FORTINET

WHITE PAPER

6 Obstacles to Effective Endpoint Security

Disaggregation Thwarts Visibility and Management for IT Infrastructure Leaders

Executive Summary

To stay competitive and drive innovation, most organizations are embracing digital innovation (DI) in the form of cloud services, smart Internet-of-Things (IoT) devices, and greater mobility. Among the benefits of DI, users gain faster, more seamless access to critical information using any device from any location at any time. However, the proliferation of connected devices also expands the attack surface, which makes endpoints prime targets for malware infections and sophisticated exploits. When it comes to protecting these disparate endpoints, the IT infrastructure leader plays a critical role. But achieving comprehensive protection and efficient operational efficiencies while having minimal impact on endpoint performance is difficult.

The Expanding Endpoint Attack Surface

In the security context, the definition of endpoint has broadened in recent years from mobile devices—such as laptops, phones, and tablets—to encompass any connected device that attackers can use to bypass the perimeter security of the enterprise network. The greatest area of growth in the endpoint attack surface is the result of IoT device explosion such as wearable fitness trackers, industrial control systems, and sensors in self-driving vehicles. IoT devices number in excess of 7 billion.[1]

With so many endpoints to target, cyber criminals are more successful than ever. Almost half of organizations indicate they had at least one endpoint breach in the past 12 months.[2] If this is not alarming enough, 20% do not know whether their organization experienced an endpoint intrusion—hardly reassuring to the IT infrastructure leader who is typically charged in managing endpoints and protecting them against cyberattacks.[3]

Certainly, the charge of protecting endpoints has never been more difficult, in large part due to the proliferation in the number and type of endpoints connecting to the network. Indeed, one study finds that enterprises use 17 different categories of endpoint devices—from desktops, to server workloads (virtualized or physical), to cloud-based services and applications, to mobile devices, to IoT devices, to various wearables (Figure 1).

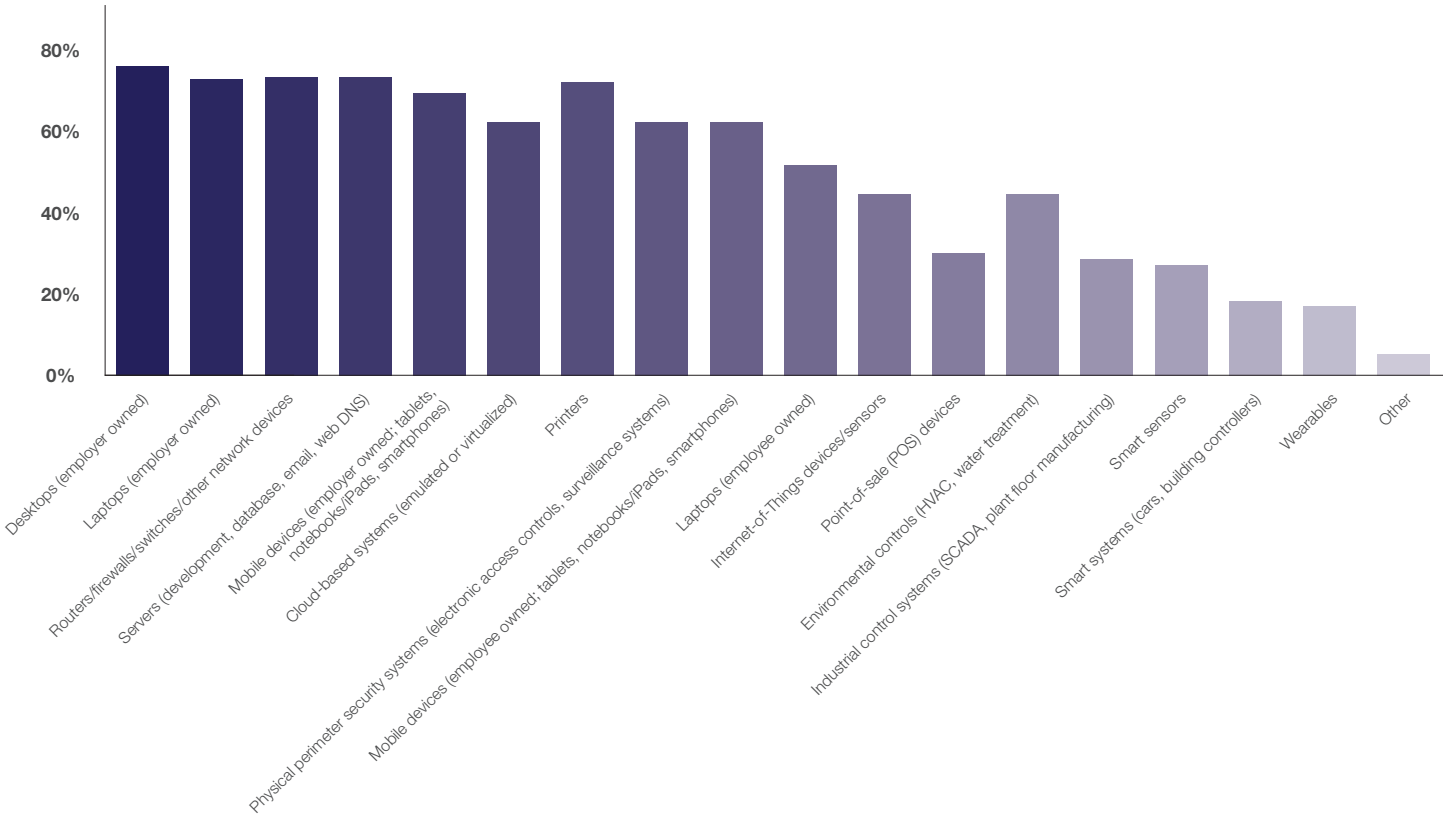

Figure 1: 17 different categories of endpoint devices.

Each category of device represents a unique security challenge: For example, exploits that target routers are very different from those that attack mobile or IoT devices. In addition, each device category includes offerings from several vendors, multiplying the complexity of the threat landscape. The net effect is that IT infrastructure teams become overwhelmed and unable to keep pace managing endpoints.

Impact of Inadequate Endpoint Security

The negative consequences of inadequate endpoint security include increased risk exposure, operational inefficiency, information exfiltration, and endpoint-initiated malware outbreaks.

Increased risk exposure

The average value of risk associated with a breached endpoint continues to increase, with the cost per breach reaching $13 million today.[4] The impact spans the gamut from productivity loss and information exfiltration to downtime and reputation degradation.

Integration and automation of endpoint security are promising. However, only 11% of organizations have a fully integrated security system, which is key to unlocking automation capabilities. Indeed, research shows that most IT infrastructure teams struggle to manually correlate data from a disparate array of point solutions, an inefficient and ineffective approach to endpoint security.

Operational inefficiency

For the IT infrastructure leader, the implications of inadequate legacy solutions and impaired visibility are profound. Disaggregated security elements, including endpoint protection, and vulnerability scanning and patching, often require manual workflows and threat-intelligence sharing that place additional pressures on overstretched operational staff. Further, to support compliance audits and reporting requirements, IT infrastructure teams spend hours on highly inefficient and time-consuming activities such as manual log pulls and data reconciliation.

This situation reduces productivity and stretches already overburdened teams. IT infrastructure leaders not only lose staff time to manual, repetitive tasks but also increasingly struggle to achieve the productivity improvements that organizations expect of them.

Information exfiltration

Depending on the type of endpoint threat in question, the impact of an infected endpoint can vary greatly. To begin, threats do not need to travel beyond the device itself to damage an organization. Laptops, tablets, and point-of-sale (POS) systems can process or store valuable data or IP in local memory, which can be immediately exfiltrated by malware upon infection.

Some threats can also harvest credentials, allowing exploits to move laterally across the network in search of valuable data. These credentials can also be quietly harvested and saved for future attacks. As an example, the Smoke Loader infection campaign steals credentials from web browsers, email clients, and other sources. Attacks begin with malicious emails carrying a weaponized Word attachment. Using social engineering, the attackers attempt to lure victims into opening the document and executing an embedded macro.[6]

Massive malware outbreaks

Infected endpoints can also initiate malware outbreaks. Once malware infects a single machine, it uses connectivity and the endpoint's credential to infect vast numbers of other endpoints on the network. Recent malware outbreak examples include LockerGoga, Emotet, and SamSam.[7] These kinds of attacks often use PowerShell to launch fileless attacks and install ransomware or cryptoware that can move laterally and spread across networks, with the goal of inflicting maximum damage and commanding larger ransoms.

Obstacles to Securing Expanded Endpoint Attack Surface

As IT infrastructure leaders address the challenges of endpoint security, they must confront a range of obstacles, including inadequate legacy solutions, dispersed workforce, bring-your-own-device (BYOD) policies, and a pressing IT and security skills shortage.

Obstacle 1: Inadequate legacy solutions

One obstacle facing infrastructure leaders is the inadequacy of legacy security systems. Solutions designed for previous-generation networks are largely ineffective for managing security for a dynamic and diverse population of endpoint devices. Further, most current endpoint security solutions exist in localized siloes, which prevents them from connecting or communicating with other parts of the broader security architecture. As a result, endpoints cannot receive or share zero-day threat intelligence; this inhibits response to broad attacks and breaches.

Exacerbating the problem is the complex network topology of many current security architectures, which gives attackers an unintended advantage by making it difficult to identify intrusions early in the attack life cycle.

Only 11% of organizations have a fully integrated security system.[8]

Obstacle 2: Lack of visibility

As an extension of the complexity problem, the sheer number of devices connected to the network obscures visibility across all endpoints and the ability to manage risk. Specifically, traditional endpoint security offers limited visibility of the device itself. To improve endpoint protection, cybersecurity teams must be able to see everything.

The list of what needs to be visible is extensive: everyone who has access to the network, what types of devices are connected, the OS versions installed, unpatched vulnerabilities, associated traffic, and all the software being used.

A particularly worrisome manifestation of the visibility problem occurs when endpoints disconnect from and then reconnect to the network. Specifically, research shows that 63% of organizations are unable to monitor endpoint devices when they leave the corporate network, and 53% reveal that malware-infected endpoints have increased in the last 12 months.[9] As the number of users and devices that exit and reenter the corporate network increase, the difficulty in ensuring that those endpoints are protecting increases. And when an infected laptop, tablet, or smartphone connects to the internal network, the organization can be exposed to viruses, malware, and other exploits with which the device has been infected while being off the network.

Obstacle 3: Dispersed workforce

Adding to the challenge of endpoint security is a geographically dispersed workforce, in which employees do their work at scores of locations—from central headquarters and satellite campuses to branch and home offices. Add that they gain access through other means and places, the attack surface expands even further. For example, as they move in the course of their work, remote workers often connect using hotspots or public Wi-Fi networks in coffee shops, airports, and automobiles, and on park benches.

Such ubiquitous connectivity may be convenient, but it also poses substantial security risks. Man-in-the-middle attacks, as an example, allow third parties to eavesdrop on all information that passes between the user and the corporate network. Attackers can exploit unpatched software vulnerabilities to inject malware into the endpoint device, to not only access local information but also gain access to the corporate network via the endpoint device.

Obstacle 4: Bring your own device

Unlike the days of corporate-specified devices, endpoints are no longer a unified extension of corporate IT infrastructure. The BYOD trend has undeniable benefits: Research shows that using portable devices for work tasks saves employees 58 minutes per day while increasing productivity by 34%.[10]

While BYOD may be popular with users and managers alike, IT infrastructure leaders cannot overlook the dangers. Information stored locally is inherently less safe than data residing within the network security perimeter. A lost or stolen device not only puts at risk local data but it can also reveal passwords that enable successful attacks on the corporate network. In a typical scenario, a user unwittingly downloads a mobile game that contains hidden malware, which then enters the corporate network at the next login.

Obstacle 5: Shadow IT

Shadow IT refers to software and hardware that users install on the network without the sanction—or even the knowledge—of the IT department. Users often cite the benefits of Shadow IT such as faster innovation and increased productivity. However, for the IT group, this trend only complicates the process of protecting the enterprise network and valuable corporate intellectual property because more and more network components fall outside the visible infrastructure and therefore cannot be effectively managed.

As it relates to endpoint devices, Shadow IT ranges from unauthorized messaging apps such as WhatsApp and Snapchat to unapproved Software-as-a-Service (SaaS) applications such as Jira and Basecamp.[11] Today, the phenomenon extends far beyond the traditional endpoint device to encompass IoT devices such as wearable fitness trackers, smart key locators, and personal assistants such as Alexa, all which are increasingly showing up on the corporate network.

Obstacle 6: Skills shortage

Organizations have long struggled with the shortage of cybersecurity-trained staff. 63% of organizations indicate security skills shortage is a top concern for them, and 58% say they have unfilled cybersecurity roles.[13] While these findings are not specific to endpoint security, the inability to hire and retain highly skilled security professionals hampers the efforts of IT managers to address all aspects of cybersecurity, including endpoint protection.

Outsourcing to managed security service providers offers an alternative method of accessing the necessary talent, but only 7% of IT infrastructure leaders outsource more than half of their security functions and more than one-third (36%) handle all security functions in-house.[14]

53% of organizations report that malware-infected endpoints have increased in the last 12 months.[12]

24% of respondents in a recent survey cite "lack of visibility across the endpoint attack surface" as a key cybersecurity challenge.[15]

Assessing Endpoint Risk

As IT infrastructure leaders grapple with the challenges of an expanding attack surface and the array of obstacles to endpoint security that lie in their paths, they should carefully evaluate the risks that an expanded set of endpoints presents. Following are some questions they should pose to determine areas of vulnerability in the categories of security integration, security management, and staffing considerations.

Security integration

- Are your endpoint security tools integrated with the rest of your cybersecurity infrastructure?
- Do endpoints in your branch offices and remote locations have the same level of cybersecurity as those in your headquarters and campus environments?
- Can you manage all endpoint security from a single console?

Security management

- Can your security team quickly assess the status of any given endpoint?
- Does your organization have tested policies and procedures for mitigating a breach that originates from a compromised endpoint?
- Does your system automatically push software updates and vulnerability patches to all endpoints as soon as vendors make them available?

Staffing considerations

- Does your organization provide cybersecurity training for all users, including how to avoid phishing attacks and other email-borne threats?
- Do you take advantage of managed security services to compensate for lack of in-house expertise?
- Have you filled all job openings that have an impact on your cybersecurity posture?

1 Knud Lasse Lueth, "State of the IoT 2018: Number of IoT devices now at 7B—Market accelerating," IoT Analytics, August 8, 2018.

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

3 Ibid.

4 Kelly Bissell, et al., "The Cost of Cybercrime: Unlocking the Value of Improved Cybersecurity Protection," Ponemon Institute and Accenture, 2019.

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

6 Ionut Arghire, "New Smoke Loader Attack Targets Multiple Credentials," SecurityWeek, July 5, 2018.

7 "Quarterly Threat Landscape Report," Fortinet, Q2 2019.

8 "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

9 John Maddison, "Are Endpoints Integrated Into Your Network Security Strategy?" Fortinet Industry Trends, April 17, 2018.

10 Lilach Bullock, "The Future Of BYOD: Statistics, Predictions And Best Practices To Prep For The Future," Forbes, January 21, 2019.

11 Zach Capers, "What is shadow IT and how should you respond to it?" GetApp, October 13, 2018.

12 John Maddison, "Are Endpoints Integrated Into Your Network Security Strategy?" Fortinet Industry Trends, April 17, 2018.

13 "Gartner Survey Shows Global Talent Shortage Is Now the Top Emerging Risk Facing Organizations," Gartner, January 17, 2019.

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

15 Mary Ann Davidson, et al., "Cloud Threat Report 2019," Oracle and KPMG, 2019.

September 8, 2019 11:39 AM

446538-0-0-EN

D:\Fortinet\Work\2019\September\090819\wp-six-obstacles-endpoint-security