OPSCURA

FORTINET

Joint Solution Brief

Expand Firewall Reach and Efficacy with Safe Deep-Level OT Access

Today's operators rely on multiple lines of defense to reduce the risk of downtime, and that includes industrial firewalls. Opscura works with market-leading firewall technology from Fortinet to expand security IT and network Level 3.5 traffic monitoring all the way down to Level 2. Opscura's approach to protect and connect at the deepest levels of your network means you can expand your security and data types to increase operational resilience.

A Joint Solution

The Fortinet Security Fabric brings together the concepts of convergence and consolidation to provide comprehensive cybersecurity protection for all users, devices, and applications and across all network edges. Fortinet provides secure networking, threat intelligence, network, and security operations solutions.

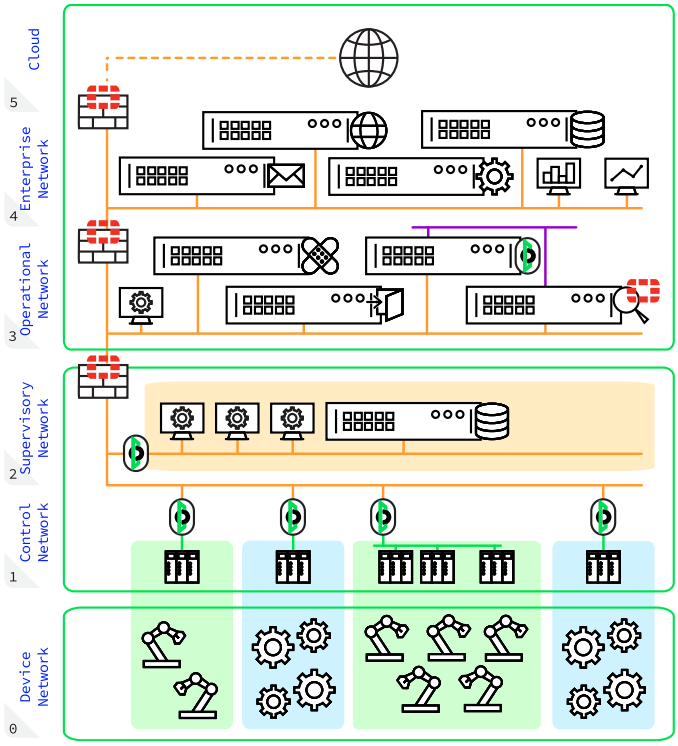
For customers with industrial control systems, Fortinet firewalls are often deployed at Purdue Model Level 3 or 3.5 and above to block or allow traffic based on anomaly detection, rules and other customer criteria. Customers may also use Fortinet management consoles and seek to act on Fortinet threat research.

Opscura provides deeper-layer OT network data from Purdue Model Levels 1 and 2 and OSI Model Layer 2 to enrich Fortinet Level 3 and 3.5 (and up) firewall capabilities. In addition, Opscura provides cloaking, cryptosegmentation, and other methods to protect industrial processes from the risk of unauthorized access, operational disruption, data theft, and hacker reconnaissance.

Opscura can also control communications between OT network segments, or IT-OT networks, providing only the data the operator deems safe to share to other security solutions.

Fortinet and Opscura solutions work together to safely share important OT data without disrupting critical operations or exposing unnecessary data that attackers could exploit. Together, they reduce risk and improve operational resilience.

Joint Solution Architecture



Deployed together, Fortinet and Opscura provide a comprehensive solution for both greenfield and brownfield deployments. Fortinet provides industry-leading firewalling capabilities, with comprehensive management, network monitoring and analysis. As shown above, FortiGate firewalls protect and control traffic from the Cloud, the Enterprise Network, the Operational Network, and the Supervisory Network.

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 protects the deep layers of the OT network, using cryptography to segment it into separate zones and to mask foreverday vulnerabilities in legacy plant assets. Opscura's network cloaking prevents surveillance, thwarting malware and attackers from completing their reconnaissance.

Working together, Opscura can provide packet streams to FortiAnalyzer and event messages to FortiSIEM. In addition to the natural fit with FortiGate firewalls, Opscura's cryptosegmentation can be deployed in conjunction with Fortinet switches as well as in mixed environments with legacy network equipment.

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 Fortinet, Opscura provides a complete firewalling 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

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