2019 Endpoint Security Trends Report

New data security threats revealed from global study of six million devices
Contents

Table of Contents

INTRODUCTION 03
KEY INSIGHTS 04
SECURITY SPENDING VERSUS MATURITY 06
TOP ENDPOINT SECURITY RISKS 06
   KEY FINDING: ENDPOINT COMPLEXITY IS DRIVING RISK 06
   KEY FINDING: ENDPOINT CONTROLS DEGRADE OVER TIME 08
   KEY FINDING: FAILED AGENTS PROLONG SECURITY EXPOSURES 08
UNLOCK VALUE FROM EXISTING INVESTMENTS 09
CONCLUSION 10
RESEARCH METHODS 12
Today’s security technology landscape is overcrowded with tools and technologies built to combat endpoint risk. At the same time, security budgets at many organizations are increasing rapidly, propelled by the mandate to protect data and devices. In fact, 24 percent of the overall security spend is allocated to endpoint security tools. And by 2020, the projected total for global IT security spend is $128 billion1. Yet, over 70 percent of breaches still originate on the endpoint2. Why?

Industry analysts Forrester3 and Gartner4 have warned about the dangers of equating IT security spending with security and risk maturity. As organizations attempt to make the endpoint more resilient by buying more security tools, it is creating endpoint complexity. With an average of 10 security agents on each device and over 5,000 common vulnerabilities and exposures (CVEs) found on the top 20 client applications in 20185 alone, the endpoint has never been more fragile.

This report outlines the findings from extensive primary research analyzing more than six million enterprise devices over a one-year period. Our analysis led to a stunning discovery: much of endpoint security spend is voided because tools and agents fail, reliably and predictably.

Studying millions of devices, agents, and apps, uncovered some startling truths:

- 42 percent of all endpoints are unprotected at any given time;
- Two percent of endpoint agents fail per week; meaning,
- 100 percent of endpoint security tools eventually fail — no tool is immune.

The clear conclusion is that increasing security spending does not increase safety. In fact, every additional security tool only increases the probability of failure and decay. The data in this report provides evidence that merely investing in more endpoint security tools is ineffective, and a new approach is needed. To secure the endpoint, the security tools already in place must be made resilient.

---

2 IDC. 2016
4 Moore, S. Gartner Says Many Organizations Falsely Equate IT Security Spending With Maturity. Gartner.
5 MITRE.ORG
Key Insights

**Endpoint Complexity is Driving Risk**

- **10** Security agents per device
- **5000+** Common Vulnerabilities and Exposures (CVEs) on the top 20 client applications each year

**Last Known State: Anti-Malware Agent**

- **28%** Endpoints unprotected at any given point in a year
- **21%** Endpoints with outdated antivirus/anti-malware
- **7%** Endpoints missing protection

**Rates of Failure: Encryption Agent Health**

- **13%** Endpoints requiring at least one repair event within 30 days
- **75%** Repaired agents requiring at least two repair events within 30 days
- **50%** Repaired agents requiring over 20 repair events within 30 days
- **5%** Repaired agents requiring over 100 repair events within 30 days

---

* Absolute
** MITRE
† IDC
‡ Forrester

---

---
Endpoints requiring at least one repair within 30 days: 19%

Repaired agents requiring at least two repairs within 30 days: 75%

Repaired agents requiring over three repairs within 30 days: 50%

Repaired agents requiring over 80 repairs within 30 days: 5%

It is pointless to invest in new technologies if the basic measures—visibility, control, and resilience—are not operating effectively first.
Security Spending Versus Maturity

As organizations continue to increase spending on data and device security, the research in this report shows that much of that spend is in vain.

As a result, IT leaders are actually seeing a negative return on investment. In a recent report, Forrester summed up the situation by stating, "The next crisis for security leaders has arrived, and it’s a crisis of accountability...a new kind of accountability, with leadership asking them [security leaders] to show how their investments create value for the organization.”

The bottom line is that without visibility into their endpoint security posture, organizations are at a loss as to how to ensure agents, applications, and controls will continue functioning and delivering value as intended.

Top Endpoint Security Risks

With 70 percent of breaches originating on the endpoint, it is the number one target for attacks. Traditional endpoint security solutions exist to keep devices secure. The three most common traditional security tools are: encryption, endpoint protection (AV/AM/EDR), and client and patch management tools.

Encryption software protects data, endpoint protection protects against cyber threats, and client and patch management ensures applications are patched and safe from vulnerabilities.

The false sense of security they provide may be the greatest source of organizational risk.

---

7 Gartner. IT Key Metrics Data 2019: Key IT Security Measures.
Ensuring that AV/AM is up-to-date is essential to endpoint resilience. However, the data shows that despite the urgency of IT and security teams — at any given point — 28 percent of endpoints are unprotected: 21 percent had outdated AV/AM and seven percent were missing altogether.

Furthermore, of the devices with AV/AM installed, more than one agent designed to perform the same service were present on the majority of devices (1.2 AV/AM agents per endpoint). This adds complexity by increasing the likelihood that agents will conflict and decay, as a result of collision when competing for device services and resources.

"To understand your security posture, you need to know: Are your endpoints operating as expected? Do they have the right protections in place?"

– Fortune 500 security executive

In addition to AV/AM proliferation, endpoints are swelling with risk-generating agents colliding with one another. While the total number of agents per device (10) is substantial, nine of those agents came from five technology categories:

- Encryption
- Unified Endpoint Management (UEM)
- Endpoint Detection and Response (EDR)
- Endpoint Protection Platform (EPP/AV/AM)
- Virtual Private Network (VPN)
KEY FINDING
Endpoint Controls Degrade Over Time

Encryption is the staple security tool most often taken for granted. While it can certainly provide protection, it is not a "set it and forget it" solution — quite the contrary. Whether disabled by users or through malfunction, encryption is regularly broken, disabled, misconfigured, or missing entirely. In fact, at any given point in time, over **42 percent of endpoints experienced encryption failures.**

However, the near half-time spent unencrypted is only part of the story. The study found that data protections are voided when chronically fragile encryption agents fail. What's more, encryption failures occur reliably and predictably — two percent of encryption agents failed every week. While half of all encryption failures occurred within two weeks, the rate of decay is constant: eight percent failure per 30 days.

In fact, regardless of industry, **100 percent of devices experienced encryption failures within one year.** On average, the median time-to-failure for encryption across all devices is just 12 days, but our data reveals that it can happen as quickly as within six hours.

Digging deeper, we also found that 13 percent of endpoints required at least one encryption agent repair event within 30 days. Of those, 75 percent reported at least two repair events and 50 percent reported more than 20 repair events. Chronically ill devices reported as many as 100 repair events every month due to endpoint complexity.

Even more concerning, encryption recovery times are lengthy — meaning the window of vulnerability (WOV) is large. The average WOV for unencrypted devices is 12 days, but 30 percent of devices remain unencrypted for more than 60 days.

KEY FINDING: Failed Agents Prolong Security Exposures

Client management and patching tools break reliably and predictably. 19 percent of endpoints require at least one client/patch management repair monthly. So, just when they are needed most, one out of five of these agents fails.

In addition to the failure rates, patch and client management agents are often repeat offenders. Of those patching agents requiring repair, 75 percent reported at least two repair events and 50 percent reported more than 20 repair events. Additionally, five percent could be considered to be chronically ill, with 80 or more repair events in the same one-month period.

Part of our analysis examined the most common endpoint applications — classifying and sub-classifying families of applications to see how vulnerabilities arise.
The 20 most common client applications published over 5,000 vulnerabilities in 2018. If every device had only the top ten applications (half), that could result in as many as 55 vulnerabilities per device just from those top ten apps. This includes browsers, OSs, and publishing tools.

Client patch management agents fail at double the rate encryption agents do. However, once failed, an encryption agent reported seven times more repair events than client management agents.

Unlocking Value from Existing Investments

The critical endpoint security solutions we rely on are flawed. They are extremely fragile, degrade quickly, and create unnecessary friction for users. The study found an average of 10 distinct agents layered onto most of the devices. With this number, it’s inevitable that agents will collide, be disabled by users, or go unpatched. These blind spots hinder the visibility of IT and security leaders and leave endpoints — and the organizations to which they belong — increasingly vulnerable over time.

It is clear that there is no shortage of security controls. The real problem organizations face is in ensuring that these controls remain in place and are functioning at all times. It is pointless to invest more money into exciting new technologies (such as blockchain, artificial intelligence, and machine learning) if the basic measures – visibility, control, and resilience – are not operating effectively first.

The data has shown how well-functioning controls fail. These failures occur without anyone — threat actors, negligent users, and bots — intending for failure to happen. Additionally, it shows how endpoint complexity amplifies this natural propensity for device security to degrade over time.
IT and security leaders must create an environment which fosters a path to:

1. Understanding what's happening on their organization's devices (Visibility);
2. Responding to suspicious events to enable the reduction of security degradation (Control); and
3. Empowering the applications to persist and automate their restoration when incidents occur (Resilience).

Forrester recently suggested that any security investment should be measured based on maturity\(^\text{10}\). Improving maturity requires coordination, scaling, and optimization of a security program's components. To move the needle, it is necessary to activate the fundamental security controls on devices to gain a persistent connection to each endpoint in a fleet.

This provides visibility and control to unlock value from existing investments. The basic tools in most enterprise security portfolios are more than capable of protecting devices, data, users, and apps – as long as they are working.

According to Forrester's "Justify Security Budget By Its Impact on Maturity", security leaders spend too much time measuring their performance based on uncontrollable external factors – threat actors, tool sets, and motivations. Measuring maturity, instead, focuses on components that can be controlled and for which success can truly be defined.

**Conclusion**

Threats are becoming more sophisticated and breaches increasingly common, causing anxiety within organizations. This fear amplifies a pervasive willingness to purchase more endpoint protection solutions. Endpoint security spend is greater than ever. And yet, the endpoint is "patient zero" in the vast majority of recent breaches, proving that simply spending more on security tools isn't enough. While the answer may be decreasing complexity on the endpoint, many of those tools are needed.

In addition, the number of combinations of security controls from a variety of vendors makes it impossible to test pre-deployment by enterprises.

Endpoints still require patches, encryption and other protections, and those controls must be resilient themselves. This resilience can only be made possible through persistence — that is, maintaining a constant, unbreakable connection to data and devices that identifies and remediates security issues as they arise.

Over 12,000 organizations today are taking advantage of Absolute’s patented Persistence®, a patented technology that delivers this visibility, control, and resilience across all devices, apps, agents, and users by orchestrating each cyber resilience indicator with precision. They have in their arsenal an intelligence service that allows a clear view into critical details about their endpoint population. They are reducing their overall security costs by monitoring how their endpoint controls work (or don’t) to reduce endpoint security decay. They validate safeguards and eliminate compliance failures. And they are responding to threats and exposures with the confidence to control devices from anywhere. Absolute is a trusted companion on the journey toward endpoint resilience, persistence, and intelligence. Learn how Absolute helps to end the ceaseless technology spend and ensure that all endpoints are secure and persistent.

About Absolute

Absolute empowers more than 12,000 customers worldwide to protect devices, data, applications, and users against theft or attack—both on and off the corporate network. With the industry’s only tamper proof endpoint visibility and control solution, Absolute allows IT organizations to enforce asset management, security hygiene, and data compliance for today’s remote digital workforces. Absolute’s patented Persistence® technology is embedded in the firmware of Dell, HP, Lenovo, and other leading manufacturers’ devices for vendor-agnostic coverage, tamper-proof resilience, and ease of deployment. See how it works at absolute.com and follow us at @absolutecorp.
Research Methods

This report outlines the results from a one-year study conducted by Absolute’s security research team. Data was gathered from over one billion change events on over six million devices.

The devices represent data from 12,000 anonymized organizations across North America and Europe. Each device had Absolute’s endpoint visibility and control platform activated.

Researchers applied an Endpoint Resiliency Index to the sample to establish a baseline and monitored the results over a 12-month period. The Endpoint Resiliency Index applies the method used by the World Economic Forum’s Environmental Performance Index to track the overall direction of key variables of quality.\(^\text{11}\)

### Endpoint Resiliency Index Model

<table>
<thead>
<tr>
<th>EHI (TOTAL)</th>
<th>OBJECTIVE</th>
<th>SECURITY POSTURE</th>
<th>CYBER HYGIENE INDICATORS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Security</td>
<td>Data Residency</td>
<td>• Sensitive Data Exposure</td>
</tr>
<tr>
<td></td>
<td>Metadata Groups</td>
<td>Metadata Groups</td>
<td>• Consumer PII Components</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Financial Transaction Data (e.g. purchasing cards)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Government Issued ID (e.g. passport records)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Corporate Data Assets (e.g. intellectual property)</td>
</tr>
<tr>
<td></td>
<td>Data Dispersion</td>
<td></td>
<td>• Localized Storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Cloud Application Storage</td>
</tr>
<tr>
<td></td>
<td>Concealment</td>
<td></td>
<td>• Full Disk Encryption</td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
<td></td>
<td>• Anti-virus, Anti-malware</td>
</tr>
<tr>
<td></td>
<td>Preventative Entry</td>
<td></td>
<td>• Device/OS Firewall</td>
</tr>
<tr>
<td></td>
<td>Secure Configuration</td>
<td></td>
<td>• Blacklist/Whitelist Applications, Services</td>
</tr>
<tr>
<td></td>
<td>Identity &amp; Authentication</td>
<td></td>
<td>• Geographical Restriction (Geofencing)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Admin &amp; Guest Account</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Indexing Encrypted Files</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Audit/Security Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Strong Key Session</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Application Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Password Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Least Privilege, Strong Authentication</td>
</tr>
</tbody>
</table>

To provide further context to the quantitative data, we commissioned a third-party research organization to conduct in-depth, exploratory interviews with senior executives from Fortune 500 organizations. We also conducted secondary research of recent studies by industry analysts.

Global Endpoint Risk Research

- **One billion** change events
- **Six million** devices
- **12,000** organizations (anonymized)
- **One-year** benchmark study
- **Five Fortune 500** executive interviews

Anonymized organizational and device data points analyzed:

- Industry
- Organization size
- Quantity of active/inactive security agents
- Quantity of active/inactive apps
- Quantity of active/inactive controls
- Recovery time of failed agents/apps/controls
- Operating system

\(^\text{11}\) World Economic Forum. 2018 Environmental Performance Index.