Endpoints Need More Than Just Antivirus Protection

OPAQ Endpoint Defend

With the increasing adoption of distributed Internet-connected devices, the average organizational attack surface is aggressively expanding. We're talking about the growing number of mobile devices being used outside the private network where they are unprotected by enterprise firewall or network security policies.

By itself, traditional, static antivirus hasn't been enough to stop malware and ransomware at the endpoints. To beat the antivirus protection, the hacker just needs to add a character to the code and recompile. Meanwhile, basic antivirus agents are not intelligent enough to share information with each other, or with other analytical security tools, and a hack or breach can turn into an expanding infection or loss of network control.

Prevent Endpoint Attacks Before They Get Started

Stop attacks before they get started to avoid the malware's spread and the compromise of company and customer data.

OPAQ Endpoint Defend is a security-as-a-service (SECaaS) software agent rapidly deployed to your end-user computing devices to provide advanced remote security beyond antivirus and firewall protection.

OPAQ Endpoint Defend is powered by Palo Alto Networks Traps™, which combines powerful endpoint protection technology with automated endpoint detection and response (EDR) capabilities. OPAQ Endpoint Defend enables security teams to automatically protect, detect, and respond using machine learning, threat intelligence, and AI to stop attacks on endpoints before they can be fully executed. Features include:

- Behavior-based ransomware protection, which safeguards the endpoint against encryption-based malware
- Threat intelligence from Palo Alto Networks WildFire® malware prevention, which quickly identifies and prevents threats
- Network sandboxing with static, dynamic, and bare-metal malware analysis
- The ability to scan for dormant malware before it is executed, using machine learning-powered malware examination flow and local analysis
- Pre-exploit protection, which blocks reconnaissance and vulnerability-profiling techniques before an attack can occur
- Technique-based exploit prevention that works to stop known and zero-day exploits

Why OPAQ Endpoint Defend?

- Automate endpoint detection and response
- Reduce the organizational attack surface by preventing known and unknown malware from infecting endpoints
- Prevent the launching of malicious executable files, DLLs, and Office macros
- Manage potentially complicated endpoint defense easily through a single cloud console
- Affordable cloud-based security – predictable per user monthly rate; no need to invest in expensive, complex security infrastructure
- Simple to deploy and manage – easy 5-minute download of the OPAQ endpoint agent.

Supporting Operating Systems

- Windows 64-bit workstation: 7, 8.1, 10
- Windows Server 64-bit: 2012, 2016, 2019
- MacOS 10.11+

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.