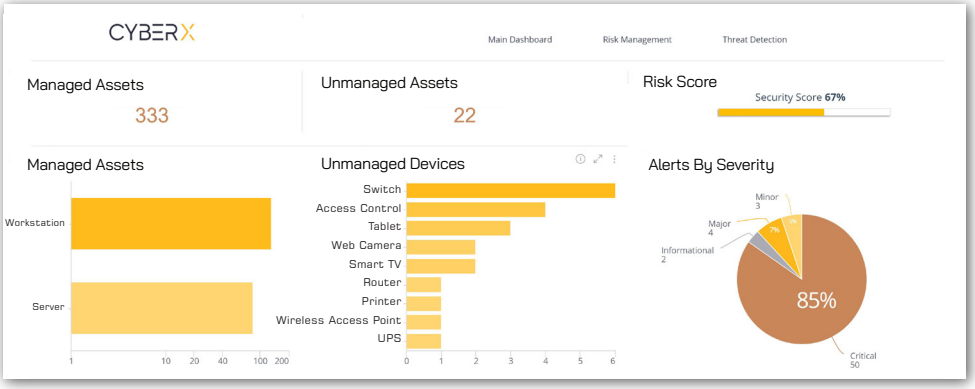
CYBERX
BATTLE-TESTED CYBERSECURITY

SOLUTION BRIEF

UNIFIED IoT/ICS SECURITY PLATFORM

Agentless discovery and protection of unmanaged IoT & ICS devices — using patented M2M-aware behavioral analytics and machine learning — enriched by IoT-focused threat intelligence



IoT & ICS Devices Bring Enterprise Risk

Every smart device requires smarter security, and enterprises have thousands of smart devices. Gartner predicts the number of IoT devices will grow to 25 billion by 2021, and the risks posed by unmanaged devices are expanding your attack surface — and risk.

Because these embedded devices can't be protected by agent-based anti-malware technologies — and are often unpatched or misconfigured — they can easily be compromised by adversaries to threaten safety, conduct ransomware attacks, pivot deeper into your network to steal sensitive intellectual property, and siphon computing resources for DDoS campaigns and cryptojacking.

These devices connect directly to your wireless or wired networks, so they can't be protected by perimeter firewalls. And traditional network-based access control solutions are often complex to configure and maintain, and don't address security issues such as identifying compromised devices and malicious activity.

Finally, traditional network scanning solutions can't be used in ICS environments due to their invasive approach, and often miss IoT devices altogether — plus even when they find assets they lack any behavioral understanding of those devices.

HIGHLIGHTS

ARCHITECTURE

- Unified security for both enterprise IoT (CCTVs, Smart TVs, wireless printers, etc.) and ICS (HMIs, PLCs, DCS, etc.)
- Fast and easy deployment via non-invasive, agentless monitoring
- Comprehensive device database with 12M+ profiles
- Broad and deep support for non-IT protocols (MQTT, BACnet, Modbus, Siemens S7, OPC, etc.)
- Cloud-based service (optional)

FUNCTIONALITY

- Asset discovery and classification
- Risk and vulnerability management
- Continuous threat monitoring via patented, M2M-aware behavioral analytics and machine learning
- IoT/ICS threat intelligence enriches analytics with latest indicators about zero-days, malware, campaigns
- Native SOC integrations with Splunk, IBM QRadar, ServiceNow, Palo Alto Networks, CyberArk, etc.

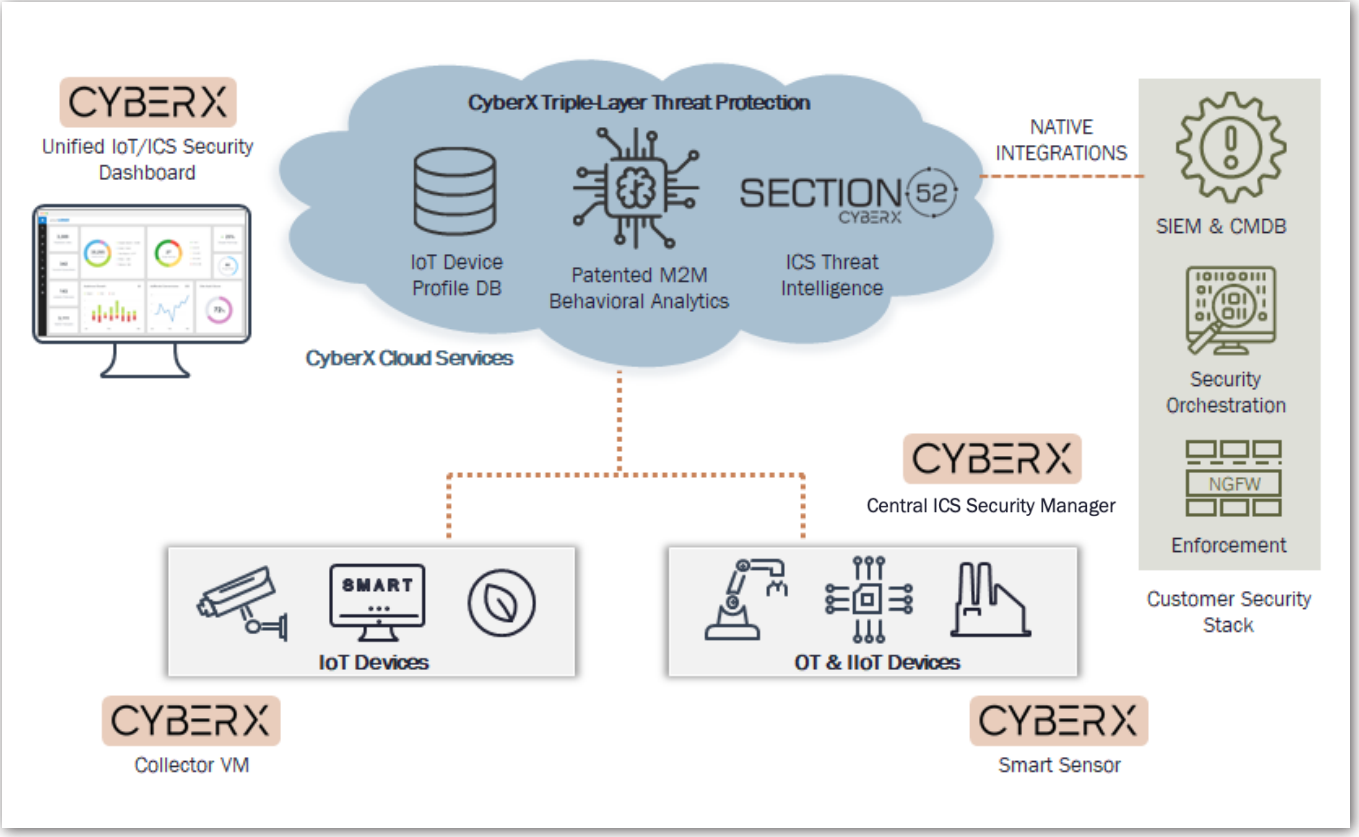
How CyberX Mitigates IoT/ICS Risk

CyberX's IoT/ICS security platform uses an agentless approach to continuously discover IoT/ICS assets, identify device risks and vulnerabilities, and monitor your network for threats.

IoT networks are monitored by a VM Collector that sits in the customer's IT network and collects information from SPAN ports, Wireless LAN Controllers, Active Directory, and SNMP.

ICS networks are monitored through an on-premises sensor appliance (physical or virtual) that listens to network traffic via a SPAN port. The information about devices, traffic, and vulnerabilities can be viewed through the on-premises central ICS security manager and/or through the cloud-based unified IoT/ICS security dashboard.

By integrating this information with your existing security stack (SIEM, CMDB, etc.) in your Security Operations Center (SOC), CyberX enables your security team to rapidly respond to and mitigate threats. Here's how CyberX works:



- CyberX passively collects network traffic from SPAN ports. This information is enriched by device and user information collected from other sources such as wireless LAN controllers, Active Directory, and SNMP.
- CyberX's cloud-based platform uses patented, M2M-aware analytics to identify assets, risks, and anomalous behavior indicating threats in your network.
- Customers view detailed information about assets, risks, and threats in the cloud-based dashboard.
- For ICS environments, all processing can be performed on-premises without requiring network traffic to be sent to the cloud. While an on-premises console is also provided, all IoT/ICS security information can also be viewed in the unified IoT/ICS security dashboard.

Triple-Layer Threat Protection: Why CyberX IoT/ICS Security is Better

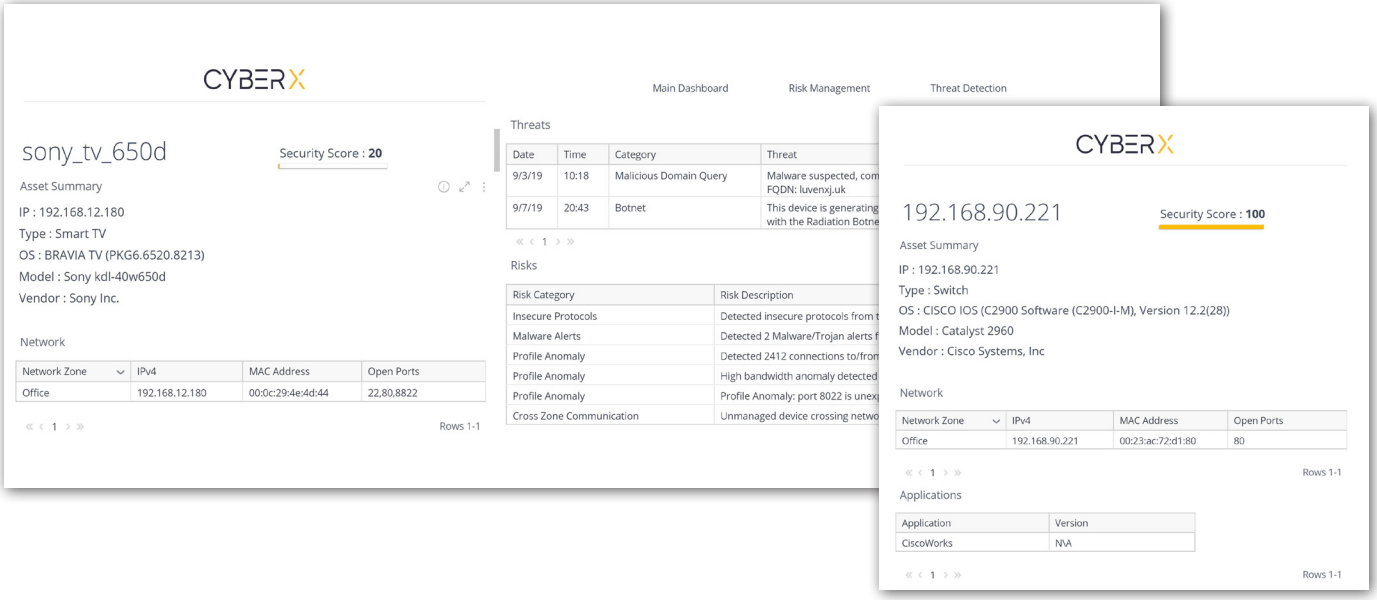
The CyberX IoT/ICS security solution features Triple-Layer Threat Protection – meaning that it answers 3 critical questions about every unmanaged device in the target environment.

1. **Device Profiles:** Is the device behaving in a way that is consistent with its standard behavior (ports, protocols, DNS, traffic volume, etc.)? Leveraging an extensive device database containing millions of unique device profiles, CyberX knows what an uninfected device's behavior looks like "in the wild." CyberX can immediately alert you when any of your devices have been compromised.
2. **Patented Behavioral Analytics:** Is the device deviating from its baseline of behavior over time? Using Layer 7 deep packet inspection (DPI) and the world's only patented, M2M-specific behavioral analytics with machine learning, CyberX establishes a baseline of behavior that allows the platform to assess whether a device is exhibiting suspicious or unauthorized behavior, based on the full context of the communication (such as which command is being sent to the device).
3. **IoT/ICS Threat Intelligence:** Is your network the target of nation-states, cybercriminals, or chaotic actors? CyberX uses an automated, ML-based threat extraction platform and a team of seasoned threat analysts to identify IoT/ICS-specific malware and campaigns targeting your organization.

Asset Discovery

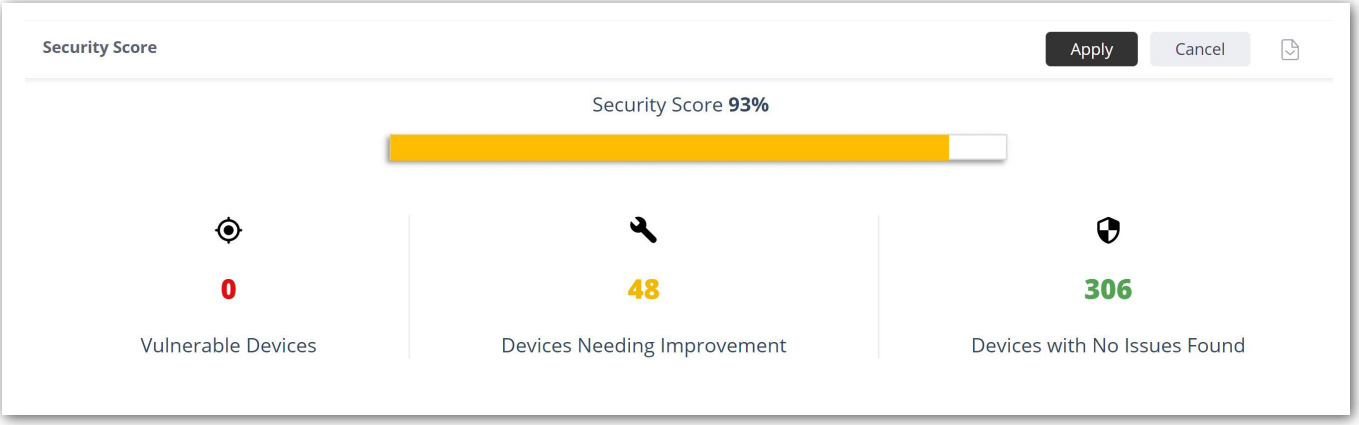
You can't protect what you can't see. With the proliferation of intelligent connected devices, it's simply not possible to effectively manage your IT/OT environment, let alone protect it, without this visibility. Asset information collected in IoT networks includes the IP/MAC address, type of device, OS, model, vendor, network zone, the list of open ports, and threats and risks associated with the IoT device. Asset information collected in ICS networks includes MAC/IP address, model #, vendor, firmware version, serial #, rack/slot, protocols used, ports, polling intervals, and security alerts.

In the main dashboard, you can view an overall security score for the network as well as the total number of managed and unmanaged assets, the types of managed and unmanaged assets, and alerts grouped and graphed by severity. You can then select any one of these devices to see additional detail as shown in the two examples below.



Risk & Vulnerability Management

CyberX includes actionable mitigation recommendations — prioritized by risk — so you know what needs to be done now, and what can wait. CyberX provides an overall security score as well as a list of devices sortable by level of security so that you can concentrate efforts on devices and issues that are least secure. Using this information you can quickly visualize and prioritize actions to ensure the actions you take have the greatest impact.



Continuous Threat Monitoring, Detection & Response

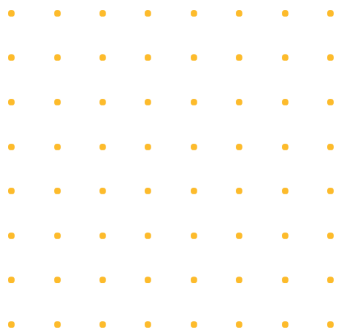
Today's attackers use multiple techniques across the attack chain to compromise your network. That's why CyberX uses 5 distinct analytics engines to immediately detect both zero-day and known threats in real time, leveraging deep packet inspection and the world's only patented M2M-aware behavioral analytics and machine learning. This provides faster detection of threats while reducing the learning period and alert noise, and eliminating the need to configure any rules or signatures.

IoT/ICS Threat Intelligence

CyberX is the only cybersecurity firm with an in-house team of IoT/ICS-focused threat intelligence analysts and security researchers — world class domain experts and data scientists who previously staffed a national CERT defending against daily nation-state cyber attacks. They bring that expertise to CyberX by tracking IoT-specific zero-days and CVEs as well as IoT campaigns, malware, and adversaries. The team has already submitted more than a dozen zero-day vulnerabilities to the US ICS-CERT, including previously unknown vulnerabilities for devices manufactured by a broad range of IoT/ICS device manufacturers.

SOC Integration

As the industry's most open and interoperable IoT/ICS cybersecurity platform, CyberX reduces complexity and eliminates silos by integrating out-of-the-box with your existing SOC workflows and security stack including major SIEMs, CMDBs, firewalls, NACs, ticketing, secure remote access systems, etc.



ABOUT CYBERX

We know what it takes.

CyberX delivers the only cybersecurity platform built by blue-team experts with a track record defending critical national infrastructure. That difference is the foundation for the most widely-deployed platform for continuously reducing IoT/ICS risk and preventing costly production outages, safety and environmental incidents, and theft of sensitive intellectual property.

CyberX delivers the only IoT/ICS security platform addressing all five requirements of the NIST CSF and all four requirements of Gartner's Adaptive Security Architecture. CyberX is also the only security company to have been awarded a patent for its M2M-aware threat analytics and machine learning technology.

Notable CyberX customers include 2 of the top 5 US energy providers; a top 5 global pharmaceutical company; a top 5 US chemical company; multiple government agencies including the US Department of Energy; as well as national electric and gas utilities across Europe and Asia-Pacific. Integration partners and MSSPs include industry leaders such as Splunk, IBM Security, RSA, Palo Alto Networks, ServiceNow, CyberArk, McAfee, Toshiba, HPE/Aruba, Fortinet, Optiv Security, DXC Technology, Singtel/Trustwave, and Deutsche-Telekom/T-Systems.

Customers choose CyberX because it's the simplest, most mature, and most interoperable solution for auto-discovering their assets, identifying critical vulnerabilities and attack vectors, and continuously monitoring their IoT/ ICS networks for malware and targeted attacks. What's more, CyberX provides the most seamless integration with existing SOC workflows for unified IT/OT security governance.

For more information, visit CyberX.io or follow @CyberX_Labs.

CYBERX

BATTLE-TESTED CYBERSECURITY