2021 Endpoint Risk Report

Four key trends impacting data and device security

Critical gaps to assess and monitor for maximum impact

ABSOLUTE®

Executive summary

The rapid shift to support new ways of working challenged even the most sophisticated organizations to maintain healthy security postures. Amidst an ever-evolving threat landscape, IT and security teams raced to adopt risk management strategies for environments that would have been unimaginable only two years ago.

Investment in cybersecurity technologies reached new heights but was outpaced by the increase in data breaches — and the average cost of a breach was significantly higher for organizations with remote teams.[2]

With 73% of respondents in a recent CSO study saying that the impact of the pandemic will alter the way their business evaluates risk for at least the next five years,[3] the third annual edition of Absolute's Endpoint Risk Report sets out to understand where organizations should focus their efforts now.

76% of IT security decision makers say their organization's use of endpoint devices increased since the beginning of the COVID-19 pandemic[1]

82% of IT security decision makers had to re-evaluate their security policies[1]

[1] Take a Proactive Approach to Endpoint Security, a commission study conducted by Forrester Consulting on behalf of Absolute, 2020
[2] 2020 Cost of a Data Breach Report, Ponemon Institute, 2020
[3] Pandemic impact report, CSO Online, 2020

Endpoint Visibility is the Key to Gaining Insight — and Control

If one theme binds the trends in this year's report, it is the unseen, unmanaged risks that result when organizations lack insight and control over their entire endpoint environment.

Unfortunately, complete endpoint visibility is difficult for many organizations to achieve. A recent Cybersecurity Insiders report found that 60% of organizations are aware of fewer than 75% of the devices on their network, and only 58% of organizations say they could identify every vulnerable asset in their organization within 24 hours of a critical exploit. Nine percent estimate it would take them one week or more.[4]

Four notable trends from this year highlight how, without this insight, organizations are dangerously — and often unknowingly — exposed:

- Vulnerabilities remain unaddressed
- More sensitive data on more devices than ever before
- Endpoint complexity is exacerbating risk
- Compromised security controls are widening the attack surface

[4] 2020 State of Endpoint Security Posture Report, Cybersecurity Insiders, 2020

Strategies to Reduce Risk

These trends are not universal. Many organizations emerged from this year with security postures measurably stronger than their peers. With Gartner CFO reporting that 74% of companies plan to permanently shift to remote work,[5] it's important to understand and embrace the strategies that set these top performers apart.

Absolute's 2021 Endpoint Risk Report explores cybersecurity trends within corporate environments. Featuring the findings from an extensive primary research study that analyzed nearly five million global enterprise devices and industry-specific insights, this report is intended as a benchmark for risk analysis and a blueprint for action.

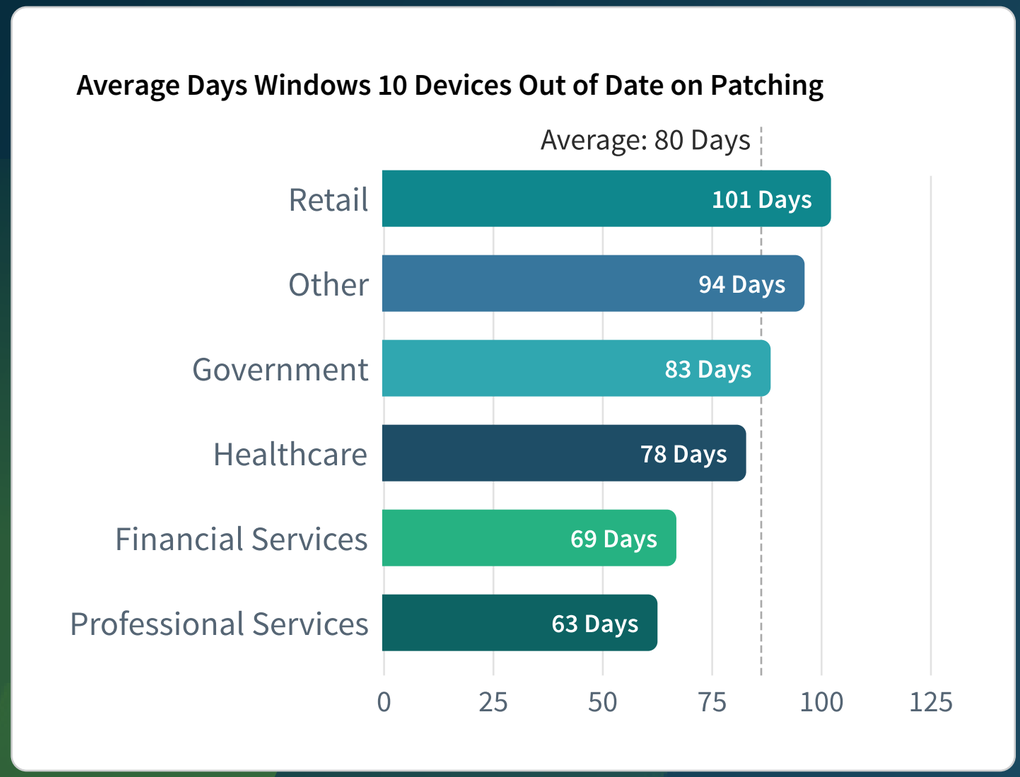
[5] CFO Actions in Response to COVID-19, Gartner, 2020

TREND 1

Vulnerabilities remain unaddressed

This year saw an expected increase in Windows 10 adoption but, perhaps surprisingly given the challenges of maintaining remote devices, a decrease in the length of time that endpoints were out-of-date with available OS patches — from 95 days last year to 80 days in 2021.

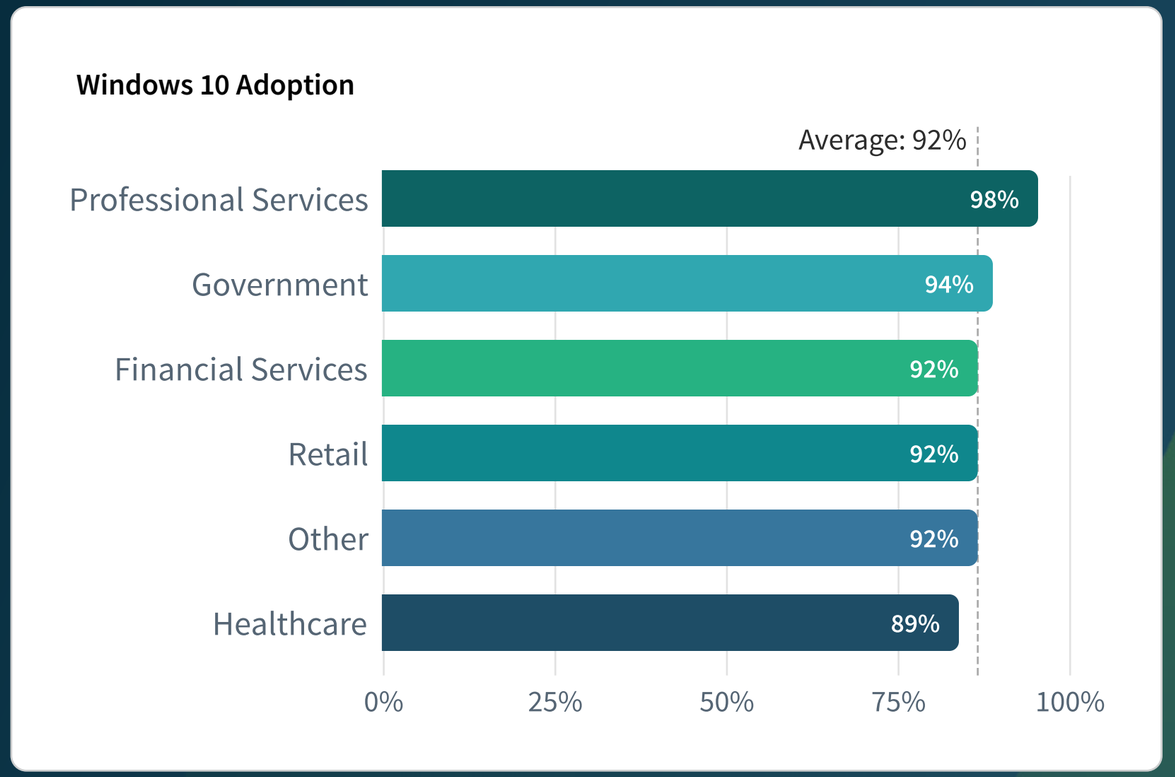
Over 40% of Windows 10 devices analyzed were running version 1909 — associated with over 1,000 known vulnerabilities.*



* Vulnerabilities calculated from CVE Details.

For some organizations, maintaining outdated or unsupported operating systems is a calculated risk, since some industries rely on core applications not yet compatible with current operating system (OS) releases.

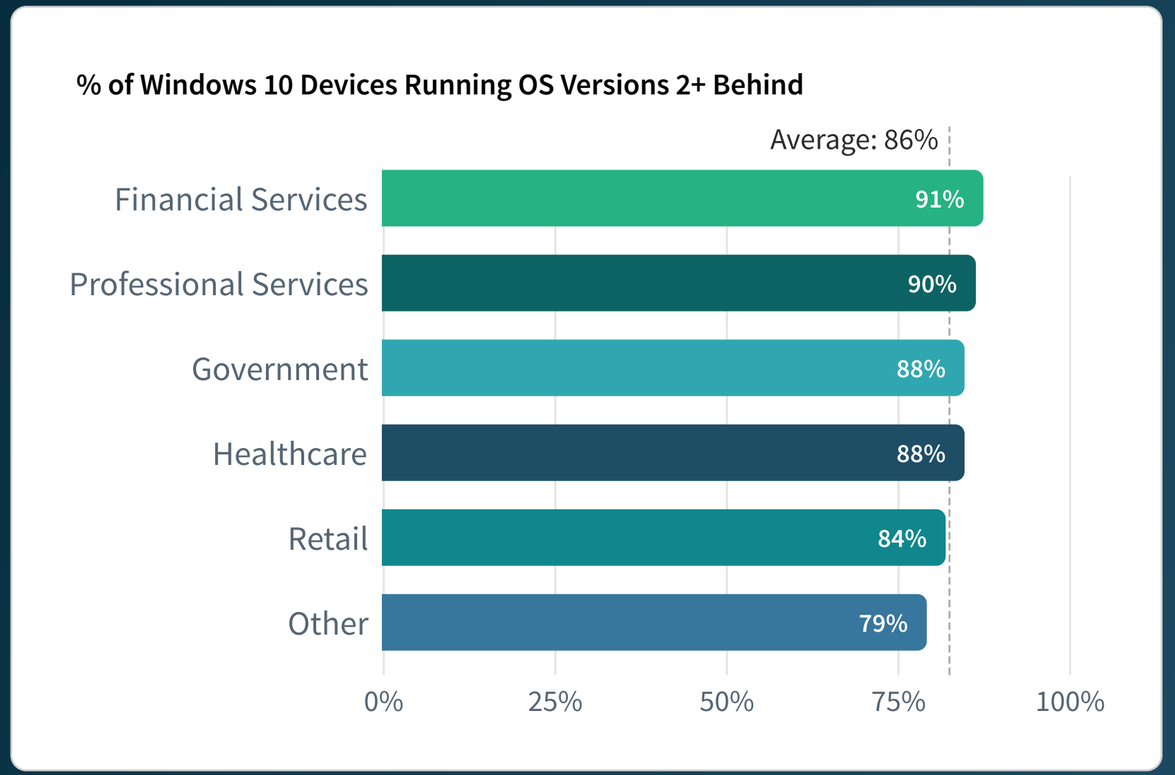
For example, Healthcare reports the highest proportion of endpoints running Windows 7, at 10%, and the lowest running Windows 10, at 89% — despite FBI warnings of an increase in successful cyberattacks in Healthcare when operating systems reach end-of-life.[6]



[6] Ransomware Activity Targeting the Healthcare and Public Health Sector, Cybersecurity and Infrastructure Security Agency, 2020

Within Windows 10 deployments, Financial Services shows the longest lag to upgrade, with 91% of devices two or more OS versions behind.

Within these environments — governed by strict regulations and entrusted with the data most targeted by would-be attackers — offsetting risk by ensuring the effectiveness of endpoint security controls is crucial.



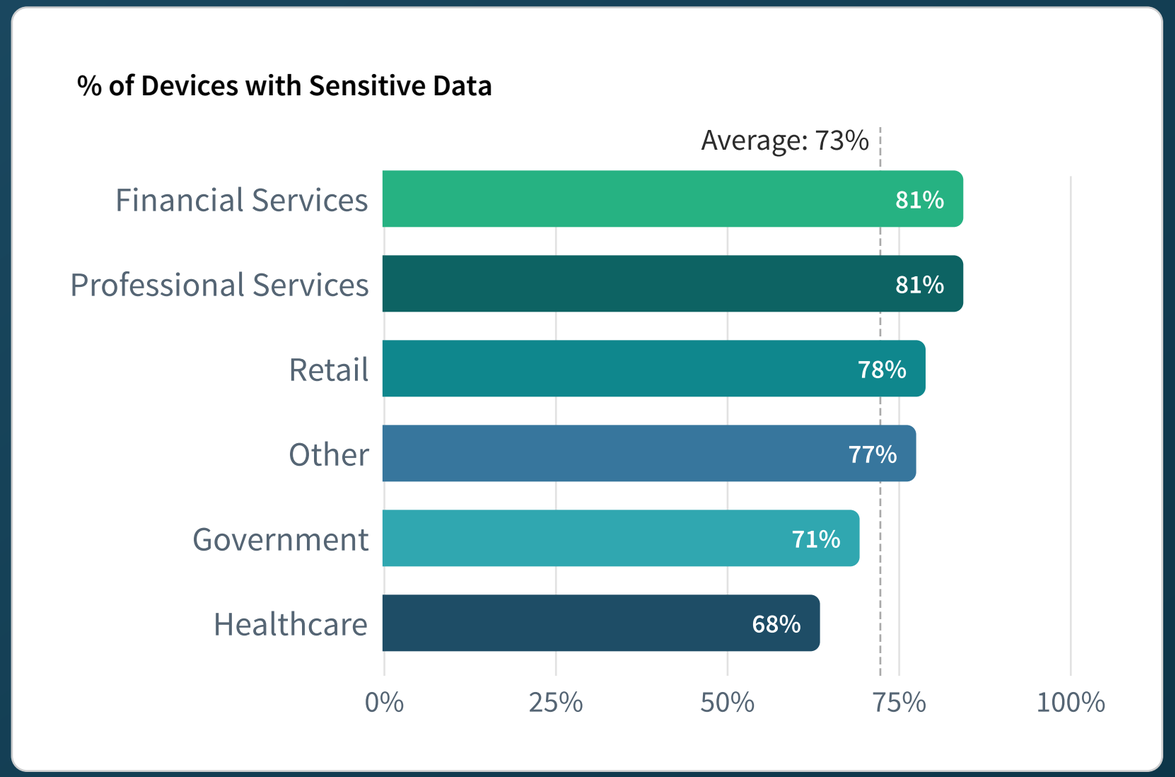
TREND 2

More sensitive data on more devices than ever before

Although every endpoint represents a potential target for cybercriminals, those containing sensitive data* pose a more serious threat. And this year, with more workers off-network and more information stored on local machines, that threat increased exponentially.

Research showed that no industry was immune, with 73% of analyzed devices containing sensitive data.

This number, coupled with dramatic increases in the amount of data most at risk — such as PII and PHI — per device underscores the need for automated discovery and remediation in today's newly remote world.



* "Sensitive data" is defined as any information that could create a data breach notification (e.g., credit card data, Protected Health Information (PHI), Personally Identifiable Information (PII)). Sensitive data can be identified but is not stored by Absolute.

Not only do most enterprise devices contain data that, if breached, could result in serious financial and reputational damage, the amount of at-risk data per device increased alarmingly this year.

Compounding the risk of exposure, 23% of devices with high levels of sensitive data also reported unhealthy encryption controls. This further underscores the need for automated discovery and remediation in today's newly remote world.

The amount of sensitive data per device has risen significantly year-over-year:

Overall 17%

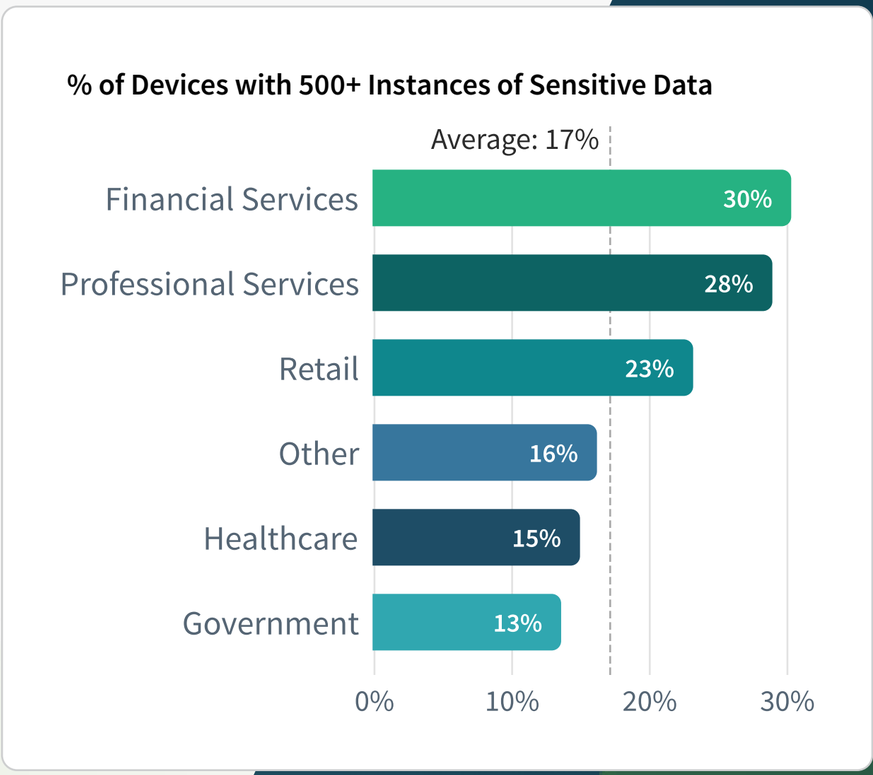
+10 percentage points increase from pre-COVID results.

Financial Services 30%

+15 percentage points increase from pre-COVID results.

Healthcare 15%

+12 percentage points increase from pre-COVID results.
Over half of sensitive data found on Healthcare devices is PHI

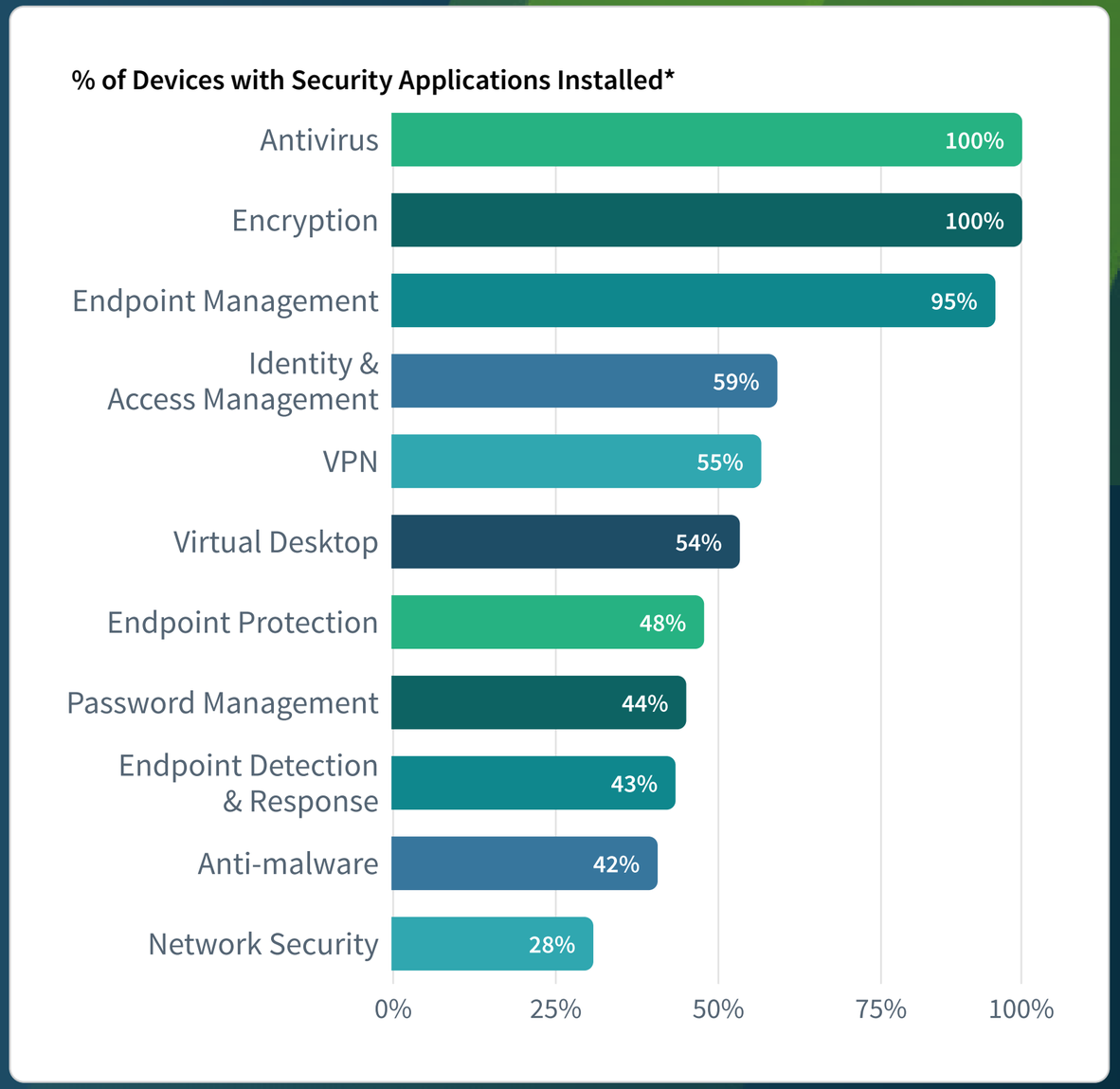


TREND 3

Endpoint complexity is exacerbating risk

The need to support and secure remote workforces drove an increase in the average number of applications installed per endpoint. With that came an accompanying risk of friction, failure, and non-compliance.

Enterprises now have an average of 96 unique applications per device, including 13 mission-critical applications. The number of security controls has also increased to 11.7 per device, with the majority of devices containing multiple controls with the same function. 100% of devices have at least one encryption application installed; 60% have two or more. 100% of devices have at least one endpoint management control; 52% have three or more. 59% of devices have at least one IAM installed, 11% have two or more.



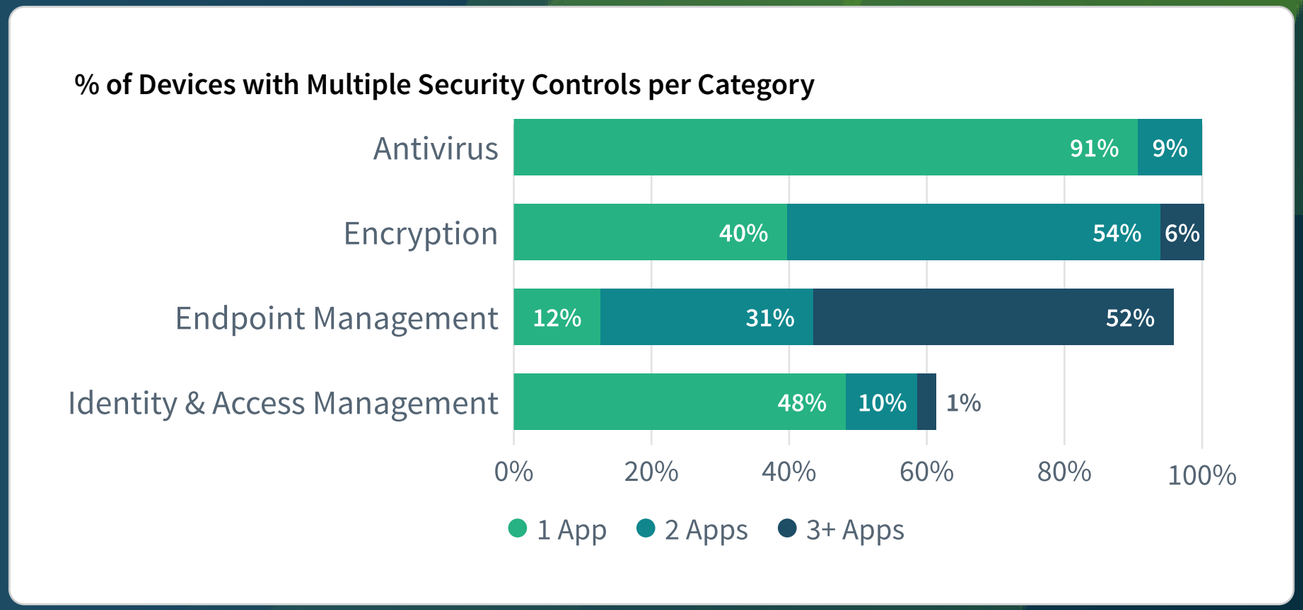
* Microsoft Defender Antivirus and BitLocker are factory-installed on every Windows device.

It's worth noting that this increased complexity is itself a security risk, as each new control adds friction to the endpoint environment, increasing the likelihood of collision and decay. The challenge of keeping applications up to date on remote devices — for example, when deploying patches off-network — increases the risk further still.

60% of devices have two or more encryption apps installed.

52% of devices have three or more endpoint management tools installed.

11% of devices have two or more IAM apps installed.



TREND 4

Compromised security controls are widening the attack surface

An enterprise's security posture is only as good as the applications that support it. As in previous years, failing applications continue to undermine the best efforts of many security teams.

Left unchecked, every one of the 11.7 security controls deployed on the average device is a potential attack vector. Complex environments cause security controls to collide and decay. Their effectiveness measurably degrades over time. And users wanting to circumvent restrictions may attempt to disable or remove them altogether.

With sophisticated attackers seeking access by any means, simply deploying protections such as encryption, VPN, antivirus, and anti-malware — and trusting that they remain effective — is not enough. To truly defend the endpoint and realize a return from these security investments, their effectiveness must be continuously monitored and maintained.

In organizations without these measures in place, one in four devices reported unhealthy applications at any given time, including critical protections.

25% of devices had unhealthy security controls at any time, including:

- **34%** Unhealthy Antivirus/Anti-malware
- **19%** Unhealthy Client Management
- **22%** Unhealthy Encryption
- **27%** Unhealthy VPN

Notably, “built-in” does not mean “better.” Twenty-one percent of Microsoft Endpoint Configuration Manager (MECM)* clients required repair or reinstallation within a 90-day period. Devices with both BitLocker™ and Microsoft Defender Antivirus reported the lowest encryption application health overall.

> Over one in five devices had unhealthy SCCM agents that needed to be repaired or reinstalled during a 90-day period.

* Formerly System Center Configuration Manager (SCCM)

Getting ahead of what comes next

More than two-thirds of North American companies surveyed by IDC said they struggle to strike the right balance between flexibility and security for remote work employees.[7]

As we return to a world of business travel, in-person conferences, and workforces newly enabled to work from anywhere, knowing where not to compromise is critical.

The trends covered in this year's report — unaddressed vulnerabilities, unprotected data, endpoint complexity, and failing security controls – underscore the critical role of device visibility and intelligence in identifying and mitigating risk in the modern workplace.

[7] Remote Work in the COVID-19 Era: Accelerating Work Transformation, IDC, 2020

Always-accurate endpoint telemetry, always-on endpoint control

An Absolute-commissioned report from Forrester found that 71% of organizations plan to extend their ability to see and monitor remote endpoints.[8]

Fundamental to achieving this is endpoint telemetry that provides the insight and control necessary to eliminate blind spots, identify weaknesses, and quickly mitigate threats.

Absolute's continuous stream of intelligence from every device includes granular geolocation data, sensitive data discovery, security control status, hardware performance, software inventory, and hundreds of additional data points, enabling teams to gauge security posture and remediate incidents in near real-time.

Devices are monitored both on and off network, and the data can be easily integrated into Security Information and Event Management (SIEM) systems for further enrichment and investigation.

[8] Take a Proactive Approach to Endpoint Security, a commission study conducted by Forrester Consulting on behalf of Absolute, 2020

Identify vulnerable endpoints

Absolute gives organizations the ability to see and manage every device — on or off network — from a single pane of glass.

Software misconfiguration and vulnerable operating systems are identified and surfaced automatically, while remote device management capabilities make it quick and painless to push updates and remediate vulnerabilities at scale.

Locate and remediate devices containing sensitive data

Given this year's concerning figures for sensitive data in the wild — and with remote work the new reality — prioritizing data risk management should be an immediate focus for every security professional.

With Absolute, organizations can identify, monitor, and secure sensitive data across their entire endpoint environment, with location and classification data surfaced alongside critical insights such as device encryption status.

Remote remediation capabilities include the ability to freeze or lock devices or render data irretrievable via cryptographic erasure.

Console-generated Certificates of Sanitization meet both NIST and HIPAA requirements which is key for regulated industries such as government, financial services, and healthcare.

Reduce endpoint complexity

Even before the shift to remote work, organizations struggled to manage increasingly complex endpoint environments. This is largely due to the rising number of applications being purchased and deployed to support remote workers and secure enterprise data.

There is currently an average of 12.9 mission-critical applications per enterprise device, 11.7 of which are security controls. As complexity on the endpoint increases, so too does the risk as applications conflict and collide with one another.

With Absolute, organizations can gain greater visibility into their devices to identify which applications are the most fragile. They can even extend Absolute's self-healing capabilities to their most valuable applications to ensure mission-critical controls remain in place and avoid productivity or security challenges.

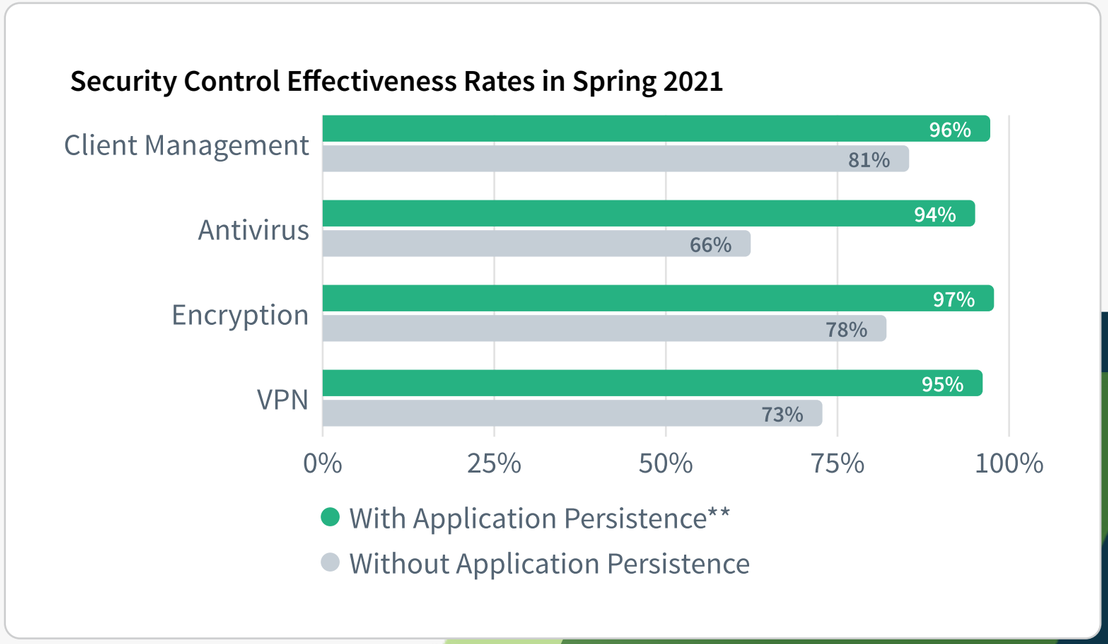
Security Control Effectiveness Ratings

Whether it’s a negligent or malicious employee, a vulnerability in software, or a physical security compromise, the vast majority of data breaches begin at the endpoint.[9]

Organizations therefore need to tackle the issue of unmonitored security controls. Absolute's Application Persistence™ service maintains the effectiveness of security controls by continuously measuring their effectiveness* and empowers the controls to automatically repair or reinstall themselves if they become compromised.

Devices running Absolute's Application Persistence report security control effectiveness 21% higher than those without.

Absolute's Application Persistence provides this capability for over 40 leading endpoint security controls, with more added all the time.



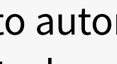
[9] 2020 Cost of a Data Breach Report, Ponemon Institute, 2020
* Effectiveness is determined by the current health and state of decay of controls, as well as their ability to react to attack, collision, and/or damage.
** Top performing customers with Absolute's Application Persistence™ service

Security + resilience = peace of mind

Absolute fortifies endpoint environments with Endpoint Resilience™ — the ability for endpoints and their security controls to autonomously maintain a secure operating state. Visibility and control are uncompromised and security investments protect the organization as intended — even in the face of inevitable cyber incidents.

Absolute's patented Persistence® technology is embedded in device firmware by 28 leading system manufacturers, including Dell, Lenovo, and HP.

Activating the Absolute agent creates a secure, unbreakable connection to every endpoint — even off-network — with hardware-level intelligence that enables endpoints to automatically detect and recover from potential threats.



Wondering how your organization stacks up?

Register for a custom demo and learn how to address these risks in your organization.

Register now

Report methodology

We analyzed anonymized data from nearly five million Absolute-enabled devices active across 13,000 customer organizations in North America and Europe as well as data and information from trusted third-party sources.

About Absolute

The Absolute Platform for Endpoint Resilience® enables devices and security controls to maintain a secure operational state automatically, without user intervention. Embedded in the firmware of over half a billion devices, Absolute is uniquely able to provide continuous visibility, control, and intelligence of the entire endpoint environment – data, devices, and applications.

Our self-healing connection and granular endpoint telemetry allow IT and security teams to streamline device management, maintain compliance, remediate threats, and help ensure that endpoint security controls are always installed, effective, and delivering their intended ROI.

ABSOLUTE.COM SALES@ABSOLUTE.COM NORTH AMERICA | EMEA

Linkedin Twitter Youtube

Secure Your Devices with the Self-Healing Power of Endpoint Resilience

Contact us by email or call 1-877-600-2295 for a custom demo.

Book a demo