OPAQ
Security without Boundaries

PRODUCTS

OPAQ Endpoint Protection

Good segmentation of the internal networks is a security best practice that organizations struggle to achieve. Most security events begin with the workstation, where the user is interacting with the online world. If a user clicks on the wrong link, to proliferation of Ransomware or the lateral east-west spread of malware across the internal network, OPAQ's software-defined network segmentation is a groundbreaking approach that provides unparalleled visibility and control over workstations and servers. It enables organizations to provide users with access to the resources they need while reducing attack surface and locking down attack vectors.

Endpoint Inventory, MDR, and Response From the OPAQ Cloud

Managed Detection and Response services need powerful capabilities on the endpoint to provide the visibility needed to investigate threats and rapidly contain them. OPAQ Endpoint Protection goes beyond typical Endpoint Detection and Response (EDR) solutions, adding continuous HW/SW asset inventory, software-defined network segmentation and instantaneous quarantine capabilities — all essential functions required to increase visibility and reduce attack surface area and response time.

No more reliance on manual processes that yield slow response times.
With **OPAQ Endpoint Protection** , you have the ability to:

- **Continually inventory** all devices communicating on your network.
- **Gain visibility** into east/west traffic and investigate incidents.
- **Limit attack surface** by segmenting network; prevent threat propagation.
- **Take action** to quarantine suspicious hosts using the cloud workbench.

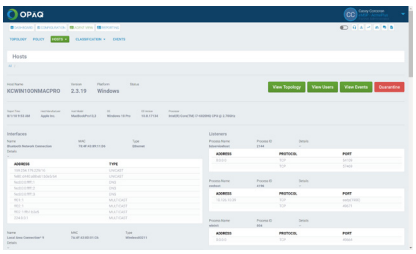
OPAQ Endpoint Protection is part of the OPAQ Cloud enterprise-grade security platform that also includes Firewall-as-a-Service, Cloud SIEM and Web Application Firewall – integrated and delivered via OPAQ's fully encrypted, secure SD-WAN.

FEATURES OF OPAQ ENDPOINT PROTECTION

PRO	ADVANCED
✓	✓

Host hardware and software asset inventory

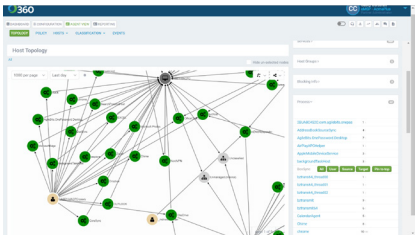
- Automatically discover hardware and software across your network
- Identify IoT, BYOD, and other unmanaged devices
- Quickly and easily report on asset details - see everying in a single view



PRO	ADVANCED
✓	✓

Endpoint dashboard and host analysis

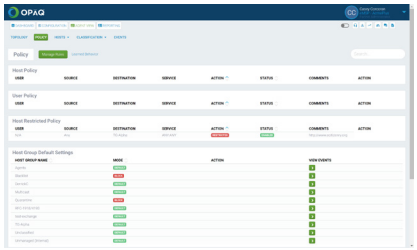
- Real-time topology views enable you to see which assets are communicating with each other
- One-click drill-down capability can zero in on individual hosts, users, process names, and TCP/IP services
- Contain known or suspicious infected hosts with a click of a button



PRO	ADVANCED
	✓

Software-Defined Network Segmentation*

- Define policies that prevent lateral east-west spread of malicious threats throughout your network
- Users on the same local network segment can be granted access to different resources depending upon their job function.
- Enforce access control based on user identity, device state and multifactor authentication
- Seamless integration with OPAQ's FWaaS for comprehensive policy enforcement



**Available only with FWaaS Advanced*

About the OPAQ Cloud

OPAQ is the premier network security cloud company. The OPAQ Cloud empowers midsize enterprises with Fortune 100-grade security-as-a-service on a fully encrypted SD-WAN optimized for speed and performance. With OPAQ, service providers and their midsize enterprises are equipped with a simplified ability to centrally monitor security performance and compliance maturity, generate reports, manage security infrastructure, and enforce policies – all through a single interface. For more information, visit opaq.com.

To learn more, visit *www.opaq.com/solution*