2020: The State of Endpoint Resilience™ Report

New research reveals gaps in enterprise device security and endpoint application health

ABSOLUTE®

Executive Summary

As we pulled together the second annual edition of 'The State of Endpoint Resilience Report,' and looked back at the trends in enterprise and endpoint security over the last year, what we found to be most striking is both how much has changed and how much has stayed the same. Last year's inaugural edition revealed many complexities plaguing the modern enterprise, and led us to the stark conclusion that **endpoint complexity itself is a vulnerability**. Our data shows this to be true even more so this year.

This complexity is being driven by three critical factors:

- **An increasing number of agents piling up on devices – 10.2 on average, up from 9.8 last year**
- **Device OS migration, resulting in fragmentation and stagnant patching practices**
- **Fragile security controls, and their varying rates of decay and collision**

This all adds up to a continued struggle to maintain foundational security hygiene practices, such as patching critical vulnerabilities, as well as protecting devices, data, and users. It also results in a struggle to maintain resiliency.

New in this year's edition, we've leveraged our endpoint intelligence to measure Application Resilience™, which we define as the health of endpoint security controls, as well as their ability to react to collision or damage. Understanding the health and behavior of commonly deployed endpoint applications, as well as application pairings, is integral to enabling IT and security teams to maximize app effectiveness and optimize security investments.

Ensuring security controls are working and delivering their intended value is especially critical in the wake of a global health crisis that incited a sudden and seismic shift in the way that the enterprise operates. The COVID-19 outbreak has affected communities and companies of all sizes, across all industries around the world, and has caused the blurred lines loosely defining today's traditional office 'perimeter' to swiftly disappear altogether. As businesses were mandated to send employees to work from home, managing device sprawl and securing endpoints became an even bigger challenge.

Like many other companies, we raced to help customers navigate the rapid shift to remote work and keep their businesses running. We leveraged our single-source-of-truth intelligence to deliver the insights enterprises needed to benchmark the health of their endpoint security posture – both before the onset of the COVID-19 outbreak, and in the months since. What we uncovered is that, in remote environments, the use of enterprise devices and collaboration apps is skyrocketing, sensitive data is piling up, and already fragile security controls are leaving gaps or blind spots that malicious actors stand ready to exploit.

If there's one thing that came clearly into focus, especially as remote and hybrid work models become the new reality, it's that there has never been a more critical time for **Endpoint Resilience**. The insights that follow are designed to help enterprises strengthen their security posture, and build the resilience needed to continue to face today's – and tomorrow's – cyber challenges head on.

It was estimated that skyrocketing cybercrime costs could hit $6 trillion annually by 2021, and it's now estimated that those costs could potentially double during the coronavirus outbreak period.

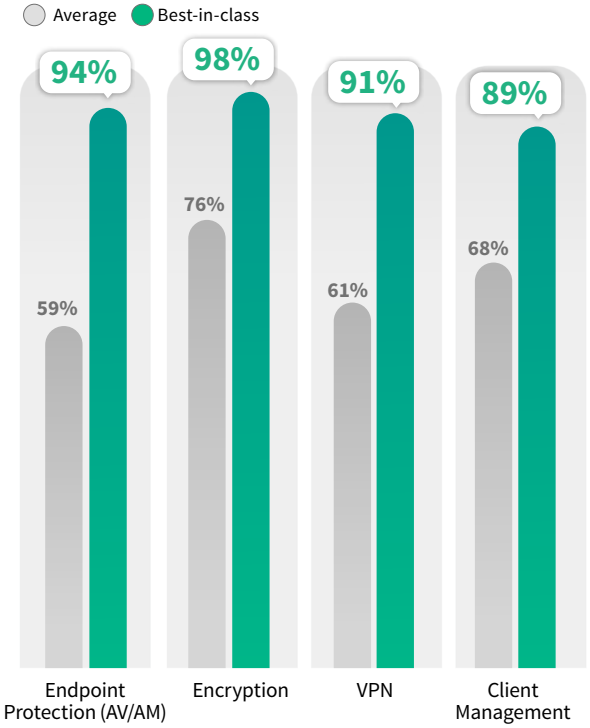
– Cybersecurity Ventures

Key Insights

This second annual edition examines the complexity of enterprise endpoint environments, the fragility of mission-critical security controls, and the overall health and resiliency of devices and applications.

Security Controls Remain Fragile

Average app compliance rate across enterprise devices*



The Power of Persistence

Best-in-class' enterprises using Absolute's Application Persistence™ solution see vast improvements in average compliance rates for critical controls, as compared to those that have not yet activated Application Persistence.

**Application compliance as defined by Absolute and specific to each of the categories listed.*

Drivers of Complexity

78%
enterprise devices running Windows 10, up from 54% last year

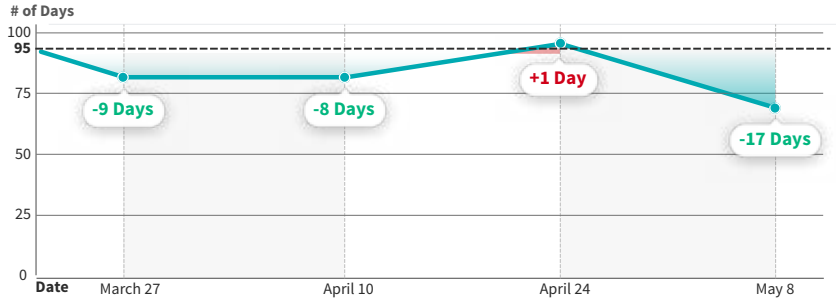
10.2
unique security controls deployed on the average endpoint device, up from 9.8 last year

96
unique applications installed on average enterprise device

419
total patch levels detected across Windows 10 Enterprise Devices

90%
Windows 10 enterprise devices running two or more versions behind

Windows 10 Fragmentation and Patching Delays



Outdated Means Vulnerable
It is unsurprising that, with so much fragmentation, the average Windows 10 enterprise device was found to be more than three months behind in patching, pre-COVID-19. Even with glimmers of improvement seen in the weeks following the outbreak, the average delay hovered well above two months.

60% **of data breaches last year were linked to a vulnerability with a patch available but not applied …**

despite a 34 percent increase, year-over-year, in weekly costs dedicated to patching.

SOURCE: "Costs and Consequences of Gaps in Vulnerability Response," ServiceNow, 2019

Endpoint Application Landscape Overview

Of the ten or more endpoint agents running on the average enterprise device, these are some of the most commonly deployed across Absolute's customer base in prominent categories.

74%

3 in 4 enterprise devices are running Microsoft BitLocker™ Device Encryption

23%

Nearly 1 in 4 devices are running Microsoft Windows Defender AV

80%

4 in 5 enterprise organizations are using Cisco VPN or AnyConnect®

Two thirds

of organizations believe remote work environments have an impact on their compliance posture

SOURCE: "Bitglass 2019 Cloud Security Report" Bitglass, 2019

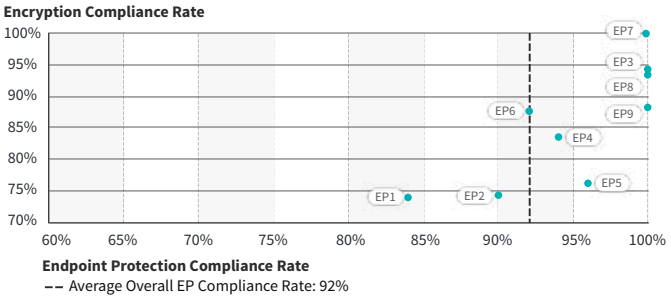
164.7M

Total number of sensitive records exposed in 2019, according to the Identify Theft Resource Center

SOURCE: "Identify Theft Resource Center, 2019 Data Breach Report"

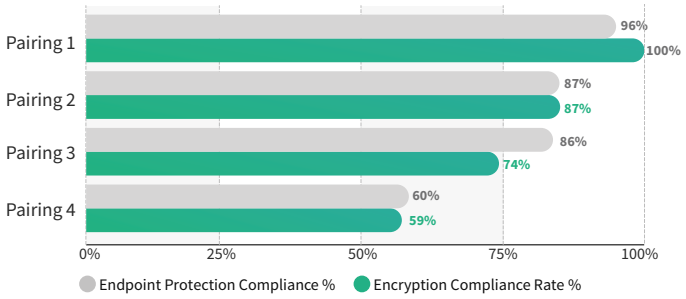
Complexity Affects Application and Endpoint Resilience

This chart gives a snapshot of the health and resiliency, or average compliance rates, of common Endpoint Protection apps deployed across enterprise devices.



App Pairings Show Varying Health and Resilience Levels

In this report, we've introduced the concept of Application Resilience™, which we define as the measure of health and compliance of critical endpoint security controls.

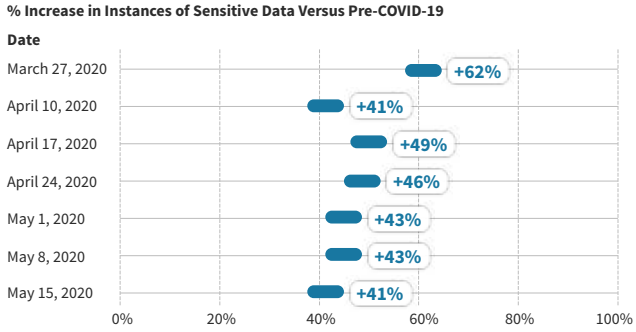


We analyzed the average compliance rates of common endpoint and encryption pairings to emphasize that no agent is immune to failure, and even those sourced from the same vendor are not guaranteed to work seamlessly together.

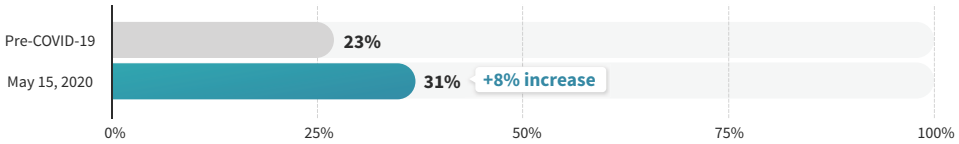
COVID-19 Outbreak Sends Vulnerable Endpoint Devices, Data Home

Sensitive Data Piles Up on Remote Enterprise Devices
Our data shows a spike in the amount of PII, PHI, and PFI identified on enterprise endpoints in the wake of devices going home to work remotely, versus pre-COVID-19.

*Absolute's Endpoint Data Discovery does not collect or store this information; it merely identifies if it is present on an endpoint device.



Increase in Heavy Device Usage*



*Defined as eight or more hours of usage per day

Data Gathering and Methodology

8.5 million

Anonymized data collected from 8.5 million active, Absolute-enabled devices

12,000+

Across more than 12,000 enterprise customers worldwide, in wide range of industries

2019 - 2020

Data gathered and analyzed over the period of November 2019 - May 2020

Endpoint Environments Fraught with Complexity

Even before the global COVID-19 outbreak, enterprise organizations have struggled with managing increasingly complex endpoint environments – driven largely by the rising number of applications being purchased and deployed.

Number of security controls per average enterprise device: **10.2**

Total installed applications on average enterprise device*: **96**

**Includes company-approved security and productivity applications and services, as well as those installed by the end user.*

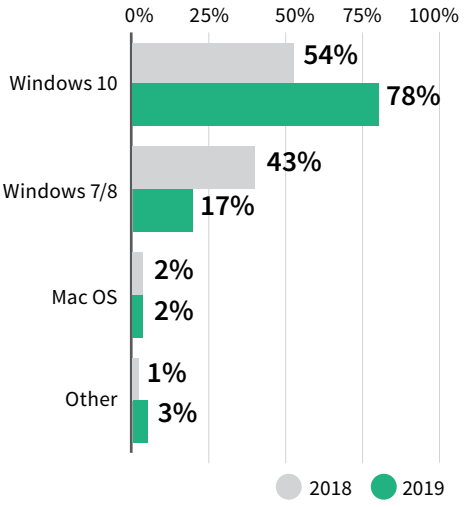
Strong Windows® 10 Migration, but Fragmentation Creates Challenges

78% of enterprise endpoint devices running Windows 10

The vast majority (78%) of Absolute-enabled enterprise devices are running Microsoft Windows 10, representing a notable year-over-year jump from 54 percent. In parallel, we saw a significant decrease in the share of enterprise devices running Windows 7 or 8 – likely attributed to organizations migrating away from these versions minimally or no longer supported by Microsoft.

Figure 1

Percentage of Enterprise Devices by OS, Year-over-Year



9 major Windows 10 versions available**

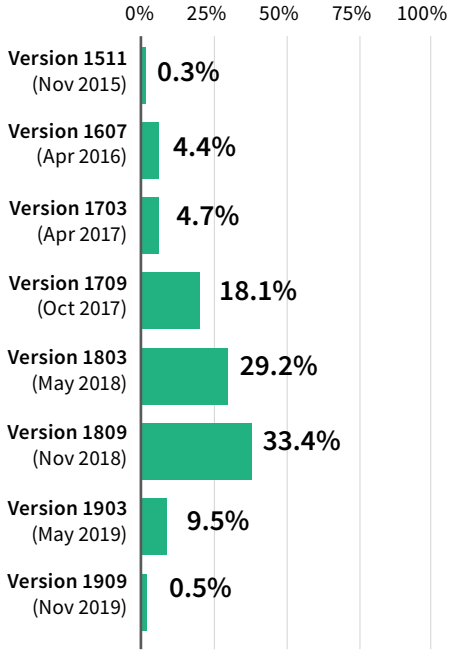
10% of Windows 10 enterprise devices running two most recent versions (Version 1903 or 1909)

While promising to see that so many organizations have adopted Windows 10, our data found 90 percent of Windows 10 enterprise devices to be running two or more versions behind – with less than one percent having been upgraded to the latest available version released in November 2019 (at the time of analysis).

*** Version 2004 had not yet been released at time of analysis.*

Figure 2

Total % of Windows 10 Enterprise Devices by Version



Fragmented Patching Leaves Organizations Exposed

95 days: Average patching delay across Windows 10 enterprise devices

419: Windows 10 patch levels detected across enterprise devices

In addition to twice-yearly major version releases, Microsoft delivers monthly quality and security updates for up to 30 months after a version is made available. As of February 2020, there were more than 400 unique build releases or patch levels recorded across Absolute-enabled Windows 10 enterprise devices.

With new build releases continuing to emerge each month on Microsoft's Patch Tuesday, it is unsurprising that our data found the average Windows 10 enterprise device to be more than three months behind in applying the latest security patches.

If we tally up the number of vulnerabilities addressed on Patch Tuesday in February through May 2020 alone, it shows that the average Windows 10 enterprise device has hundreds of potential vulnerabilities without a fix applied – including four zero-day vulnerabilities.

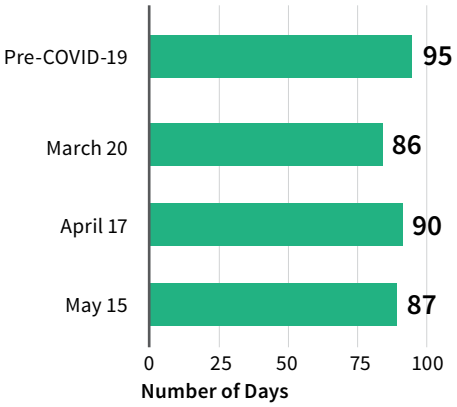
This delay is concerning, notably in remote work environments where successfully deploying patches to off-network devices comes with its own set of challenges. Unpatched software vulnerabilities remain a common attack vector for cybercriminals — **one recent study** found that 60 percent of breaches can be linked to a vulnerability where a patch was available, but not applied.

Average Patch Delay Since COVID-19 Outbreak

While we've seen glimmers of improvement in Windows 10 patching delays as enterprise devices went home in the weeks following the COVID-19 outbreak, the average time to patch has continued to hover well above two months.

Figure 3

Average Windows 10 Patch Age, Pre- and Post-COVID-19 Outbreak



Endpoint Security Controls Remain Fragile

An enterprise's security posture is only as strong as the applications that support it. With challenges introduced by fragmentation and complexity, and more than 10 agents deployed on the average enterprise device, the probability of critical endpoint apps colliding, decaying and failing to stay health and compliant only continues to rise.

Last year's report revealed one in five devices had an outdated antivirus (AV) agent — and seven percent of devices were missing one altogether — while more than 10 percent of devices had an encryption agent that required one monthly repair.

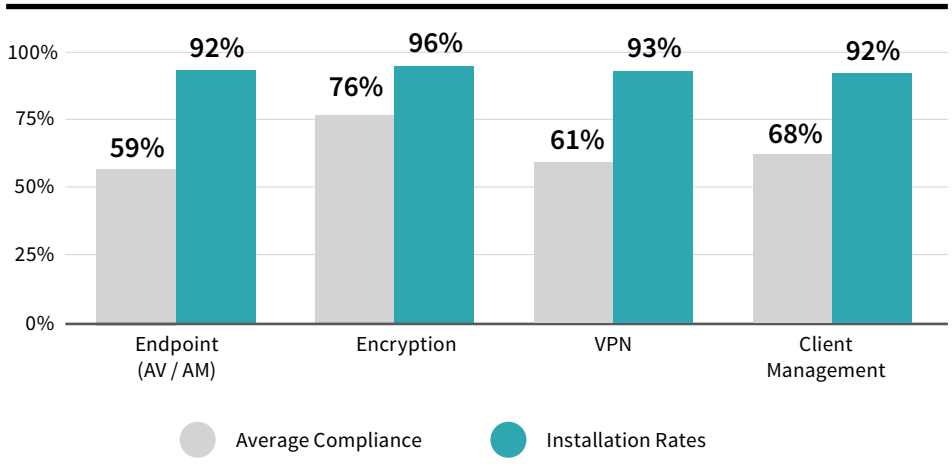
This year, while we conducted our analysis a bit differently, the results paint a picture of security controls that are just as — if not more — fragile than we saw previously.

Our data found that nearly one in three enterprise devices had an Endpoint Protection (EP), client management or VPN application out of compliance, and more than five percent of enterprise devices were missing one or more of these critical controls altogether.

Note: For the purposes of this report, AV and anti-malware apps are included in the Endpoint Protection category.

Figure 4

Security Controls: Average Compliance Rate / Installation Rate ***



***Security compliance as defined by Absolute. These compliance rates reflect those seen across 'Average' enterprise accounts that do not yet have Absolute's Application Persistence™ technology running.

Categories and associated compliance rates are defined as:

- **EP (AV/AM):** Software designed to prevent malware or viruses from causing an infection on a computer. Compliant AV means that the definition has been updated within 45 days.
- **Encryption:** The process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Compliant encryption means that a fully-activated encryption volume was identified on the device.
- **VPN:** Extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Compliant VPN means that the version is current, and key components are installed and functioning.
- **Client Management:** Software used for remote control, patch management, operating system deployment, network protection and other various services on a computer. Non-compliance factors typically include missing data, data pending, reboot pending, or health check fail.

Endpoint Application Landscape Overview

Of the ten or more endpoint agents running on the average enterprise device, these are some of the most commonly deployed across Absolute's enterprise customer base in prominent app categories.

NOTE: Only includes apps or app pairings running on five percent or more of Absolute-enabled enterprise endpoint devices or enterprise accounts.

Figure 5
Endpoint Protection (AV/AM)

McAfee® Endpoint Security	**24%**
Microsoft Windows Defender AV	**23%**
Symantec™ Endpoint Protection	**21%**
Cylance-PROTECT® by BlackBerry®	**10%**
Trend Micro Apex One™	**8%**
Sophos® Endpoint Protection	**5%**

SOURCE: Percentage of total enterprise devices with these applications installed.

Figure 6
Encryption

Microsoft BitLocker™ Device Encryption	**74%**
Symantec Drive Encryption, Desktop Encryption	**9%**
McAfee Complete Data Protection	**7%**

SOURCE: Percentage of total enterprise devices with these applications installed.

Figure 7
Virtual Private Network (VPN)*

Cisco VPN, AnyConnect®	**80%**
Citrix Receiver™ (now Citrix Workspace™)	**65%**
Pulse Secure® VPNs	**25%**
FortiClient® by Fortinet®	**13%**
WatchGuard® Mobile VPN	**9%**
Check Point® Capsule	**9%**
F5® VPN	**7%**

Figure 8
Client Management*

Microsoft Systems Center Configuration Manager (SCCM)	**63%**
ManageEngine™ Desktop Central	**20%**
Quest KACE®	**18%**
Connectwise Automate™	**11%**
Kaseya® Network Monitoring	**10%**

** SOURCE: Percentage of total customers with these applications installed. Because organizations may have multiple tools in a particular category installed across their fleet of devices, total percentage number may exceed 100.*

Customer Insight

> *"I trust Absolute. We always buy it for every laptop."*

Paul Baird
IT Security Operations Manager
Bovis Homes

Due to the large number of temporary employees working remotely at Bovis Homes, a residential development company in the UK, devices often went rogue. From a GDPR compliance perspective, a lack of clarity into their security posture was concerning. Without knowing how many devices they actually had, the location of each device, or the encryption status, Bovis Homes' IT team realized the company was at risk.

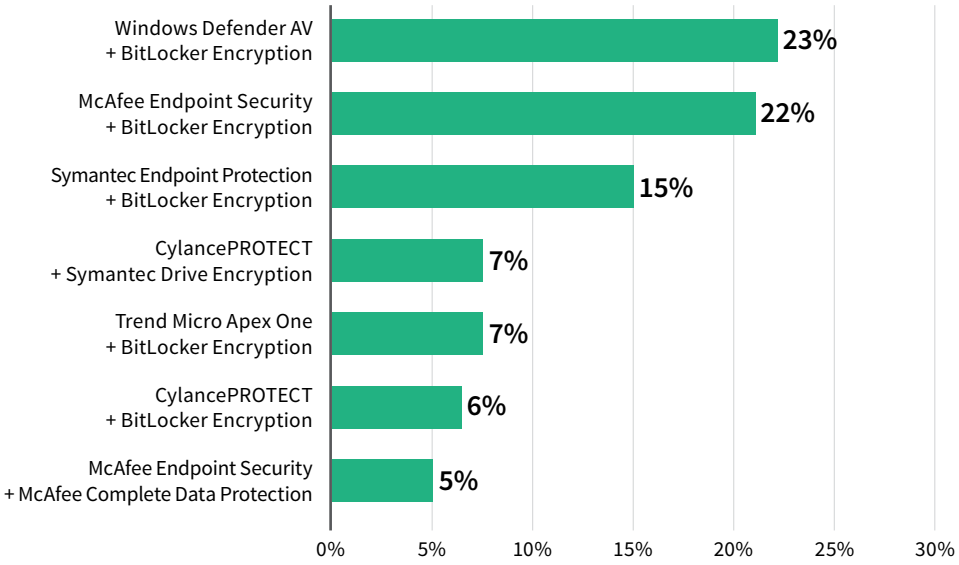
Engaging in a proof of concept with Absolute showed them what the status of encryption was at all times, on every device — and Absolute is now a staple across Bovis devices.

Endpoint Protection (AV/AM) and Encryption Pairings

When it comes to the most widely deployed cohorts of AV and encryption apps, we see that organizations are clearly taking advantage of the AV and encryption agents available natively in Windows 10, Microsoft Windows Defender AV, and BitLocker Encryption. Even more notably, BitLocker Encryption is present in four of the five most common AV and encryption pairings seen across enterprise devices.

Figure 9

Endpoint Protection (AV/AM) and Encryption Pairings



SOURCE: Percentage of total enterprise devices with top endpoint protection and encryption applications installed.

Measuring Application Resilience™

New in this edition, we've introduced the concept of Application Resilience, which we define as the measure of health, compliance and endpoint security controls, as well as their ability to react to attack, collision or damage.

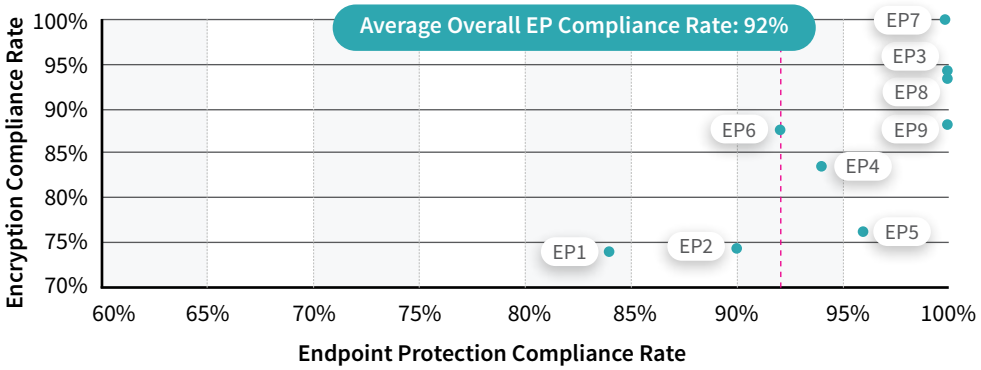
In this section, we've leveraged our unique endpoint intelligence and anonymized data to measure the health and compliance of common endpoint protection and encryption apps and app pairings, across Absolute-enabled enterprise devices.

Understanding potential conflicts between endpoint agents, and how various combinations of security controls might work together, is integral to ensuring the highest levels of Application Resilience – and, ultimately, Endpoint Resilience.

Application Resilience Snapshot: Endpoint Protection (AV/AM)
This chart gives a snapshot of the average compliance rate of common endpoint protection apps, as well as the average compliance rate of the encryption agent deployed on the same enterprise device.

Figure 10

Endpoint Protection (AV/AM): Average Compliance Rates

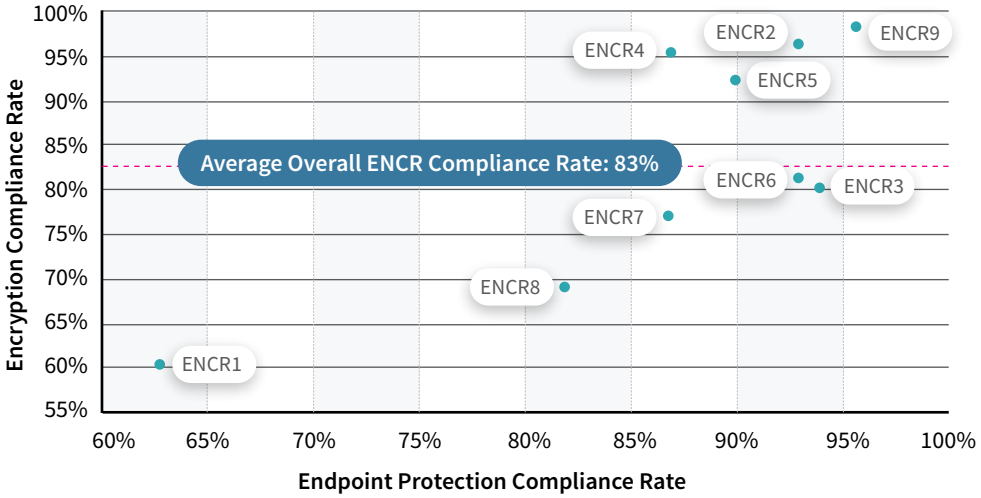


SOURCE: Subset of Absolute-enabled enterprise devices with the most common endpoint protection and encryption agents installed.

Application Resilience Snapshot: Encryption
This chart gives a snapshot of the average compliance rates of common encryption apps deployed across Absolute-enabled enterprise devices.

Figure 11

Encryption: Average Compliance Rates



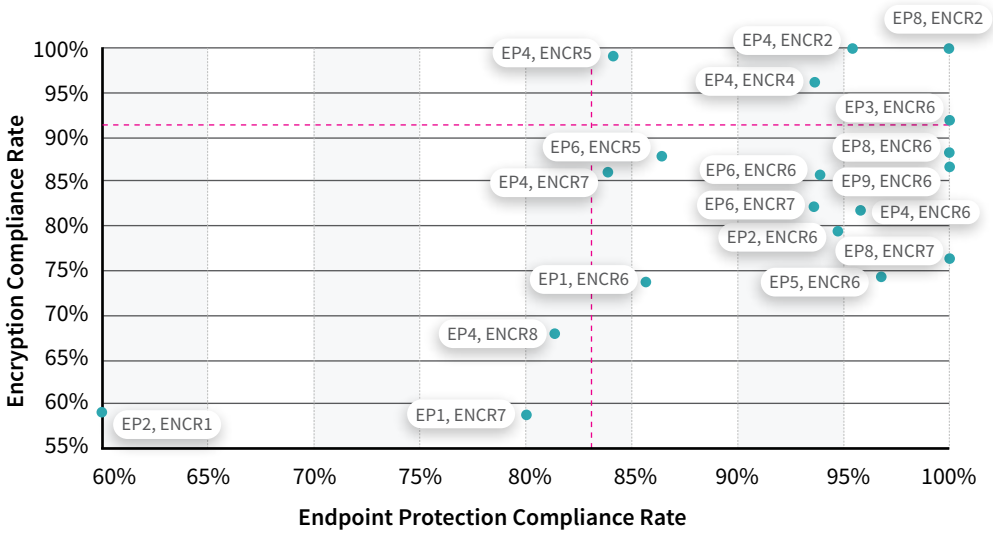
SOURCE: Subset of Absolute-enabled enterprise devices with the most common endpoint protection and encryption agents installed.

Application Resilience Snapshot: Endpoint Protection + Encryption Cohorts

One particularly interesting insight we uncovered upon examining common endpoint protection and encryption app pairings was that the resiliency of an application can vary dramatically based on what else it is paired with. Additionally, same-vendor pairings did not necessarily fair better or show higher average compliance rates than pairings from different vendors, which tells us that sourcing agents from a single vendor does not guarantee that those agents will work seamlessly together.

Figure 12

EP & Encryption Pairings: Average Compliance Rates



SOURCE: Subset of Absolute-enabled enterprise devices with the most common endpoint protection and encryption agents installed.

The endpoint protection applications analyzed in this section include Crowdstrike Falcon®, CylancePROTECT by BlackBerry, FireEye® Endpoint Security, Microsoft Windows Defender AV, McAfee Endpoint Security, Symantec Endpoint Protection, Sophos Endpoint Protection, Traps™ by Palo Alto Networks®, Trend Micro Apex One.

The encryption applications analyzed in this section include Check Point Capsule, Dell Encryption and Credant Technologies (acquired by Dell), McAfee Complete Data Protection, Microsoft BitLocker Device Encryption, Symantec Endpoint Encryption and Symantec Desktop Encryption (formerly PGP Desktop Encryption), Trend Micro Endpoint Encryption.

NOTE: Apps listed alphabetically by vendor name; alphabetical order does not in any way correspond to numerical order used in above compliance charts.

COVID-19 Outbreak Sends Vulnerable Data and Devices Home

The COVID-19 outbreak brought a sudden and sizable shift to the way enterprise organizations operate, sending millions of employees and endpoint devices home to work remotely. With most organizations ill-prepared to manage and secure remote work environments — while relying on already fragile security controls — the number of potential vulnerabilities and endpoint security blind spots are putting them at heightened risk of a potential breach or privacy-related compliance violation.

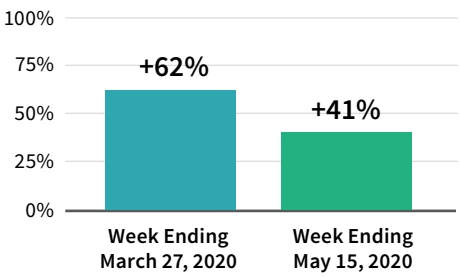
Sensitive Data Piles Up on Remote Devices

Directly on the heels of devices being sent home in mid-March, our data shows a significant and sustained spike in the instances of sensitive data – such as Personally Identifiable Information (PII) and Protected Health Information (PHI) – identified on enterprise endpoints, compared to pre-COVID-19.

NOTE: Absolute's Endpoint Discovery Tool does not collect or store this information; it merely indicates if this type of information is present on endpoint devices.

Figure 13

% Increase in Instances of Sensitive Data on Enterprise Devices, Versus Pre-COVID-19



Increase in Device Usage, Collaboration Apps Expands Attack Surface

Our data also shows a massive increase of 176 percent in the number of enterprise devices with collaboration apps installed as of May 15, 2020, as well as a 50 percent increase in the number of devices being used heavily (8+ hours per day), compared to pre-COVID-19.

While video conferencing and instant messaging apps have become practically indispensable in remote work environments, their skyrocketing usage has caught the attention of malicious actors looking to exploit software vulnerabilities, gain access to confidential information, and run social engineering schemes. So, it is critically important for IT and security teams to ensure these types of apps running on employee devices are sanctioned, up-to-date and fully secured.

Figure 14

% Increase in Number of Enterprise Devices with Collaboration Apps Installed, Versus Pre-COVID-19

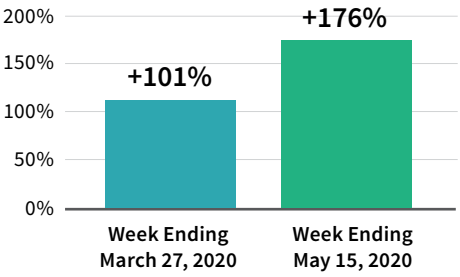


Figure 15

Percentage of Enterprise Devices Used Heavily (8+ Hours / Day)

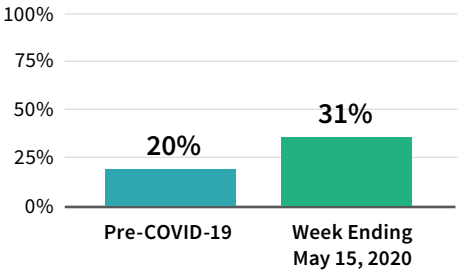
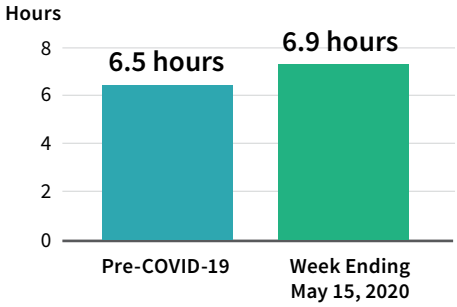


Figure 16

Average Active Daily Hours Per Enterprise Device



****For the purposes of this dashboard, the following apps are considered 'collaboration apps:' Cisco WebEx®, Zoom, Skype™, Microsoft Teams™, Slack®, Blue Jeans, Pidgin, Flock, GoToMeeting®, Microsoft Lync, and Join.Me®

One-third (33%) of organizations said they were not fully prepared for a rapid shift from on-premise to remote work.

– *Pulse Secure*

Endpoint Resilience Requires An Unbreakable Connection

The key takeaway here? The continuously increasing number of endpoint controls being deployed are creating a false sense of security across today's enterprise as all security controls are prone to some amount of decay.

Our data shows that it is time to shed the longstanding belief that the more you buy, the more secure and protected your organization, devices and data will be. The truth is that every security agent added to an endpoint device has the potential to accelerate complexity and risk exposure, contribute to application decay, and affect overall device health and security.

And with COVID-19 likely forever changing the way we work, this level of vulnerability and complexity is multiplying exponentially. Users, as well their devices, are working harder than ever before — and so are the security controls that have been tasked to protect them. Even as the future of the enterprise remains largely uncertain, and the 'Next Normal' only loosely defined, the one known is that remote work will play a significant role indefinitely.

IT and security teams need to ensure that their organizations can run effectively and securely within whichever operating model they choose to adopt, and that devices and sensitive data are protected no matter where they are. And they need to ensure their enterprise security approaches are built on Endpoint Resilience — an emerging and critical KPI for enterprise security strategy.

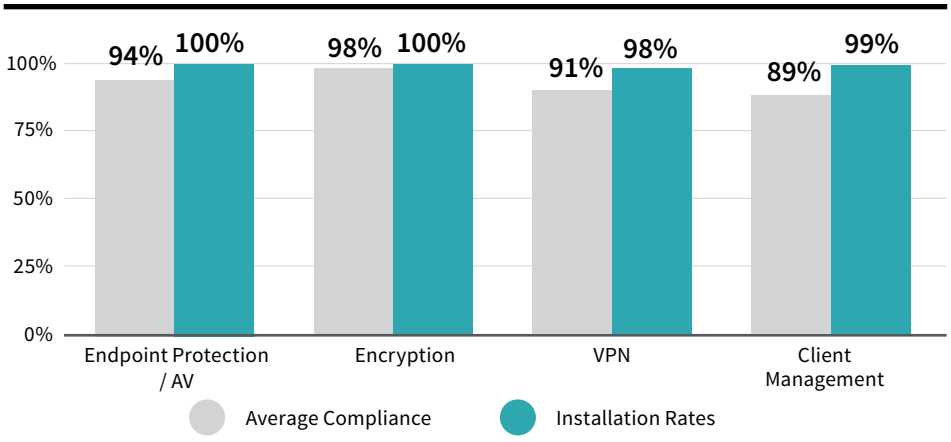
Endpoint Resilience requires a digital tether that provides an unbreakable connection between the endpoint and the enterprise who distributed it. Its purpose is to be the lifeline and single source of truth: to know where devices are, what apps are installed and healthy, and where there are vulnerabilities. Most importantly, it delivers the ability to persist and self-heal the mission-critical apps on that device, should it be necessary, whether on or off the corporate network.

The Power Of Persistence And Self-Healing

Absolute's patented Persistence® technology provides organizations with the ability to self-heal their critical security applications when they're disabled, altered or otherwise made vulnerable. Our data shows that enterprise organizations using Application Persistence™ see vast improvements – upwards of 20 percentage points – in average compliance rates in these critical app categories.

Figure 17

'Best-In-Class' Security Control Health: Average Compliance / Installation Rates



SOURCE: Enterprise accounts with 'mature deployments' with Absolute Persistence turned on. 'Best-in-Class' is defined as customers using Application Persistence to maintain the health and compliance of their critical security apps.

Customer Insight

> *"As a CIO, Absolute gives me peace-of-mind so I can sleep at night. It has strengthened our security posture, allowing us to stay in compliance and giving us that extra level of comfort."*

George Gunther
VP & CIO
Asplundh

With Absolute, Asplundh can ensure critical security applications have self-healing capabilities on all endpoints, no matter the location – which provides persistent protection against a security compromise.

Absolute is the industry's only undeletable defense platform, embedded in the firmware of more than a half billion devices and deployed across more than 12,000 customer organizations. This unique position enables our customers to look at endpoint protection holistically – to see the complete picture and create a feedback loop that enables IT and security teams to eliminate blind spots. We're defining the next generation of endpoint security — true Endpoint Resilience.

To learn more about how your organization can achieve Endpoint Resilience with Absolute, contact an Absolute sales representative at **sales@absolute.com** or 1-877-600-2295, or request a demo **here**.

Find out how our solutions can benefit your organization.

REQUEST DEMO

Report Methodology

This report leverages anonymized data from enterprise-specific subsets of nearly 8.5 million Absolute-enabled devices active across 12,000+ customer organizations in North America and Europe.

Types of anonymized endpoint device data that was analyzed include:

- Device operating system and latest version installed
- Number of security applications installed
- Names and types of security applications installed
- Compliance rates of security applications, based on Absolute-defined parameters

Pre-COVID-19 insights use data points collected in late 2019 (November–December). Insights that reflect trends or changes seen in post COVID-19 outbreak timeframe use data points collected from late March through late May 2020.

This report also includes certain data and information from trusted public third-party sources, which is cited accordingly.

About Absolute

Absolute serves as the industry benchmark for Endpoint Resilience, visibility and control. Embedded in over a half-billion devices, the company enables more than 12,000 customers with Self-Healing Endpoint® security, always-connected visibility into their devices, data, users and applications – whether endpoints are on or off the corporate network – and the ultimate level of control and confidence required to support the modern enterprise. For the latest information, visit www.absolute.com and follow us on LinkedIn or Twitter.

EMAIL:
sales@absolute.com

SALES:
absolute.com/request-a-demo

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

WEBSITE:
absolute.com