OPAQ®
Security without Boundaries

DATA SHEET

The OPAQ Cloud Platform

Network Security Made Simple

The OPAQ cloud platform fully integrates networking and security enabling partners to monitor, deliver, and manage comprehensive network security-as-a-service from a single cloud console. This makes network security:

- Easier to manage and control
- Scalable and adaptable
- Affordable and effective

The OPAQ cloud platform consists of 3 core components:

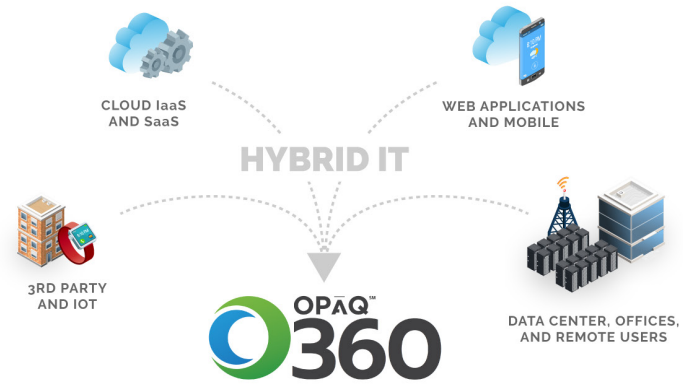
1

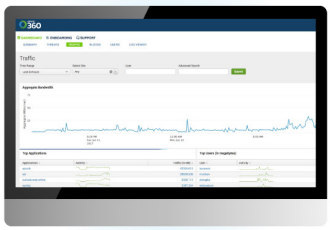
OPAQ 360 Cloud Console

Automation for a Cloud-First World

We've combined networking and security into a single cloud service that can be centrally monitored, analyzed, managed, and reported all from the OPAQ 360 cloud console. All the complexity you would typically associate with network security has been abstracted and automated, simplifying your ability to reduce and manage risk, instead of managing dozens of products. OPAQ 360 cloud console capabiltiies include:

- Service deployment
- Security policy configuration
- User and endpoint management
- Analytics and reporting
- Service ordering
- One-touch 24/7/365 support





Enterprise-Grade Security

2

Fully Integrated Protection from the OPAQ Cloud

Firewall-as-a-Service

Advanced Next-Generation Firewall

protection powered by Palo Alto Networks delivered by the automation and agility of the OPAQ Cloud.

Features include: network IPS/IDS, network anti-virus/spyware/malware, network URL inspection and filtering, DNS sinkholing, network encrypted packet inspection (SSL decryption), Zero-Day packet inspection and threat prevention, OPAQ Cloud edge connect, NG firewall policy and configuration management, network IP inspection and filtering, network file auditing and blocking, secure cloud access, directory integration, security log forwarding, web application firewall, reduced Internet exposure, carrier-grade upstream transit capacity in-excess of 150Gbps, and continuous analytics and reporting

Endpoint Protection-as-a-Service

Always-on protection follows users wherever they go, reduces attack surface, and improves incident response.

- **Endpoint Protect** features include: network IPS/IDS, network anti-virus/spyware/malware, external IP inspection and filtering, URL inspection and filtering, Zero-Day protection, reduced Internet exposure, carrier-grade upstream transit capacity in excess of 150 Gbps, and continuous analytics and reporting

- **Endpoint Control** features include: host hardware and software asset inventory, host group and user group based software-defined network segmentation, instantaneous host quarantine, endpoint analysis console with continuous analytics and reporting

- **Endpoint Defend** features include: prevents known and unknown malware from infecting endpoints, deep-intelligence driven analysis, scans for dormant malware before it is executed, zero-day protection

OPAQ Cloud Network

3

Purpose-Built for Security and Performance

- OPAQ operates its own global IP backbone (AS25885) with network Pods at major carrier hotels around the world.

- Our network is among the top 8% most interconnected in the world. We combine multiple high-performance transit providers with approximately 180 private peering relationships with Amazon, Google, Apple, Facebook, Netflix, and many others

- More than 60% of network traffic never touches the Internet — it takes the fastest possible route to its destination

- IP transit providers include Internap and NTT America

- OPAQ's routing policy dynamically leverages the best Internet paths available, and makes more than 1 million route changes daily. This allows OPAQ to reduce standard Internet latency by as much as 35 milliseconds per packet round-trip time on average

- Every OPAQ Pod routing policy is operated independently, allowing customers to achieve a highly available connection to the OPAQ Cloud. When a customer connects to multiple OPAQ Pods, OPAQ provides a high-availability option with faster failover times

- Traffic going between Pods utilizes our dedicated backbone circuits, which are maintained by OPAQ engineers — by avoiding the public Internet, we reduce Pod-to-Pod latency while increasing reliability