FOUR WAYS TO IMPROVE ENDPOINT SECURITY: MOVING BEYOND TRADITIONAL APPROACHES
# TABLE OF CONTENTS

1. **INTRODUCTION**  
   NETWORK AND ENDPOINT SECURITY INTEGRATION

2. **SECTION 1**  
   RISK-BASED VISIBILITY

3. **SECTION 2**  
   CONTROL

4. **SECTION 3**  
   THREAT INTELLIGENCE SHARING AND ALERT RESOLUTION

5. **SECTION 4**  
   AUTOMATION

6. **SUMMARY**  
   WHAT TO LOOK FOR
Endpoint devices continue to be one of the favorite targets for cyber-attacks. A successfully compromised laptop provides a foothold for a threat to move laterally and infect other endpoints within the organization. To address this critical vulnerability, security leaders must integrate endpoint security into their broader network security architecture. A deep connection between endpoint and network security offers key improvements to holistic enterprise protection. It provides risk-based visibility of all endpoint devices, establishes policy-based access controls, enables real-time threat intelligence sharing, and automates security responses and workflows for effective and efficient protection that conserves time and money.

EXECUTIVE SUMMARY
INTRODUCTION: NETWORK AND ENDPOINT SECURITY INTEGRATION

Endpoint devices represent some of the most common targets for cyber-attacks. If a vulnerable laptop is compromised by threat actors in the field, that infection can rapidly spread to the rest of the organization upon reconnecting to the network. In 2017, the average cost of a successful endpoint attack was over $5 million per organization.¹ This is why enterprises currently spend a whopping 1,156 hours each week to detect and contain endpoint-borne risks—an average of $3.4 million weekly.²

Beyond the threats themselves, the problem behind these resource-intensive defenses (and endpoint vulnerability in general) is that network security and endpoint security typically operate in complete isolation from one another and exhibit little interoperability. To improve both endpoint protection and holistic enterprise security, this needs to change.

There are four main areas where this kind of deep integration can offer significant improvements to enterprise security: risk-based visibility, control, threat intelligence sharing, and automation.

of organizations report that malware-infected endpoints have increased in the last 12 months.

*The Cost of Insecure Endpoints,* Ponemon Institute, June 2017.
01: RISK-BASED VISIBILITY

Organizations need full awareness of endpoints when they are on and off the corporate network without forcing VPN sessions. Security must be able to see all users and devices and be able to assess/monitor the inherent risks. This includes unpatched vulnerabilities, outdated software, and potentially unwanted applications due to risky end-user behavior.

Risk-based visibility requires telemetry data for all endpoint can be seen and shared in real time with network security tools (firewalls, sandboxes, web filters) across the organization.

Network directors should be able to tell at a glance if the organization is improving its defensive stance day by day. Simplified, single-pane-of-glass management can offer a complete view of associated endpoint risk exposures—including user identities, protection status, unpatched vulnerabilities, and security events.
The endpoint visibility and control market is expected to grow 23.2% through 2021, aiding the discovery and prevention of potential threats.

*Endpoint Security Software Market Will Reach $5.9 Billion by 2021,* Forrester, August 21, 2017.
Once visibility is established, proper controls can be imposed. Endpoints must be hardened and the correct procedures must be applied to maintain security hygiene, which strengthens the enterprise’s holistic security posture.

Your endpoint security solution should enforce policies and controls across all devices; only endpoints that meet all compliance and security standards should be granted access to the network resources. Using telemetry data, policy-based access controls can be applied. If a rogue or compromised endpoint with too high a risk is discovered, it can be safely contained and flagged for remediation.

HARDENING YOUR ENDPOINTS
Organizations must identify, install, and configure effective security solutions—as well as establish baseline readings. Key success factors include ease of data collection (49%), correlation of data into usable information (47%), skilled operators (46%), and automation/tool interoperability (43%).

56% of IT professionals report that they cannot determine compliance for endpoint devices (such as checking for unpatched vulnerabilities).

03: THREAT INTELLIGENCE SHARING AND ALERT RESOLUTION

Deep integration between endpoints and network security tools supports the instant, bidirectional exchange of threat intelligence. This key defensive capability will become increasingly valuable as attacks become even more targeted through the use of spear phishing and custom malware.

Sharing real-time information across the organization supports instantaneous responses to coordinated attacks against a specific organization or industry. When a network, web gateway, or endpoint security solution intercepts a new threat, this intelligence can automatically be sent to all other endpoints and security solutions deployed across the organization.

Endpoint security that both sends and receives threat intelligence in coordination with network security can also offer alert verification and resolution features. This means that endpoint security can cross-reference events with network traffic or threat intelligence feeds to verify alerts, surface threats, and potential compromises. This enhances an organization’s “signal-to-noise” ratio—minimizing false positives and alert fatigue—for a more complete and accurate picture of the network’s immediate security posture.
“Endpoint threat intelligence should feed into detection and response systems. This should reduce the time to detect, respond, and ultimately remediate the threat/vulnerability the attacker was trying to exploit.”

04: AUTOMATION

Automation is the “holy grail” of integration. Automated responses and workflows enable faster detection and better protection, while reducing the strain on overburdened/under-resourced IT teams. Without human involvement to bog down the response time, attacks and incidents can be handled with speed, efficiency, and efficacy. Following are some of the ways endpoint security automation can be used:

**Vulnerability management** capabilities should allow your endpoint security solution to automatically patch software/operating systems and to provide flexible remediation of minor issues. These features help eliminate basic defensive gaps while reducing the manual processes churn of underresourced IT teams.

**Automated incident response and containment** functions support instantaneous responsiveness to detected threats that prevent wider outbreaks from occurring. If an endpoint exhibits suspicious behavior that meets indicators of compromise (IOCs) criteria, it can be instantly quarantined from the rest of the network to prevent the spread of infection among other devices or lateral movement within the organization. Automated quarantining protects sensitive data and limits exposure without burdening IT staff, accelerating time-to-containment/resolution windows. It also helps network engineering leadership ensure that their infrastructures support increasingly strict data privacy standards and industry regulations.

To enable the broadest possible interoperability of your solution’s automation capabilities across the network security architecture, be sure to look for endpoint security based on an open API that’s compatible with other third-party security products. This extends security integration while helping to maximize your existing investment in other AV solutions or security products.
“Automating endpoint detection and response solutions is the top priority for IT professionals trying to put actionable controls around their endpoints.”

Lots of different security vendors use integration as a buzzword. However, it’s important to understand that not all levels of integration are the same. Effective integration between endpoint security and network security should address the following questions:

**Visibility**
- Can you see all devices and identify users?
- Can you monitor associated risks? Unpatched vulnerabilities? Outdated applications? IOCs?
- Can an endpoint’s telemetry data be shared in real time with the rest of the enterprise?

**Control**
- Can you enforce policy-based controls based on IOCs or specific compliance requirements at a network level?
- Does your solution help harden endpoints?
- Can it limit access based on basic security hygiene?

**Threat Intelligence Sharing**
- Can the solution exchange threat intelligence with other parts of the security architecture within the enterprise?

**Alert Resolution**
- Does it include alert verification/resolution capabilities to reduce “alert fatigue”?

**Automation**
- Does the solution provide remediation tools, such as auto-patching?
- Can you set policies to automate responses—such as notifications, quarantine, or other access controls?

**Open Ecosystem**
- Does the solution integrate seamlessly with other third-party solutions?