Securing OT Devices with Netskope

Solution Brief

Netskope Device Intelligence for operational technology (OT) combines best-in-class device discovery capabilities with machine learning to generate deep device insights and orchestrate actions to secure the industrial and manufacturing networks against modern-day cybersecurity threats.

Quick Glance

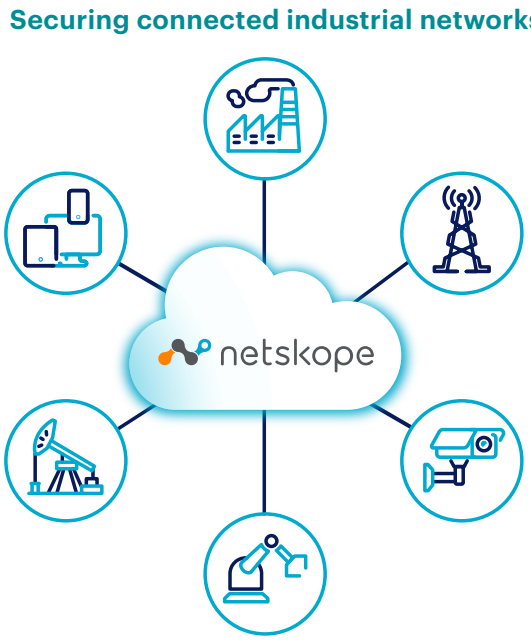
- Agentless solution providing broad visibility, extensive security coverage and controls needed for the modern IT and OT networks
- Effective monitoring of the communication patterns between the OT devices in a comprehensive manner
- Continuous detection and mitigation of device-level threats in the industrial environments
- Reduced deployment friction, enhanced device management, and alert handling capabilities with powerful third-party integrations

The Challenges

The rise of Industrial Internet of Things (IIoT) and Industry 4.0 has led to the proliferation of operational technology (OT) devices in the industrial environments, such as utilities and manufacturing plants. With more industrial systems connecting to the internet for data-driven management and efficiency, the gap between IT and OT technologies is gradually dissolving. This introduces multiple cybersecurity challenges. Traditional OT devices were not designed with security in mind. Lack of centralized management, real-time monitoring, and software updates makes these devices highly vulnerable to cyber threats. Addressing these challenges is critical to ensure the safety and reliability of OT systems, while improving their overall security posture.

The Solution

Netskope Device Intelligence provides deep visibility into OT environments and generates valuable device insights to hunt down and remediate security risks at scale. The agentless solution discovers all the connected devices, such as engineering workstations, industrial control systems, PLCs, etc., across industrial networks and analyzes their behavior using proprietary AI/ML models to generate deep contextual intelligence for cyber-physical asset management, risk assessment, mitigating cyber threats, and securing the attack surface. The solution can be deployed in both hardware and virtual appliances, and seamlessly integrates with multiple network security, asset management, vulnerability management, and threat intelligence tools, providing powerful integration capabilities to leverage investments across the security and IT stacks.



Deep visibility into the OT networks

Netskope Device Intelligence discovers all the connected OT devices and profiles every discovered device on hundreds of attributes to generate granular device context information. These attributes include device type, device function, category, OS, IP address, geolocation, ownership, risk and vulnerability information, etc. Accurate device discovery allows for deeper visibility into the asset inventory, analyzing device behavior to identify potential risks, while uncovering unauthorized devices in the network and taking necessary corrective actions. The discovery technique includes a combination of both active and passive methods, while also supporting integrations with third-party systems to pull in device details and context.

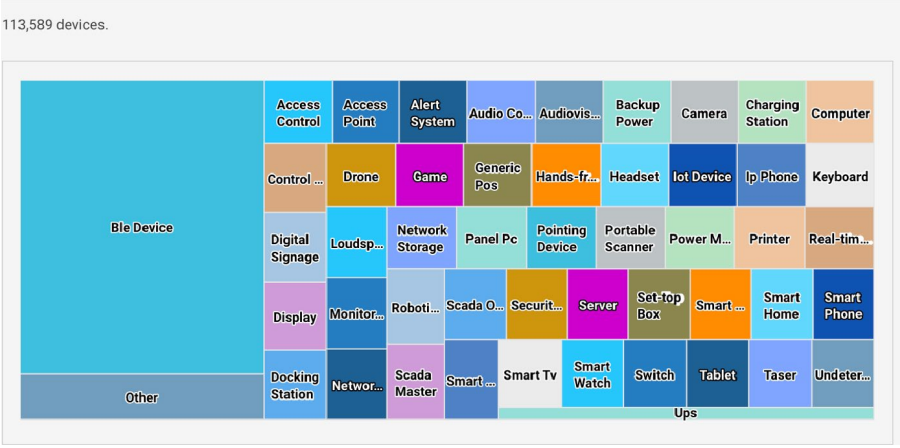


Fig. Discovered Device Types

Understand device communications

Netskope Device Intelligence provides a detailed overview of the connections between the OT devices and the supervisory networks. The connection information includes the source device, IP address, and port with the destination device, IP address, device activity (read/write/cold restart), station ID, protocol payload, and port in the transfer for analysis. The device activities are listed in chronological order. Through a topological layout, the solution provides a clear mapping of the device interconnectivity and data transmissions within the OT environment.

RECTION	SOURCE IP	SOURCE PORT	DESTINATION IP	DESTINATION PORT	SEVERITY	INCIDENT SUB TYPE	DESCRIPTION	TIMESTAMP
to_server					Low	DNP3	DNP3 Read-Var Requ...	12 Jun 2023 11:19:32 AM
to_client					Low	DNP3	DNP3 Solicited Resp...	12 Jun 2023 11:19:32 AM
to_server					Low	DNP3	DNP3 Read-Var Requ...	12 Jun 2023 11:19:32 AM
to_server					Low	DNP3	DNP3 Read-Var Requ...	12 Jun 2023 11:19:32 AM
to_client					Low	DNP3	DNP3 Solicited Resp...	12 Jun 2023 11:19:32 AM
to_server					Low	DNP3	DNP3 Read-Var Requ...	12 Jun 2023 11:19:32 AM
to_server					Low	DNP3	DNP3 Read-Var Requ...	12 Jun 2023 11:19:32 AM
to_server					Low	DNP3	DNP3 Read-Var Requ...	12 Jun 2023 11:19:32 AM
to_client					Low	DNP3	DNP3 Solicited Resp...	12 Jun 2023 11:19:32 AM
to_server					Low	DNP3	DNP3 Read-Var Requ...	12 Jun 2023 11:19:32 AM

Fig. Device Communication Details

Detect and prevent known threats

With more and more OT devices becoming part of the connected industrial ecosystem, the threat landscape has dramatically expanded and bad actors are constantly launching sophisticated attacks to infiltrate critical systems. Netskope Device Intelligence continuously monitors the OT devices for any behavioral anomalies, malware, and threats. Any indicator of compromise detected is immediately reported and the risky device is isolated (blocked/quarantined) to mitigate the threat.

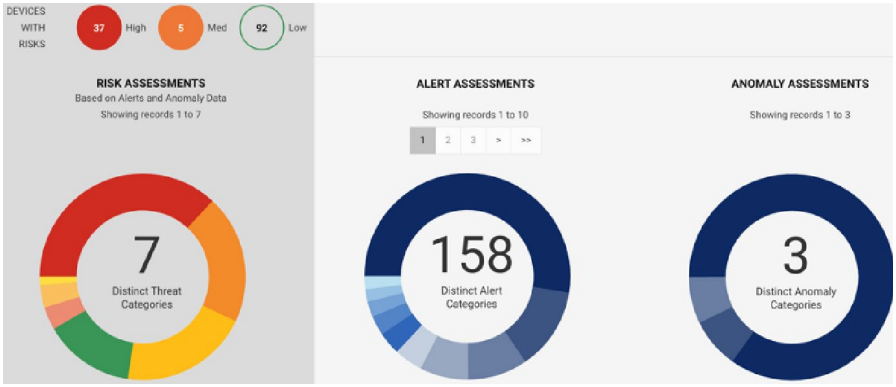


Fig. Device Security Dashboard

Leverage investments with powerful integrations

Security event alert overload in OT environments can lead to alert fatigue within the security and operations team and result in breaches caused by missed alerts. Netskope Device Intelligence seamlessly integrates with leading SIEM and SOAR solutions and feeds them with deeper device insights, empowering the SOC teams with enriched threat intelligence. Advanced correlation capabilities significantly reduce the threat hunting time and allow security personnel to identify potential threats that may have been missed during manual inspection. The enriched SIEM alerts are ingested into SOAR playbooks for automating threat responses and improving the security hygiene of the OT environments.

BENEFITS	DESCRIPTION
Rich device telemetry	Provides comprehensive visibility into the industrial networks with deep insights into every connected device. User-defined device tags and groups further customize the device context for every business need and requirement.
Secure the critical infrastructure	Effectively identifies and safeguards industrial networks against a wide array of known threats that can propagate through connected OT devices. By continuously evaluating device risk scores based on detected anomalies and alerts, context-aware and real-time decisions are made to isolate high-risk devices and mitigate potential threats.
Drive IT/OT convergence	Allows the management of all connected enterprise IoT and OT devices from a single interface, allowing streamlined visibility, unified policy enforcement, and incident management of devices operating on different protocols, across IT and industrial deployments.
Align with SASE vision	Aims to bring the OT devices under Netskope's truly unified Secure Access Service Edge (SASE) framework for delivering fast and reliable connectivity to every OT asset, with complete zero trust security services delivered from the cloud.