in the myriad of features, and distinguishing between the "nice to haves" and the "must haves." This 12-point checklist makes comparing platforms easier and can be used as the basis for your requirements setting process.

1. Agentless technology

Why it's important:

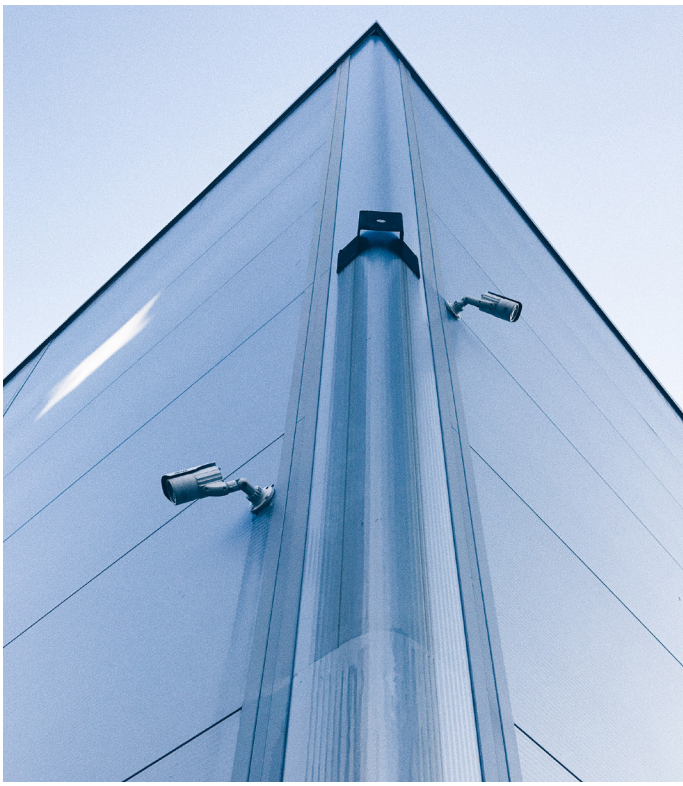
Traditional endpoint security involves the use of agents. But, IoT devices were never designed for agents due to their limited memory and CPU resources, and non-standard operating systems.

What's more, they're difficult to patch and often misconfigured, leaving them vulnerable to compromise. Adversaries know that IoT devices are soft targets, and use them to gain access to corporate and OT networks.

How we do it:

Rather than placing an agent of each device (which is impractical or impossible), CyberX detects attacks by analyzing data at the network layer. This non-invasive technique is known as Network Traffic Analysis (NTA) or passive monitoring.

By monitoring and analyzing network traffic, CyberX provides full visibility into your IoT devices and their risk posture without requiring agents or impacting network performance.



5.0

2. Rapid, easy deployment

Why it's important:

A key concern of CISOs and managers is 'how long will it take to deploy and how many of my FTEs will be required?' The concern is well-founded — platforms that are difficult to deploy or require additional in-house resources are often the first to be shelved.

How we do it:

The CyberX platform delivers insights within minutes of being connected to the network. Machine learning algorithms eliminate the need to configure any rules or signatures or have any prior knowledge of the network.

3. Available as a cloud-based service or on-premises

Why it's important:

As your organization scales and your cybersecurity policies evolve, you don't want to be locked into a fully on-premises or cloud-based solution. Choosing a solution with the option of migrating seamlessly from one to the other gives you the flexibility to stay agile.

How we do it:

CyberX not only offers you the choice of on-premises or cloud, we also provide a seamless migration path from one to the other. To eliminate any privacy or security concerns, CyberX only sends network metadata to the cloud. Additionally, each client's data is stored in their own virtual private cloud.

5.0

"How do we track and identify IoT devices?"

4. IoT asset discovery that is continuous, automated and complete — enabling zero-trust strategies and micro-segmentation policies

Why it's important:

You can't protect what you don't know about. With the proliferation of intelligent devices and networks, it's simply not possible to effectively manage your IoT environment, let alone protect it, without an automated asset management capability..

How we do it:

CyberX maintains the most comprehensive IoT profile database in the industry, containing millions of unique device profiles, across the broadest range of device types and protocols.

Profiles include detailed information about the device's unique DNA, such as ports used, protocols (both standard and proprietary), DNS locations, normal traffic volume, traffic destinations, etc.

Importantly, the discovery capability built into CyberX is both automated and continuous. It silently works in the background so that you're immediately alerted when a new (and potentially malicious) device is added to the network.

This visibility makes it significantly easier to segment IoT devices into separate networks and/or implement micro-segmentation policies to tightly control which devices can communicate with each other, corporate IT networks, and the outside world.

5.0

5. Risk assessment and scoring for each device — so you know what to fix first

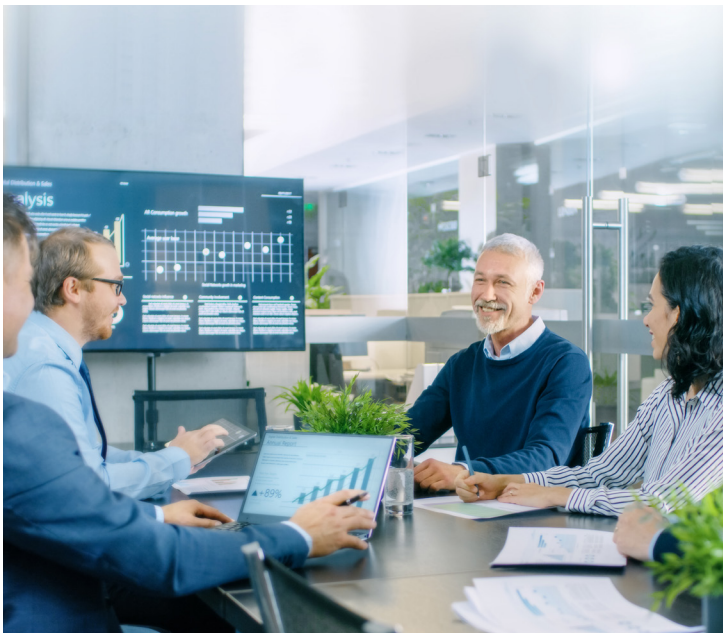
Why it's important:

Having an inventory of devices is one thing; knowing which ones to fix first is the key to properly allocating your time and resources to minimize risk. Otherwise, the real risk is being overwhelmed with vulnerability data and not knowing what to do with it.

How we do it:

CyberX analyzes each device and provides a risk score based on vulnerabilities detected (default credentials, insecure protocols, open ports, CVEs, misconfiguration, etc.)

The CyberX risk assessment isn't a basic data dump; it provides a list of actionable mitigation recommendations for each device.



"How do we assess risk and prioritize mitigation activities for IoT devices?"

5.0

6. Multiple threat detection mechanisms for faster and more accurate threat detection

Why it's important:

Platforms that rely on a single threat detection mechanism are prone to false positives and missed threats.

How we do it:

CyberX provides **Triple-Layer Threat Protection** to minimize false positives and accurately detect compromised devices. These 3 layers consist of:

6.1 IoT Device Profile Database: Leveraging an extensive device database containing millions of unique device profiles, CyberX can immediately identify devices that deviate from their expected profile (ports, DNS, etc).

6.2 Patented Behavioral Analytics: Using Layer 7 deep packet inspection (DPI) and the world's only patented, M2M-aware behavioral analytics and machine learning, CyberX establishes a baseline of device behavior over time. This allows the platform to immediately detect if a device is exhibiting suspicious or unauthorized behavior, based on the full context of the communication.

6.3 IoT Threat Intelligence: CyberX's Section 52 threat intelligence team uses an automated, ML-based threat extraction platform and IoT-specific malware sandbox to collect data from a range of open and closed sources in order to identify IoT-specific malware and campaigns targeting your organization. These Indicators of Compromise (IoCs) are continuously fed into our platform, providing a third mechanism for detecting malicious activity. CyberX is the only cybersecurity company to have this capability.

"How would we know if an adversary has already compromised one of our IoT devices?"

5.0

7. Integration with existing IT security stacks (SIEMs, ticketing, SOAR, CMDB, etc.)

Why it's important:

If you're like most enterprises, you've likely made significant investments in corporate SOCs to monitor and respond to threats. A platform that does not integrate with existing IT security stacks doesn't allow you to leverage existing people, training, workflows, and runbooks to operationalize IoT security alerts.

How we do it:

CyberX has developed native, API-level integrations with all major SIEMs, ticketing and SOAR systems, and CMDBs. Native integration means seamless, bidirectional communication. Plus, an open REST API enables custom integrations to quickly be added at any time to address specific requirements.

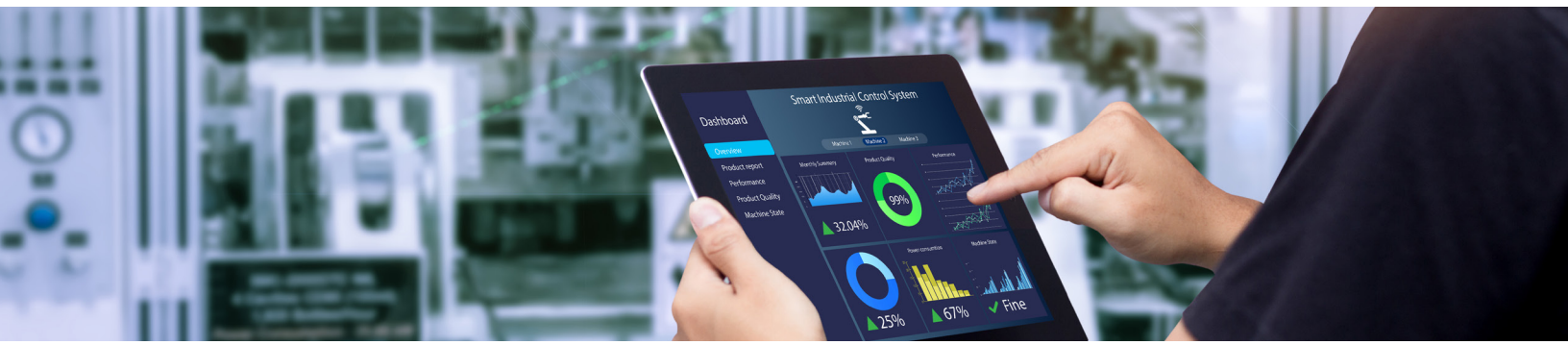
8. Unified solution for securing all unmanaged devices (IoT/BMS/IIoT/OT) to reduce TCO and complexity

Why it's important:

Today's CISO is responsible and accountable for creating a safety- and security-first enterprise — including IoT, BMS, IIoT, and "brownfield" OT devices. Having disparate solutions increases TCO and complexity, which increases risk — precisely the opposite of what you want to achieve.

How we do it:

CyberX is the only platform that provides a unified solution that addresses all these M2M domains with a holistic, single pane-of-glass solution. This unified approach is essential in helping CISOs pass security audits and demonstrate a unified IT/IoT/BMS/OT security governance strategy to the board.



5.0

9. Automated response — accelerating the time between threat detection and prevention

Why it's important:

Unless a compromised device is immediately isolated from the rest of the network, malware will quickly spread through it and adversaries will have more time to attack higher-value systems and privileged accounts.

How we do it:

By tightly integrating with a broad range of next-generation firewalls and Network Access Control (NAC) systems, CyberX enables compromised devices to be automatically blocked or isolated via policies.

10. Integrated with cloud IoT platforms

Why it's important:

Enterprises undergoing digital transformation via cloud IoT platforms are looking for security to be integrated seamlessly with their underlying platforms.

How we do it:

CyberX has developed an integration with Microsoft Azure Security Center for IoT to provide unified visibility across workloads running on edge, on-premises, in Azure, and in other clouds.

"Once we discover a compromised IoT device, how do we quickly respond and mitigate the threat?"

5.0

11. Open Development Environment (ODE) and SDK to rapidly support new and proprietary protocols

Why it's important:

New IoT protocols are being developed all the time, plus some protocols are proprietary. Without an Open Development Environment, devices with new or proprietary protocols can't easily or rapidly be supported by the platform.

How we do it:

Unique in the industry, CyberX offers the Horizon Open Development Environment (ODE) and SDK. This innovative solution enables clients and partners to easily add new protocol dissectors as simple plugins to the CyberX platform, without sharing PCAPs or divulging any sensitive information.

12. A mature solution that includes both robust technology and comprehensive services... because successful deployments are always about more than the technology.

Why it's important:

Incomplete platforms and solutions that don't take the human element into account usually lead to failed deployments.

How we do it:

CyberX has been deployed in more than 3,000 production networks worldwide, in some of the world's largest and most diverse IoT/OT environments. As a company, we have the deep expertise, organizational best practices, and comprehensive services required to help you successfully address your particular scale and complexity challenges.

ABOUT CYBERX

Funded by Norwest Venture Partners, Qualcomm Ventures and other leading venture firms, CyberX delivers the only cybersecurity platform built by blue-team experts with a track record of defending critical national infrastructure. That difference is the foundation for the most widely deployed platform for continuously reducing IoT risk and preventing costly outages, safety and environmental incidents, theft of intellectual property, and operational inefficiencies.

CyberX clients include Global 2000 organizations across diverse verticals such as healthcare, manufacturing, oil & gas, data centers, energy and water utilities, retail, mining, and transportation. Notable clients include three of the top 10 global pharmaceutical companies; three of the top ten US energy utilities; a top 5 cloud data center provider; multiple government agencies including the US Department of Energy; and national electric and gas utilities across Europe and Asia-Pacific.

Integration partners and MSSPs include industry leaders such as Splunk, Microsoft, IBM Security, Palo Alto Networks, ServiceNow, Fortinet, HPE/Aruba, Cisco, RSA, McAfee, Optiv Security, DXC Technology, Toshiba, Singtel/Trustwave, and Deutsche-Telekom/T-Systems. For more information visit CyberX.io or follow @CyberX_Labs.

CYBERX

BATTLE-TESTED CYBERSECURITY