FORTINET

# Which Next-generation Endpoint Security Enhancements Are Required

## How IT Infrastructure Leaders Can Protect Endpoints and Improve Operational Efficiency

# Table of Contents

# Executive Overview

Endpoints continue to be one of the favorite targets for cyberattacks. A successfully compromised laptop, smartphone, or Internet-of-Things (IoT) device can provide a foothold for threats to move laterally, infect other endpoints within the organization, and moreover enable attackers to gain access to other critical assets. In addition to weakened security, intrusions also divert staff time away from activities that enhance network performance and streamline operations.

To address these challenges, IT infrastructure leaders need integrated network and security solutions that protect the endpoints, minimize the operational impact associated with the expanding attack surface, and allow their teams to scale. A deep connection between endpoint and network security offers key improvements to holistic enterprise protection by providing risk-based visibility of all endpoint devices, policy-based access controls, real-time threat-intelligence sharing, and automated security responses and workflows.

# Only 26% of technology leaders say they are “well prepared” for cyberattacks.[1]

# Introduction: The IT Infrastructure Leader and Endpoint Security

The endpoint attack surface is expanding rapidly, driven by an exponential growth in end-user devices. This is exacerbated by a proliferation in connected devices such as IoT sensors, wearables, industrial control systems (ICS), and self-driving vehicles. As a result, successful cyberattacks are prevalent and continue to grow, with half of organizations experiencing at least one endpoint breach in the past 12 months.[2] Most organizations look to their IT infrastructure leaders to address the problem, with nearly three-quarters (73%) directly responsible for endpoint security.[3]

Beyond the threats themselves, there are serious problems with network and endpoint security—which typically reside in separate silos and do not communicate. Traditional approaches to network and endpoint security fail to integrate the multiple security components involved. In response, IT infrastructure leaders need to break down these siloes by embracing a security architecture that integrates network and security elements, including endpoints, into an intelligent security platform. This transformation requires four essential enhancements: improved risk visibility, dynamic access controls, threat-intelligence sharing, and automated security workflows.

# 56%

**of IT infrastructure leaders spend more than half their time dealing with cybersecurity.[4]**

## Requirement 1: Improve Risk Visibility

Visibility is a key prerequisite for effective endpoint security—you cannot secure what you cannot see. IT infrastructure staff require full awareness of the status of endpoints both on and off the corporate network, including unpatched vulnerabilities, outdated software, potentially unwanted applications, risky behavior, and policy violations. Risk-based visibility depends on a clear understanding of endpoint risk exposures, including user identities, protection status, and security events.

For the IT infrastructure leader, the mandate is to select endpoint security solutions that can share real-time telemetry with other security tools. This includes firewalls, sandboxes, and web filters. It also means security workflows and threat mitigation must interact seamlessly between each of the elements. All of this can consume valuable staff time without the right integration points. Thus, a next-generation endpoint security solution must enable at-a-glance assessments of security status through single-pane-of-glass management tools.

# $8.19M

## Average total cost of a data breach in the U.S.[5]

## Requirement 2: Upgrade Access Controls

Once risk visibility is in place, IT infrastructure leaders require more granular and dynamic network access control. Here, endpoint security should enforce policies and controls across all devices and defend against attacks initiated via endpoint devices. In doing so, endpoint security must ensure that endpoints meet all compliance and security standards before granting network access. It must also have the ability to analyze and quarantine rogue and compromised endpoints.

Grouping endpoint devices into intent-based segments that enable dynamic access control is an important part of the process. This requires streamlined deployment and management capabilities, including compliance activities and reporting, for IT infrastructure staff who are overburdened and unable to manage these activities manually.

# 67%

**of technology leaders say the skills shortage prevents the organization from keeping up with the pace of change.[6]**

## Requirement 3: Share Threat Intelligence

As attacks become more targeted and virulent, the time window for effective incident response continues to shrink. Accelerating time to resolution requires instant, bidirectional sharing of threat intelligence through deep integration between endpoints and network security tools. When one network component intercepts a new threat, it automatically sends the intelligence to other endpoints and security solutions deployed across the organization, instantaneously.

Real-time information sharing allows IT infrastructure staff to gain a complete and accurate picture of the network's immediate security posture. Endpoint security cross-references events with work traffic and threat-intelligence feeds to verify alerts, discover threats, and identify potential compromises. Deep integration helps to enhance the signal-to-noise ratio, minimizing false positives and alert fatigue and providing a more accurate picture of the network's immediate security posture.

To maximize staff productivity, IT infrastructure leaders need to consider augmenting endpoint security with a subscription to a security rating service. IT infrastructure leaders can use the tools in the security rating service to better understand their organization's security posture as compared with peer organizations and recognized standards. They also can get detailed guidance and "to-do" lists to systematically improve their security posture and report those improvements to executives.

# 206 days

**Mean time to identify a data breach, up 5% from last year.[7]**

# Requirement 4: Automate Security Workflows

Automating key security workflows is an essential enhancement that allows IT infrastructure leaders to achieve effective endpoint security while reducing the strain on their overburdened and often under-resourced teams. Endpoint security automation offers advantages to the organization's security posture through vulnerability management, automated incident response and containment, and endpoint compliance. Following are some of the key capabilities IT infrastructure leaders need to achieve such in an endpoint security solution:

**Vulnerability management.** Vulnerability management includes the ability to automate patching for endpoint software and operating systems and to provide flexible, automated remediation of minor security issues without human intervention. These capabilities help to eliminate basic defensive gaps in the endpoint security posture while reducing manual, repetitive tasks for IT infrastructure personnel.

**Automation of incident response.** Automated incident response and containment accelerates time to containment and resolution by eliminating the time for human response from security workflows. Endpoint security should automatically quarantine suspicious or compromised endpoints to prevent the spread of infection to other devices as well as lateral movement of threats within the organization. Doing so also helps to minimize human errors and facilitates endpoint compliance with increasingly strict data privacy standards and industry regulations.

**Open API architecture.** To enable the broadest possible interoperability of the endpoint security solution's automation capabilities across the network security architecture, IT infrastructure leaders require an endpoint security solution based on an open API architecture that is compatible with other third-party security products. This capability extends security integration while helping to maximize existing investments in other antivirus solutions and security products.

**“With a global army of connected devices and an attack surface that includes every partner and vendor in the company’s ecosystem, threat actors have the clear advantage.”[8]**

# Summary: What to Look For

Rapid expansion in the attack surface, which is closely tied to the growth in endpoints connecting to and residing on the network, makes it more difficult to protect against cyberattacks. It also ratchets up the time IT infrastructure teams spend managing endpoints.

Unable to see across endpoints and to centrally and proactively manage vulnerabilities, IT infrastructure leaders require a next-generation approach to endpoint security. It must not increase cost or the amount of time spent managing endpoint security. Rather, endpoint security must break down the silos between endpoints themselves as well as endpoints and the network. This enables real-time threat-intelligence sharing and telemetry, offers centralized access control, and automates compliance audits and reporting and workflows around patching and incident response.

[1] Anna Frazzetto, et al., "A Changing Perspective: CIO Survey 2019," Harvey Nash/KPMG, 2019.

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

[3] "The IT Infrastructure Leader and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, August 18, 2019.

[4] Ibid.

[5] "Cost of a Data Breach Report 2019," IBM Security and Ponemon Institute, April 2019.

[6] Anna Frazzetto, et al., "A Changing Perspective: CIO Survey 2019," Harvey Nash/KPMG, 2019.

[7] "Cost of a Data Breach Report 2019," IBM Security and Ponemon Institute, April 2019.

[8] "The Post-Digital Era is Upon Us: Are You Ready for What's Next?," Accenture, 2019.

www.fortinet.com



446935-0-0-EN

October 28, 2019 8:43 PM

eb-next-generation-endpoint-security