5 reasons the security of your endpoints could be at risk

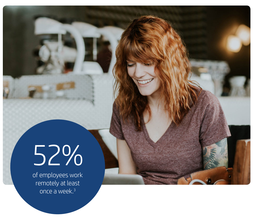
Cybersecurity threats are evolving, and organizations must keep up with endpoint security or risk being breached.

Confronting a disruptive force

The current face of cybersecurity makes device protection a complex task, and organizations can find themselves without sufficient defenses. From 2016 to 2018, almost a third of organizations were victims of cybercrime[1] – resulting in financial and reputational disruption.

Endpoints as the target

Cyberattacks are targeting endpoints – and it's a growing trend. In 2018, Ponemon surveyed 660 IT and IT security professionals from global companies, and almost two thirds reported a major breach that started at an endpoint, up 17% on the previous year.[2] It's no surprise, as cybercriminals have become more sophisticated and devices more complex to secure. Here are five reasons why your endpoints could be leaving you vulnerable.



01.

The workplace is decentralized

Where employees were once confined to an office, they're now spread across locations and time zones: 52% of employees work remotely at least once a week.[3] Increased flexibility brings increased risk. More employees log on to personal devices for work, and 60% of these devices are not monitored for security[4] – making it challenging to keep tech protected.

02.

Employees can miss threats

Many successful cyberattacks depend on human weakness. Over half of breaches in small and medium companies are caused by human error, found Ponemon.[5] And there's plenty of opportunity for employees to become a victim of cybercrime: one in ten emails reported by users are identified as malicious.[6]

03.

Antivirus is no longer enough

To sufficiently protect endpoints, organizations need to think past traditional antivirus software. Over half of endpoint attacks are missed by antivirus[2] and zero-day attacks are ready to exploit security vulnerabilities. Released into systems, for example through clicking links or downloading files from emails or browsers, zero-day threats are four times more likely to compromise organizations than a known attack.[2]

04.

A lack of visibility compromises safety

A breach is quick to cause disruption and systems can be compromised within minutes. Yet, two thirds of breaches aren't discovered until months after the attack.[7] Without a clear oversight of device health, organizations can suffer further financial and data losses.

05.

Expertise is in short supply

Endpoint security isn't just about securing devices. Organizations must consider device management and monitoring. Yet, IT departments are feeling the strain. There is a distinct lack of IT professionals available to tackle threats, with a shortfall in the cybersecurity workforce of just under three million.[8]

From weakest link to best defense

Support is available for endpoint security. HP Device as a Service (DaaS) with Proactive Security takes your whole organization beyond traditional antivirus to keep devices safe and employee productivity high.

Real-time threat isolation technology insulates zero-day attacks from email attachments, phishing links, browser downloads and file attacks, and stops them spreading – protecting devices from human error and keeping you up and running.

Security and threat analytics and reporting with HP TechPulse provides the visibility and insights needed to predict issues and proactively protect devices and data.

Plus, with the HP managed service, you can rely on our cybersecurity experts for added security, while reducing the burden on your IT team. HP Security Experts' monitor protection status and analyze threats to safeguard against future attacks – allowing your IT teams to utilize resources to focus on other priority projects.

HP DaaS Proactive Security transforms endpoints from your biggest risk to your best defense. And, HP delivers the world's most secure PCs, a worthy consideration for endpoint security protection.**

LEARN MORE

*Security Experts available in the Proactive Security Enhanced plan only.

**Based on HP's unique and comprehensive security capabilities at no additional cost and HP Manageability Integration Kit's management of every aspect of a PC including hardware, BIOS and software management using Microsoft System Center Configuration Manager among vendors with > 1M unit annual sales as of November 2016 on HP Elite PCs with 7th Gen and higher Intel® Core® Processors, Intel® integrated graphics, and Intel® WLAN, and on HP Workstations with 7th Gen and higher Intel® Core™ Processors as of January 2017.

Sources

[1] PwC, Pulling fraud out the shadows: Global economic crime and fraud survey, 2018.
[2] Ponemon Institute, 2018 State of Endpoint Security Risk sponsored by Barkly, October 2018.
[3] Owl Labs, Global State of Remote Work Report 2018, March, 2019.
[4] HR Dive, Employees use personal devices for work without much oversight, May 2018.
[5] Ponemon Institute, 2018 State of Cybersecurity in Small & Medium Size Businesses, November 2018.
[6] Cofense, State of Phishing Defense 2018, 2018.
[7] Verizon, 2018 Data Breach Investigations report 11th Edition, 2018.
[8] ISC2, Cybersecurity professionals focus on developing new skills as workforce gap widens, 2018.

HP DaaS plans and/or included components may vary by region or by Authorized HP DaaS Service Partner. Please contact your local HP Representative or Authorized DaaS Partner for specific details in your location. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product.

HP Services are governed by the applicable HP terms and conditions of service provided or indicated to the Customer at the time of purchase. The Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with an HP product.

© Copyright 2019 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA7-5762ENW, June 2019