Securing the Convergence of IT and OT with Cubro and Forescout

Joint Solution Brief

In today's interconnected world, ensuring robust cybersecurity measures in both IT and OT landscapes is paramount. With the increasing sophistication of cyber threats, organizations must prioritize network security to safeguard against potential attacks. By leveraging advanced solutions like Forescout and Cubro, companies can establish comprehensive protection across their entire network infrastructure.

Challenges to Address

Securing both IT (Information Technology) and OT (Operational Technology) environments poses several challenges for companies that must address the distinct security challenges of both IT and OT environments to safeguard their operations, data, and reputation from cyber threats.

Integration Complexity: Integrating OT systems with traditional IT networks can create security gaps that hackers can exploit. Managing and securing a complex network with varying operating systems and abilities to stay current can be challenging and increase the risk of security incidents.

Remote Access: Providing remote access to IT and OT systems for maintenance or monitoring purposes can increase the attack surface and make the network more vulnerable.

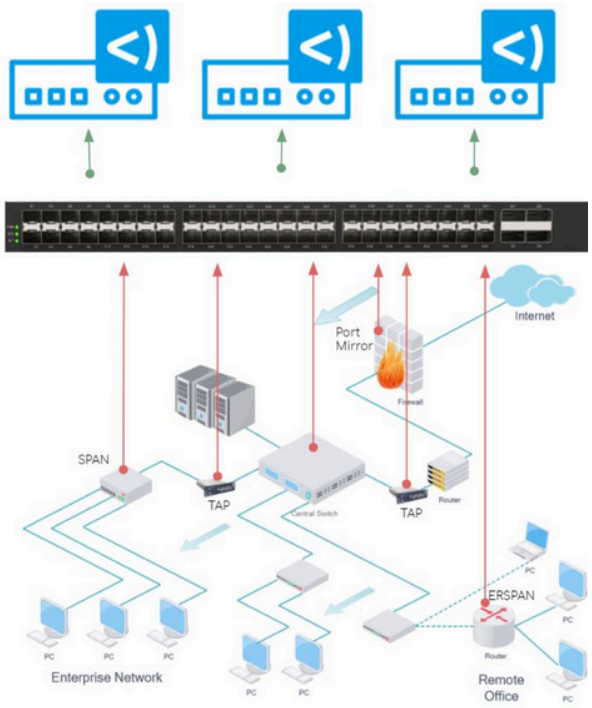
Third-Party Risks: Both IT and OT environments often rely on third-party vendors for equipment and services, which can introduce additional security risks if not properly managed.

Regulatory Compliance Requirements: Ensuring compliance with industry regulations and data protection laws adds an extra layer of complexity to network security efforts.

Limited Visibility: Monitoring and managing security incidents in converged IT and OT environments can be challenging due to limited visibility into network traffic and system behavior.

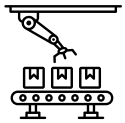
Architecture

Cubro enhances visibility with a passive network TAP, ensuring fail-safe access to network data which is sent to packet brokers that aggregate and filter the data before sending to Forescout sensors on the network. Forescout then analyzes this data to determine potential threats in the environment as well as provide detailed status and health of equipment.



Example Use Cases:

Cubro's aggregation and filtering of data provides reduced noise and targeted intel on activity in both IT and OT environments.



Manufacturing and warehouse facilities depend on effectively automated processes with as minimal down time as possible. Cubro enhances Forescout data to help provide valuable insights into assets needing updates, diagnostics, and misconfigurations of equipment.

Hospitals have a combination of offices and labs creating a complex IT and OT network infrastructure. Using Cubro's enriched network telemetry, Forescout can provide detailed information about all assets on the network as well as segmentation of these varying items for enhanced security.

Advantages

- **Enhanced visibility without latency or disruption:** The integration of Forescout and Cubro solutions enhances visibility into network traffic, enabling easier detection and response to potential threats in real-time. This increased visibility can help organizations proactively secure their IT and OT environments against cyber threats.

- **Reduced attack surface:** Implementing Cubro's TAPs for data sent to Forescout sensors allows for monitoring of incoming and outgoing traffic simultaneously, providing a comprehensive view of network activity. Threats from both external and internal sources are considered, leading to a more secure environment with a minimized attack surface.

- **Adherence to Compliance Needs:** Both IT and OT environments have guidelines and regulations depending on the industry, such as NIST Special Publication 800-82, IEC 62443, and ISO 27001. Visbility in crucial in determining asset inventory, health status, and potential threats in the environment.

About Forescout

Forescout is the only automated cybersecurity vendor with a single platform for continuously identifying and mitigating risk across all managed and unmanaged assets – IT, IoT, IoMT and OT – from campus to data center to edge. For more than 20 years, we have delivered cybersecurity innovations that protect many of the world's largest, most trusted organizations in finance, government, healthcare, manufacturing and other industries.

The Forescout Platform delivers comprehensive capabilities for network security, risk and exposure management, and extended detection and response. With seamless context sharing and workflow orchestration via ecosystem partners, it enables customers to more effectively manage cyber risk and mitigate threats.

About Cubro

Cubro delivers innovative solutions which will assist you in bringing your network performance and security monitoring efforts to their peak level. Our network visibility solutions help to unlock valuable insights into your network traffic.

We are a world-leading manufacturer and supplier of network visibility products like Network TAPs, Network Packet Brokers, Bypass and Probes that provide network monitoring, security and analytics visibility solutions for Service Provider and Enterprise organizations.

Cubro has a global presence with offices in different geographic locations to serve customers across different time zones. Over the years, we have expanded our reach and impact in all continents. As a result, we offer seamless and timely support to our customers across the globe.

Learn More

Schedule a demo at forescout.com | cubro.com