OPAQ®
Security without Boundaries

DATA SHEET

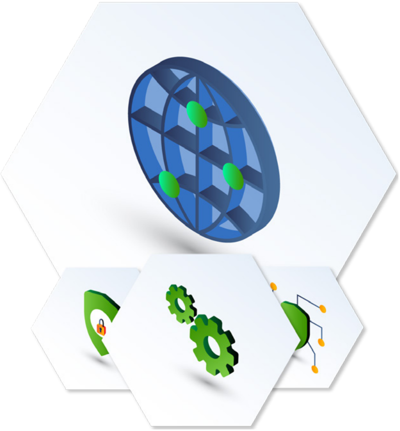
Stop Malicious Lateral Spread with Software-Defined Segmentation

OPAQ Endpoint Control

Stopping the lateral movement of infected machines isn't easy. In just four days in 2018, WannaCry was able to knock out 200,000 computers across 150 countries, including some hospitals.

Organizations and their security IT proxies need to see a threat agent in order to stop it. They need visibility into how endpoints are behaving and what network processes they are running. For example, they must be able to discover why an employee's laptop is initiating remote desktop connections across the entire network. They also need to be able to immediately isolate endpoints that are acting suspiciously or running malware, whether inside the cloud or the private network.

OPAQ Endpoint Control gives you the visibility to see suspicious activity, quickly search for malicious network processes across your user base, and shut down network communication to and from infected endpoints.



Network Segmentation at the Endpoint

Don't let compromised endpoints infect your network and data

The network perimeter flexes constantly, ranging into unchartered territories, and firewalls can only stop so much. This is why protecting your internal network assets is essential.

OPAQ Endpoint Control enables security management teams to more easily control what their local users' devices connect to. It also protects your hosted network servers as well as servers hosted in the cloud, thanks to security-as-a-service that can be easily implemented to segment your local, hosted, and cloud-based assets (i.e., microsegmentation).

OPAQ Endpoint Control provides visibility and control to reduce attack surface and improve incident response. With it, organizations and managed service providers can gain greater visibility into lateral east-west traffic, reduce response time, and apply Zero Trust security best practices through segmentation – all from the OPAQ cloud console. Features include:

- Host asset inventory
- Host group and user group based software-defined network segmentation
- Instantaneous host quarantine
- Endpoint analysis console

Why OPAQ Endpoint Control?

- Simple policy logic for stopping users from talking to each other over ports commonly used for malicious propagation
- Network topology and analytic views that show who's talking to who and what network processes are running on which endpoint
- Greater visibility into lateral east-west traffic for optimum network performance and incident response time
- Easier network segmentation / microsegmentation, which empowers you to structure traffic smartly to protect key enterprise assets from impact
- The ability to apply Zero Trust security best practices
- Advanced endpoint security in minutes rather than months, managed through a single cloud console

Supporting Operating Systems

- Windows 64-bit workstation: 7, 8.1, 10
- Windows Server 64-bit: 2012, 2016, 2019
- MacOS 10.11+
- Linux versions:
  - Debian 6+
  - Ubuntu 10+
  - CentOS 5+
  - Red Hat Enterprise Linux (RHEL) 5+
  - Oracle Linux 5+
  - Fedora Core 17+

Connection Types

- TCP 2125(SSL), TCP 443(SSL)

About the OPAQ Cloud

OPAQ is the premier network security cloud company. The OPAQ Cloud empowers organizations with Fortune 100-grade security-as-a-service on infrastructure optimized for security and hyperscale performance. With OPAQ, service providers and their customers can centrally monitor security performance and compliance maturity, generate reports, manage security infrastructure, and enforce policies – all through a single cloud console. For more information, visit opaq.com.