FORTICLIENT CONNECTS VULNERABLE ENDPOINTS TO NETWORK SECURITY

EXECUTIVE SUMMARY

Endpoints remain one of the primary attack targets for cyber criminals because of the valuable data and credentials they contain. In response, Fortinet's FortiClient integrates endpoint security with the broader network security architecture of the Fortinet Security Fabric. The deep connection between FortiClient and the Fortinet Security Fabric supports sharing of endpoint telemetry and bidirectional application of real-time threat intelligence. This, in turn, facilitates greater visibility of all endpoint devices, enhances enterprise security posture, and automates security responses and workflows. And this results in more effective and efficient protection that saves security teams both time and money.

In a 2018 SANS Institute survey, 42% of respondents report that their endpoints have been exploited in the last year—and 20% don't even know if they'd been breached.[1] Endpoint devices represent the most common targets for cyber threats. In addition to data stored locally on the computer, a compromised laptop provides a valuable access point for the attacker. Using it as an initial foothold, attackers can use its credential to move laterally to higher-value targets, or to infect more endpoints on the network and inflict greater damage.

While endpoint protection (EPP) has improved in recent years, a majority of endpoint security solutions still operate in silos, disconnected from more robust network security defenses. This separation hinders visibility and potentially slows threat responses. Integrating endpoint and network security can offer many benefits—but not all levels of integration are the same.

FORTICLIENT PROVIDES BROAD VISIBILITY AND CONTROL

To address this fundamental problem, Fortinet's FortiClient solution connects with key Fortinet Security Fabric elements (e.g., FortiSandbox, FortiGate, FortiAnalyzer) to enhance endpoint visibility, share endpoint data, and exchange real-time threat intelligence across the organization.

This design enables a better holistic security posture against attacks by providing risk-based visibility, compliance control, vulnerability management, and automation—all within an open-solution ecosystem.

Effective endpoint security requires comprehensive optics and control, both on- and off-network. FortiClient delivers broad visibility of both hosts and endpoint devices. It assesses an endpoint's risks and security profile before it can connect to the network, enabling clear, policy-based access controls.

Risk Awareness. FortiClient establishes risk awareness by sharing real-time endpoint telemetry with security solutions across the broader Security Fabric architecture. This data includes device information, user identities, protection status, unpatched vulnerabilities, endpoint events, and more.

For example, FortiClient sends endpoint telemetry to FortiAnalyzer, which collects logs and events information from all Security Fabric components and incorporates global threat intelligence—including an indicator of compromise (IOC) feed—from FortiGuard Labs. By connecting the dots between individual endpoint data points, security leaders can have a more complete picture of endpoint security and receive alerts to potential compromises.

Endpoint Security Hygiene. Once endpoint telemetry is shared, the next step is enforcing proper controls. To strengthen the enterprise's overall security posture, endpoints must be hardened and the correct procedures must be applied to maintain security hygiene.

The integration between FortiClient and FortiGate enables network security administrators to enforce compliance control, so that only devices that meet security standards can access the network and applications. FortiClient's vulnerability management capabilities prioritize vulnerabilities based on criticality and provide flexible remediation options, including automatic patching of software/operating systems. The system also automatically rescans and verifies that patches are successfully applied and it flags failed patches. These features help eliminate defensive gaps while reducing the churn of manual processes for under-resourced IT teams.

FORTICLIENT SECURES ACCESS WHILE REDUCING REAL-TIME THREAT EXPOSURE

Multiple FortiClient features—including built-in VPN, single sign-on (SSO), and two-factor authentication—provide additional layers of security access controls that limit organizational risk while ensuring security best practices. FortiClient exchanges real-time threat intelligence from individual devices across all other endpoints and security elements within the Security Fabric (e.g., FortiGate, FortiAnalyzer, FortiSandbox) to block unknown (zero-day), advanced, and targeted threats.

Threat Intelligence Sharing. FortiClient automatically submits unknown or suspicious objects to FortiSandbox for detailed analysis. Once FortiSandbox identifies a threat, all FortiClient-protected endpoints and other elements across the Security Fabric become aware of the problem—providing enterprise-wide protection in real time, regardless of where the threat is first discovered.

For example, FortiSandbox receives a potentially malicious script attachment from an email. Sandboxing analysis shows that this script would reach out to a command-and-control (C&C) server and download an additional payload, such as a remote access Trojan. The tight integration between FortiClient, FortiSandbox, and the rest of the Fabric architecture allows for almost instantaneous dissemination of intelligence regarding the original script, the malicious URL, and the payload across the entire organization. Not only is the initial malicious email threat blocked at email and web gateways but all endpoints are made immediately aware. This threat intelligence exchange protects the enterprise across all threat vectors and dramatically shrinks the enterprise attack surface.

FORTICLIENT AUTOMATES ACTIONS AND WORKFLOWS

FortiClient helps transform network security by unlocking automated workflows and processes related to threat intrusion detection, prevention, and remediation. As a result, security teams and network engineering groups can do more with less. Integrated sharing of real time threat intelligence across all endpoints and security elements also unlocks the power of automated defensive actions, which can almost instantly contain threats and control outbreaks.

Automated Incident Response and Containment. FortiClient extends the Security Fabric's policy-based automation capabilities for responding to incidents and limiting their impact. If an endpoint exhibits suspicious behavior that meets IOC criteria, it can be automatically quarantined from the rest of the network to prevent the spread of infection among other devices or lateral movement within the organization.

Additionally, when the Security Fabric finds a device that is out of compliance or with unpatched vulnerabilities, in addition to warning the users, it can leverage virtual network segmentation and network access control to automatically relegate the rogue endpoint to a safe segment of the network. This automated quarantining prevents access to critical corporate assets, thereby protecting sensitive data and limiting exposure at a policy level without burdening IT staff. It also helps business leaders ensure that their operations adhere to increasingly strict data privacy standards and industry regulations.

Alert Verification and Resolution. As a sub-function of the enterprise-wide threat intelligence exchange, integration between FortiClient and other network security tools enables cross-referencing of events with network traffic. This helps to verify alerts, surface threats, and potential compromises, enhancing an organization's "signal-to-noise" ratio and thus minimizing false positives and alert fatigue for more accurate diagnoses. In this case, automated resolution responses may include end-user prompts, auto-patching, remote endpoint quarantine, or applying other network access controls.

Open Ecosystem. As part of the Fortinet Security Fabric's open API-based ecosystem, FortiClient extends compatibility to third-party solutions—including EPP and endpoint detection and response (EDR) products. As a result, organizations can continue to gain benefits from their existing investments without worrying about conflicts.

HOLISTIC NETWORK PROTECTION THAT COVERS ENDPOINTS

With mobile devices continuing to be a top risk exposure for organizations, Fortinet's deep integration between endpoint security and network security strengthens enterprise-wide defenses while streamlining operations and reducing total cost of ownership (TCO).

By exchanging real-time threat intelligence with other security solutions across the enterprise, FortiClient helps solidify the overall defensive posture by:

- Sharing intelligence in real time to reduce exposure
- Improving visibility and control through risk awareness and better security hygiene
- Securing remote access
- Automating workflows and security responses
- Providing compatibility with existing AV solutions without causing conflicts

[1] Lee Neely, "Endpoint Protection and Response: A SANS Survey," SANS Institute, June 12, 2018.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

August 10, 2018 5:35 AM

247068-0-0-EN Macintosh HD:Users:ckluck:Documents:FORTINET_ck:FortiClient_SB_BOFU:FortiClient_SB_BOFU_ck2