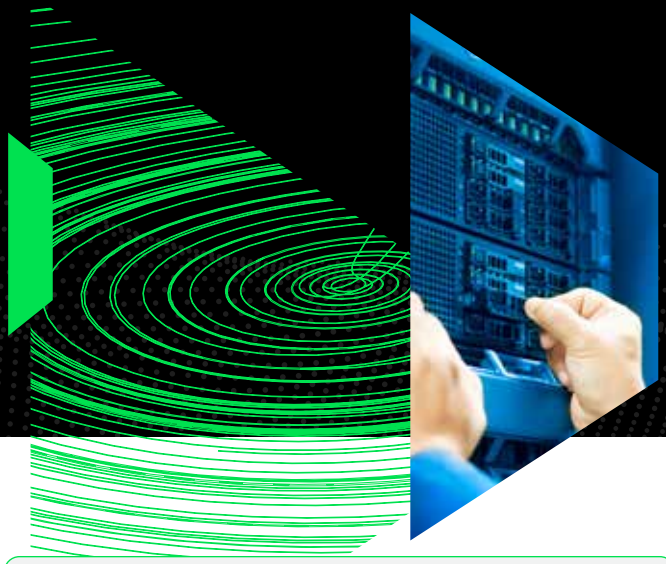
OPSCURA

Joint Solution Brief

CLAROTY



Extend Your Defenses to Protect Against OT Cybersecurity Threats

Cybersecurity is an ongoing practice, much like operations, and requires varied types of defensive layers depending on your site's objectives and metrics. Opscura specializes in protecting and connecting brownfield and greenfield industrial assets and their critical related processes. Assets can include PLCs, RTUs, IEDs, and PCs, and any photovoltaic panels, robots, kilns, and pumps connected to them.

Partnering with operational threat monitoring tools, such as Claroty's Continuous Threat Detection (CTD) solution, Opscura solutions extend industrial cybersecurity from identifying and detecting threats, to live protection of OT assets and data. Opscura uses cloaking, segmentation, and other methods to protect deep level industrial processes from the risk of unauthorized access, operational disruption, data theft, and hacker reconnaissance. Opscura's virtual SPAN port capabilities make it easy to provide network data to Claroty CTD, even in challenging and complex network environments, accelerating time-to-value of deployments.

Easily Enrich Threat Monitoring Data

Claroty's state-of-the-art threat monitoring requires data for effective analysis and follow-up mitigation. Claroty Continuous Threat Detection (CTD) provides visibility across the OT landscape of assets, providing a rich management interface to identify and detect threats. Opscura provides deeper-layer data from Purdue Model Level 2 to enhance Claroty visibility. Opscura can also control communications between network segments, providing only the data the operator deems safe to share.

The two solutions can be deployed either in sequence, with Opscura first to segment and gather data and Claroty second to perform monitoring, or simultaneously as a plant security upgrade during regular maintenance cycles.

Joint Solution Benefits

Opscura reduces operational risks by protecting vulnerable legacy industrial assets and data, eliminating deeper-level attack surfaces, and enriching threat monitoring data with deeper visibility. Together with Claroty, Opscura provides a complete monitoring and protection solution for OT environments.

- Detects threats for the entire OT environment, without requiring taps or network reconfiguration
- Continuously updates with the latest threat information
- Protects OT assets, isolating them from threats
- Enables operators to quickly identify at-risk equipment and safely isolate it

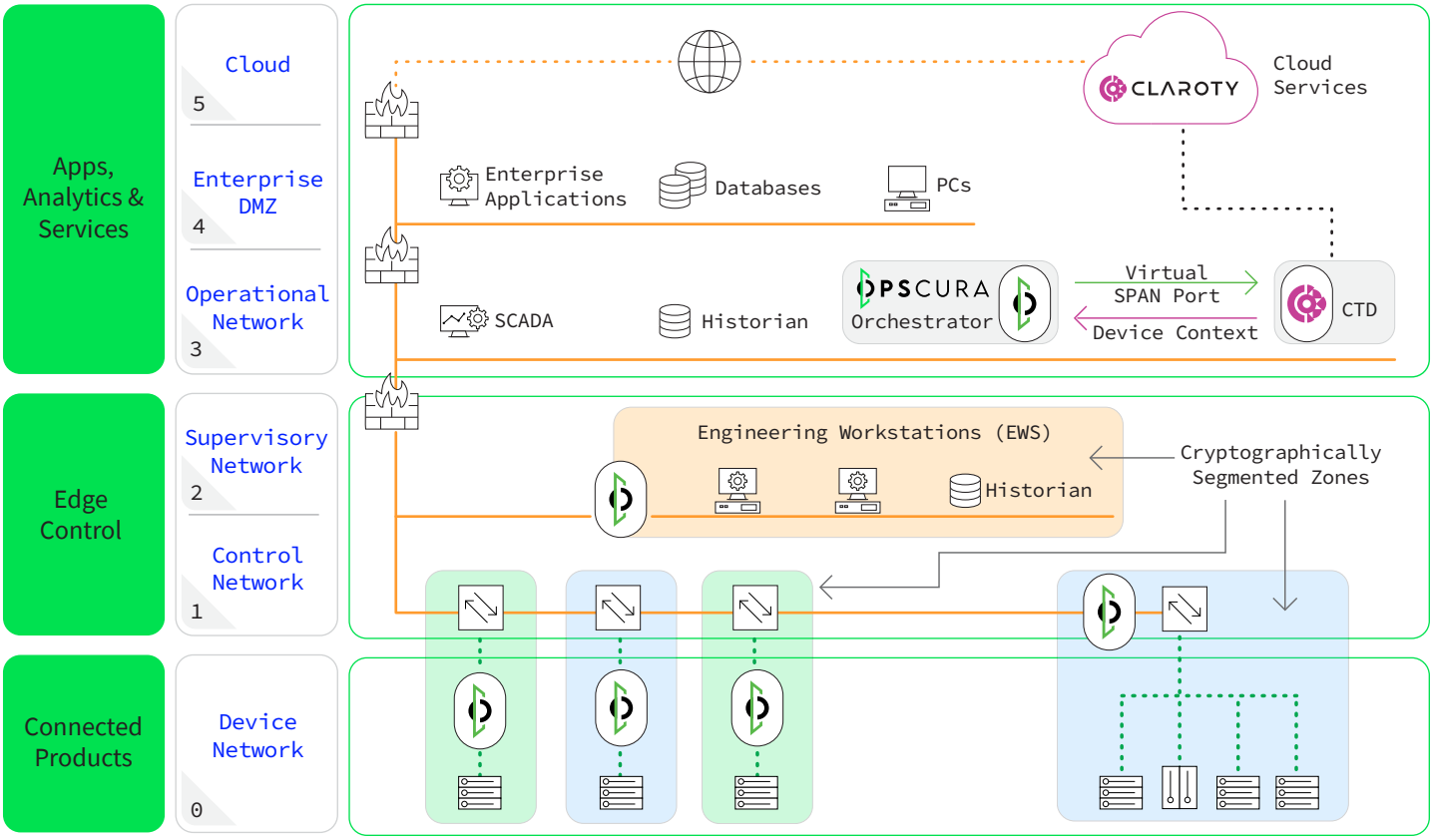
Opscura Solution Benefits

- Easy to deploy in both OT and IT environments
- Deploys transparently without rearchitecting the network, reconfiguring switches or routers, or changing IP addresses
- Cloaks traffic from observation, preventing attacker discovery and reconnaissance
- Shields vulnerable assets from attack
- Allows selective communication between IT and OT assets, while maximizing OT security
- Can be deployed without disrupting time-critical, latency sensitive processes
- Deploys quickly without requiring IT networking experts
- Enables network monitoring and observability tools
- Enforces zero-trust access to OT assets

Opscura Solution Features

- Available as an industrial appliance with hardware Ethernet bypass or a virtual machine
- Operates at Layer 2
- Transparent encrypted tunnels
- High-speed low-latency encryption
- Integral Layer 2 and Layer 3 filtering
- Temporal ports
- Integral network discovery tools
- Virtual SPAN port

Joint Solution Architecture



The architecture diagram depicts Opscura's solution deployed to protect an industrial control systems network. Three cryptographic segments have been created: orange for engineering workstations, and blue and green for different plant processes. Opscura allows the operator to easily control what traffic is allowed to flow between and within the different cryptographically segmented zones. Should an attacker penetrate the IT/OT (Level 3.5) firewall, the traffic is fully encrypted, cloaking it from observation. Traffic from outside the zones is rejected, preventing access to sensitive equipment and protecting OT assets.

As operators monitor their OT network for threats and vulnerabilities, Opscura mirrors all traffic observed on different zones to Claroty's Continuous Threat Detection (CTD) solution. Clear-text traffic from the zones is compressed, encrypted, and transmitted to the Opscura's Orchestrator, which replays it out a dedicated SPAN port to CTD. Connecting Opscura to CTD provides the Claroty solution the data it needs to be effective – data that is often unavailable because of the limitations of network equipment common in industrial environments.

Industrial assets identified by Claroty as vulnerable can be placed in dedicated zones or protected with additional filtering. Assets identified by Claroty as malicious can be prevented from accessing protected assets. Claroty CTD and Opscura solutions together enable operators to know what is occurring on their network, deeper, and take actions.

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

Contact Claroty

For more details,
claroty.com/contact-us

About Opscura

Opscura protects and connects industrial networks with easy-to-use innovations that are safe to use deep within operational infrastructure. Validated by global partners such as Schneider Electric, Opscura reduces operational risks by protecting vulnerable legacy industrial assets and data, eliminating deep-level attacker footholds, and enriching threat visibility data. Brownfield and greenfield global customers rely on Opscura for OT cloaking, isolation, and Zero Trust authentication, together with simplified IT-OT connectivity.

Learn more about Opscura or request a demo at www.opscura.io

Contact Opscura

For more details,
reach us at
contact@opscura.io