Joint Solution

Microsoft Defender for IoT + Corelight

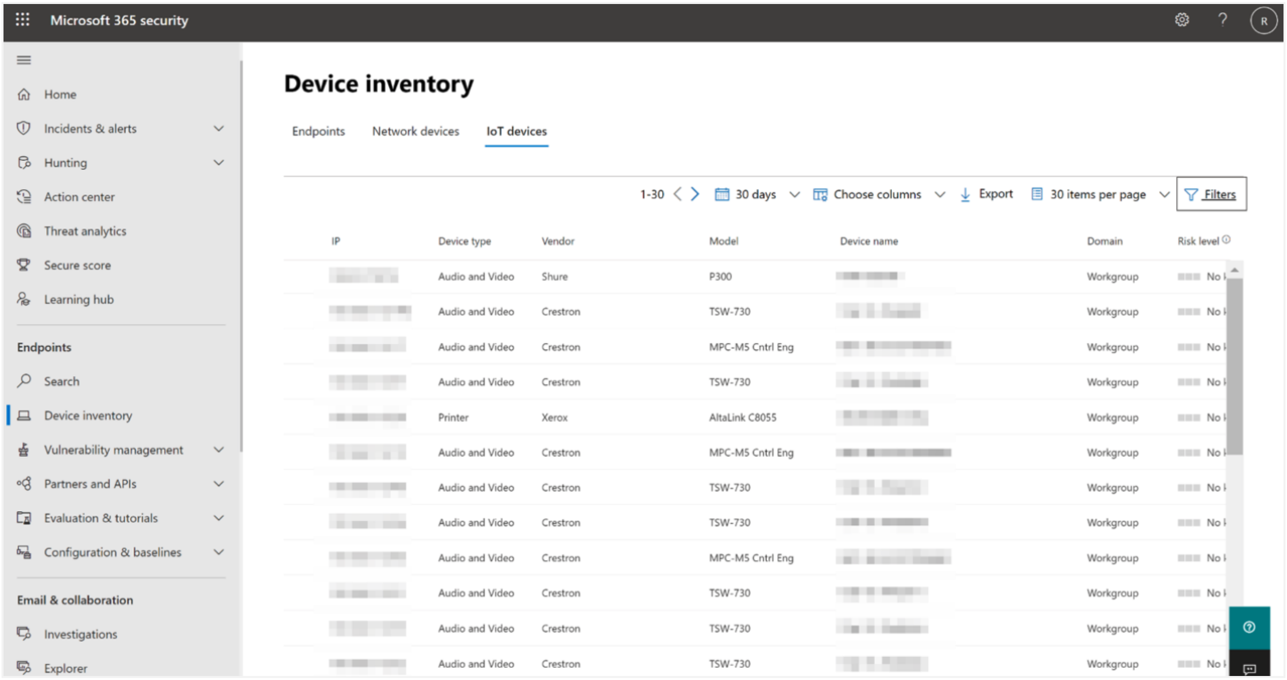
Broadest coverage for detecting IoT devices and attacks through network telemetry

Joint solution highlights

- Complete coverage and visibility of IoT/OT devices
- Risk analysis for any device on any network
- Behavioral analytics and threat intelligence to match the speed of attacks
- Visibility into multi-stage attacks across IT/IoT/OT, and mitigation with automated playbooks
- Coverage of any device type with Zeek®-based open Network Detection and Response capabilities

The number of unmanaged systems on the Internet is soaring, creating an ever-expanding attack surface. Unfortunately, most defenders lack the critical information they need to protect the IoT and OT systems in their environment.

By integrating Corelight with Microsoft Defender for IoT, Microsoft Defender for IoT can leverage the Zeek-based network signal from Corelight Sensors to perform behavioral analytics and machine learning to discover and classify IoT/OT assets, assess vulnerability and risk, and detect attacks. The result is deeper insight into IoT footprint, behavior, risk, and more efficient incident response.



Device inventory

IP	Device type	Vendor	Model	Device name	Domain	Risk level
[redacted]	Audio and Video	Shure	P300	[redacted]	Workgroup	No
[redacted]	Audio and Video	Crestron	TSW-730	[redacted]	Workgroup	No
[redacted]	Audio and Video	Crestron	MPC-M5 Cntrl Eng	[redacted]	Workgroup	No
[redacted]	Audio and Video	Crestron	TSW-730	[redacted]	Workgroup	No
[redacted]	Printer	Xerox	AltaLink C8055	[redacted]	Workgroup	No
[redacted]	Audio and Video	Crestron	MPC-M5 Cntrl Eng	[redacted]	Workgroup	No
[redacted]	Audio and Video	Crestron	TSW-730	[redacted]	Workgroup	No
[redacted]	Audio and Video	Crestron	TSW-730	[redacted]	Workgroup	No
[redacted]	Audio and Video	Crestron	MPC-M5 Cntrl Eng	[redacted]	Workgroup	No
[redacted]	Audio and Video	Crestron	TSW-730	[redacted]	Workgroup	No
[redacted]	Audio and Video	Crestron	TSW-730	[redacted]	Workgroup	No
[redacted]	Audio and Video	Crestron	TSW-730	[redacted]	Workgroup	No

Using Corelight network telemetry data and Microsoft Defender for IoT analytics, Defender for IoT can get a complete view of all IoT and OT devices. Devices are accurately classified by a machine learning engine that reviews hardware, software, behavioral and network attributes.

Joint solution value

A unified security solution for IoT and OT

Discover, classify, and contextualize all your IoT devices in a single unified solution.

Complete asset inventory in Microsoft 365 Defender

View your complete IT and IoT inventory alongside the rest of your IT devices (workstations, servers and mobile) within a single unified view.

Integrated vulnerability management in Microsoft 365 Defender

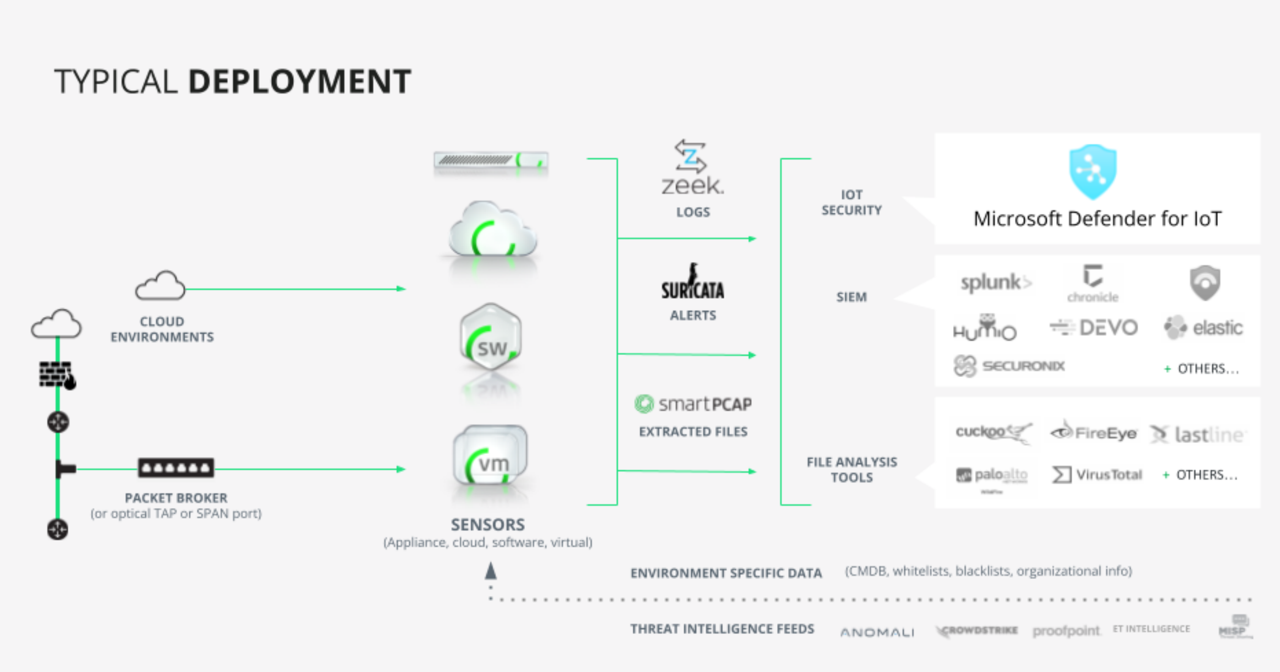
Identify and prioritize vulnerabilities and misconfigurations across all your IT and IoT devices and use integrated workflows to bring devices into a more secure state.

Prioritized incidents in Microsoft 365 Defender

View prioritized incidents that are inclusive of IT and IoT devices all in a single dashboard to reduce confusion, clutter, investigation times, and alert fatigue.

How it works

Corelight Sensors transform every network connection into Zeek data that's comprehensive, structured, and correlated. Microsoft Defender for IoT/OT uses this data for device discovery and classification, vulnerability management, and detection and response, forgoing the need to deploy Defender for IoT's IoT/OT specific network sensor.



Microsoft Defender for IoT applies its behavioral analytics and machine learning to Zeek network data from Corelight Sensors. Corelight can also send data to multiple other destinations simultaneously, including Microsoft 365 Defender, Microsoft Sentinel, Splunk, and other analytic tools.

Plus, gain all the benefits of Corelight including:

Faster answers for analysts and hunters

Capture rich, structured network data from 35+ protocols, and 400+ data fields in real time to provide additional context for Microsoft Defender for IoT alerts, accelerating incident response and dramatically expanding your threat hunting capabilities.

A single platform for NDR

Gain a platform that provides everything SecOps teams need for network detection and response, built on open standards including Zeek for telemetry, Suricata for alerts, and Smart PCAP for packets.

Integrates with your existing SOC toolset

Correlate rich network telemetry from Corelight with threat intelligence feeds for sending to multiple destinations simultaneously, including Microsoft 365 Defender, Microsoft Sentinel, Splunk, and other analytic tools.

Deeper security insights

Take advantage of unique insights that allow you to hunt for attackers without agents or decrypting network traffic, find C2 activity with over 50 unique insights that cover both known C2 toolkits and MITRE ATT&CK C2 techniques, and more.

Microsoft

Microsoft enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more.

corelight

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com | 888-547-9497