WHY YOUR TRADITIONAL ENDPOINT SECURITY MAY BE PUTTING YOU AT RISK

EXECUTIVE SUMMARY

When it comes to securing all the parts of a modern distributed network, endpoints remain the most vulnerable outlier. Mobility has brought a flood of different devices that cross in and out of enterprise networks on a daily basis. This public exposure, combined with inadequate traditional endpoint security and a high degree of user autonomy, makes these devices prime targets for malware infections and other forms of sophisticated attack that seek to exploit the broader organization. And threat actors are finding enormous success along these vectors.

To stay competitive, most organizations are currently embracing digital transformation (DX)—including cloud services, smart Internet of Things (IoT) devices, and greater mobility. These adaptations provide organizations with faster and more seamless access to critical information, regardless of the device being used to access it. However, as distributed networks expand and become more difficult to manage, the endpoint remains a weak link in the security chain.

ENDPOINTS ARE FREQUENT ATTACK TARGETS

Endpoint devices represent some of the most common targets of compromise for organizations. Part of this is due to the growing volume of connected devices touching the network. At any given time, an individual user may access networked resources using several devices simultaneously—a laptop, smartphone, tablet, or even smartwatch.

$6M is spent annually due to inefficient and ineffective endpoint strategies.[1]

Endpoints remain one of the **most common targets of compromise** for organizations.

$3.4M is spent annually on detection and containment of insecure endpoints alone.[1]

Unfortunately, most IT teams treat endpoints separately from the rest of the network due to the sheer number of devices and the need to support end-users. Endpoint security is commonly applied to devices as an isolated solution, usually in the form of antivirus protection or an endpoint security package. Network security typically begins at the point where an endpoint device touches the network. And once an endpoint connects to your network, that device (and everything it contains) becomes part of your local area network (LAN)/wide area network (WAN).

But due to the above, the demarcation point between the endpoint and network is becoming increasingly difficult to define and defend. This situation is made worse by additional factors driving the need for better endpoint security.

One operational reason motivating this need for change is that endpoints are no longer a unified extension of corporate IT. Users now have substantial autonomy in choosing their devices, installing software, and even delaying security patch and update installations.

And it's this kind of user independence that creates what's known as Shadow IT—user-administered applications and endpoint management that is neither authorized nor overseen by the organization's IT experts. But this decision to cede control to end-users for the sake of usability and productivity creates security issues. Specifically, while it's not done with any ill intent, Shadow IT describes a widespread trend that exposes organizations to significant risks.[2]

Another reason prompting change is greater threat exposure. Endpoints (and the resources they access) are not always behind a corporate firewall. Users may connect to commercial Software-as-a-Service (SaaS) applications or cloud services (e.g., Dropbox, Box) both onsite or in the field. Users at some organizations aren't even required to connect via a virtual private network (VPN) to access corporate data. This public exposure leaves endpoints vulnerable to direct attacks, contact with contagions, and compromises resulting from human error or gullibility (the errant click on a bad file or link).

Cyber criminals are exploiting these vulnerabilities. In the last year, there were a total of 2,216 confirmed data breaches. Of those, 73% were perpetrated by outsiders. Phishing and pretexting represent 93% of breaches. Email continues to be the most common vector (96%).[4] Suffice to say, email-based attacks typically target endpoint users and their devices. When successful, the cost of these attacks is substantial: the average cost of a successful endpoint attack in 2017 was over $5 million per organization.[5]

On average, **4%** of people will take the bait in any given phishing campaign.[3]

To provide better holistic protection of organizations, enterprise security must address a number of acute environmental problems and systemic shortcomings that are leaving endpoint devices exposed in the current era.

THE ATTACK SURFACE IS EXPANDING

According to one study, 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.[6] When an employee's infected laptop or smartphone connects to the internal network, the organization can then be exposed to whatever threats (e.g., viruses or malware) with which the device has come in contact when it was off-network.

Depending on the type of endpoint threat that is present, there can be a few different, broader outcomes from a compromised endpoint. First, threats don't have 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.

Second, once an infected device reconnects to the internal network, some threats can also harvest the endpoint's credential to move laterally across the business in search of valuable data. These credentials can also be quietly harvested and saved for future attacks.

Finally, this connection pattern can also initiate malware outbreaks. Once malware infects a single machine, the threat uses connectivity and the endpoint's credential to infect vast numbers of other devices on the network. Recent malware outbreaks include WannaCry, Petya/GoldenEye, or Bad Rabbit. These attacks used ransomware or cryptoware that not only lock out infected endpoints but also have the worm-like capability to spread across networks, with the goal of inflicting maximum damage and commanding larger ransoms.

With each passing day, attacks increase in volume, velocity, and sophistication. A recent Forrester survey of 342 security leaders found that their largest cybersecurity challenge is adapting to the rapidly evolving nature of cyber threats.[7] While antivirus security on endpoints is now largely standard, modern threats are becoming too fast, too large, and too intricate for isolated, localized defenses to contain on a per-machine basis.

DISCONNECTED SECURITY CAN'T PROTECT COMPLEX ENVIRONMENTS

Outdated security controls designed for previous-generation networks simply cannot keep pace with the churn of an ever-changing threat landscape. Because current endpoint security solutions exist in a localized silo, they don't connect or communicate with other parts of the broader security architecture.

In this arrangement, endpoints can't receive or share zero-day threat intelligence. This inhibits the ability of security organizations to respond to broad attacks and breaches with speed, efficiency, and efficacy. The complex, disaggregated network topology of many current security architectures works to the advantage of new threats that make it beyond an endpoint and onto the open network.

In a recent survey of enterprise IT professionals regarding endpoint security, deployment and management complexity was one of the top-three problems reported (along with a lack of adequate protection and a high number of false-positive alerts).[9] There are several reasons why endpoint management has become more complex.

First, endpoint management complexity is part of a broader security complexity problem. IT teams struggle to effectively manage and protect the entire network due to security architectures that rely on a vast assortment of isolated point security products. These products tend to be added in a piecemeal fashion for a variety of reasons—to close newly exposed security gaps, to address growing network demands (e.g., SSL/TLS inspection, SD-WAN), and to respond to ever-increasing compliance standards and regulatory requirements.

Second, multiple consoles for managing different isolated products make operations much more difficult for staff. At the same time, they increase the opportunity for human error. This compounds the workloads of cybersecurity and IT teams that are already overwhelmed due to budgetary and staffing constraints.[10]

Top Attack Vectors[8]

- **74%** of threats entered as an email attachment or link
- **48%** entered the browser via web-based drive-by or download
- **30%** entered through application vulnerabilities on user endpoints
- **26%** entered via web servers and web application vulnerabilities

Finally, as proof of endpoints having slipped beyond the reach of IT, 56% of IT professionals report that they cannot determine compliance for endpoint devices (such as checking for unpatched vulnerabilities)—and more than one-third of devices (36%) fail compliance tests when checked.[11] These numbers reveal a significant blind spot within organizations—not just in terms of threat exposure but also to subsequent fallout from regulatory penalties and potential legal damages in the event of a breach.

YOU CAN'T PROTECT WHAT YOU CAN'T SEE

As an extension of the complexity problem, the sheer number of devices connected to the network obscures IT's ability to see everything and manage risk. Thus, many network managers lack transparent visibility and the ability to centrally manage security policy controls across the network.

Traditional endpoint security offers limited visibility of the device itself. To improve endpoint protection, cybersecurity teams must be able to see everything. It's an extensive list: 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.

BRINGING WAYWARD ENDPOINTS BACK INTO THE SECURITY FOLD

Endpoints can no longer live on their own private island. In the face of an increasingly hostile threat landscape, reduced IT oversight, and greater business complexity, enterprise security must do a better job of protecting these targeted devices that exist on the network edge.

Endpoint security is the responsibility of far more than the endpoint or desktop IT team. Beyond protecting individual devices, it also must close off attack paths to ensure the safety of enterprise data, network resources, and information systems. Therefore, it must become part of a broader, integrated network security architecture.

50% of companies require **35+ full-time employees** to manage endpoints.[12]

User action is the most common means of threat introduction and also currently a top means of **identifying compromise or infection** with the endpoints they are operating.[13]

1 Ibid.
2 Christy Pettey, "Don't Let Shadow IT Put Your Business at Risk," Gartner, May 3, 2016.
3 "2018 Breach Data Investigations Report," Verizon, April 10, 2018.
4 Ibid.
5 Charlie Osborne, "Fileless attacks surge in 2017, security solutions are not stopping them," ZDNet, November 15, 2017.
6 "The Cost of Insecure Endpoints," Ponemon Institute, June 2017.
7 "Center Security On Advanced Technology," Forrester Consulting, July 2017.
8 Lee Neely, "2017 Threat Landscape Survey," SANS Institute, August 2017.
9 Charlie Osborne, "Fileless attacks surge in 2017, security solutions are not stopping them," ZDNet, November 15, 2017.
10 Jon Oltsik, "Research suggests cybersecurity skills shortage is getting worse," CSO, January 11, 2018.
11 "The Cost of Insecure Endpoints," Ponemon Institute, June 2017.
12 Ibid.
13 Lee Neely, "2017 Threat Landscape Survey," SANS Institute, August 2017.

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

June 1, 2018 10:26 AM
Macintosh HD:Users:bhoulihan:Documents:_Projects:White Paper:white paper - endpoint protection:White-Paper-endpoint-protection-6-1-2018-1100am