Kensington

WHITE PAPER:

Identifying the Gaps in Your Data Protection Plan

June 2020

In This Paper

This document identifies concerns around data protection and security, specifically leveraging new data obtained on device security policies, physical security, authentication methods, visual security, and compromised printed data. It also provides best practices for overcoming common challenges associated with these concerns. This information is primarily intended to support the data protection and compliance efforts of Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), IT Security Managers, engineers and administrators, IT Compliance and Security Operation Centers (SOCs), and others responsible for planning, implementing, and maintaining the security of devices used to access company networks.

Disclaimer: Nothing contained herein should be construed as legal advice. Organizations should consult legal counsel with regard to compliance with applicable laws or regulations.

Contents

About the Key Reference Survey

Key statistical information for this document was derived from the Kensington Global Data Protection Study (February 2020). This study was independently conducted by Applied Marketing Research, Inc. and administered to 400 global IT leaders in their native language. The study consisted of 50 respondents across eight geographic regions. The primary objectives included identifying and addressing the most current data available on the primary concerns around data protection and security; the types of devices and percentage of devices protected or secured from theft/loss; the proportion of firms that have data protection and security policies in place, and the issues related to compliance with those policies; and the types of data security devices used by firms.

Situation Overview

Growing Impact of Cybercrime

According to the latest report by the Center for Strategic and International Studies and McAfee, **cybercrime now costs the world almost $600 billion**, or 0.8 percent of global GDP.[1] To put that statistic in perspective, when you look at the cost of cybercrime in relation to the global internet economy, **cybercrime can be viewed as a 14% tax on growth**.[2] Cybercriminals are adopting new technologies at an unprecedented pace and growing their financial sophistication to capitalize on their conquests — pushing IT security and compliance teams to strengthen their data protection plans.

360° Data Protection

To fully protect corporate data moving in and out of the network cloud, IT teams are tasked with implementing 360° data protection plans. These plans address three components of data protection:

AVAILABILITY

Addressing replication, backup, and redundant systems

INTEGRITY

Managing arrays and disk subsystems to ensure that any data written to the disk (mechanical or flash based) is the same when it is read as it was when written

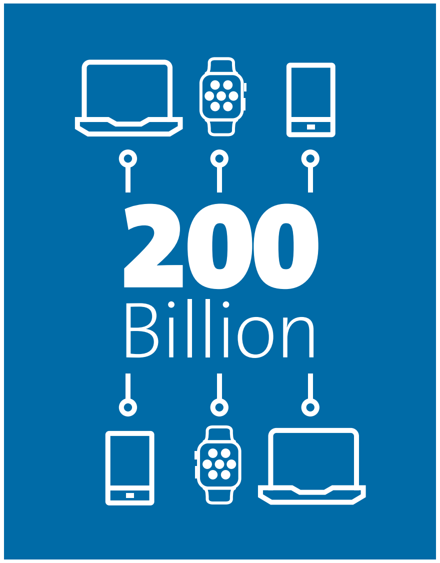
SECURITY

Managing access and making sure that only authorized users, or applications, have access to the data; data is encrypted at rest and in flight

For data availability, the ultimate goal is to have all data replicated to a disaster recovery site, whether in its native format via array or software based replication, or in its backup state via an offsite tape copy or de-duplicated backup replica. Data integrity is now common via enterprise arrays and via midrange and object-based storage systems and software. For data security, the goal is to prevent data loss. Since data can be compromised in flight and at rest, it is important to encrypt data and prevent tapes, drives, laptops, tablets, and other data storage devices from being lost or stolen. Data encryption alone will not help if a server or application that has access to the data is compromised. If a device is stolen, and the encrypted data is readable, a hacker has access to everything. This highlights the importance of endpoint security. As the direct descendent of the first forms of computer protection in the earliest days of IT, endpoint security has continued to evolve to meet the demands of a multi-device world.

Organizations Need to be Laying Strong Foundations for Endpoint Security

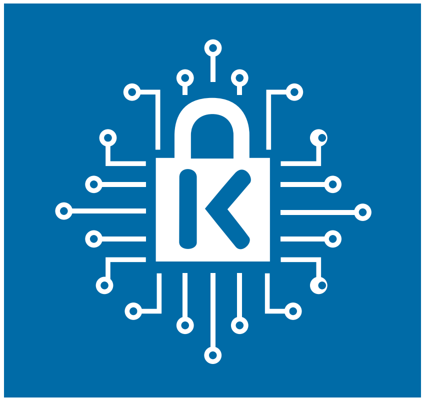
Data security is becoming the most complicated aspect of 360° data protection because of the exponential number of laptops, tablets, and mobile phones connecting to the corporate network. The risk is quantifiable with the Internet of Things (IoT) and it is growing. According to the Symantec Internet Security Threat Report, there are 25 connected devices per 100 inhabitants in the U.S. alone, and **by the end of 2020, there will be roughly 200 billion connected devices**.[3]



These new devices have created new attack paths and security threats for organizations that are further complicated by the increasing number of bring-your-own-device (BYOD) programs, as well as the increase in desk sharing and remote workforces. While convenient and arguably cost-effective, employees using their own devices make it more difficult for IT to control and protect the environments in which their company's sensitive information resides.

Desk sharing, hoteling, and remote workforces generate additional security challenges that further complicate data protection strategies. Employees working from home or connecting to Wi-Fi networks to work on-the-go means that the enterprise network security perimeter is more porous than ever.

Seizing the opportunities created by the growing number of remote connections to the network, today's cybercriminals are leveraging new and harder-to-detect methods of committing a breach. Yet according to survey research conducted by CISO MAG, **nearly 15% of enterprises do not use any form of endpoint security**. However, at the same time, almost half of enterprise respondents agreed that endpoint security offered improved visibility, and over a fifth of them agreed that data breaches continue to increase in volume and complexity.[4] In addition, **80% of security breaches involve privileged credentials which provides additional exposure concerns**.[5] Organizations need to treat data security like a science — starting with laying a strong fundamental foundation for endpoint security.



Endpoint Security Supports Data Protection Compliance and Certification Requirements

Data protection legislation is growing across the globe to protect personal data from the efforts of cybercriminals. The initial wave of legislation includes the European Union's General Data Protection Regulation (GDPR), Brazil's Lei Geral de Protecao de Dados (LGPD), India's Personal Data Protection Bill (DPB) and the California Consumer Privacy Act (CCPA). In addition, the United States currently has similar bills or bill drafts in at least 25 states and in Puerto Rico. Furthermore, important industry certification programs contain data security compliance mandates to protect personal and corporate data. HIPPA, SOX, PCI-DSS, ISO:27001, and SOC 2 are just a few of the certification programs that can audit an organization's data protection policies for compliance.

The increased penalties for non-compliance with regulations are also encouraging organizations to explore stronger foundations for endpoint security. Hacks and data thefts enabled by weak security, cover-ups, or **avoidable mistakes have cost companies more than $1.45 billion over the last eight years**.[6]

Key Components of Endpoint Security

Endpoint security is an approach to the protection of computer networks that are remotely bridged to client devices. The connection of laptops, tablets, mobile phones, and other wireless devices to corporate networks creates attack paths for security threats. Many endpoint security solutions are under-utilized, straightforward and cost-effective. This section discusses the key components of endpoint security, IT controlled and end-user controlled, and additional motivations for implementing reasonable endpoint security measures.

IT Controlled

The IT controlled components of endpoint security are managed by software. Endpoint security software uses encryption and application control to secure devices accessing the enterprise network. Many organizations still have not implemented endpoint security software. According to the Kensington Global Data Protection Study, only 55% of organizations report using security tokens to secure access to their enterprise network.[7] This represents a possible security gap opportunity for organizations who need to implement or update their endpoint security software. In addition, anti-virus software is considered another front line of defense to protect the network. Gaps may exist with anti-virus software because of the many individual devices that connect to the network that are often overlooked, such as mobile phones, tablets, and external drives.

End-User Controlled

A complex component of endpoint security includes end-user controlled laptops, tablets, and mobile phones. These can be a mix of organization-issued devices and devices granted permission to the network via an approved BYOD program. End-user controlled devices often expose gaps in data protection compliance and lead to preventable network risks. The following highlights a few of the key security risks associated with end-user controlled devices.

SECURITY RISKS ASSOCIATED WITH END-USER CONTROLLED DEVICES

Device Theft Device theft remains a key security threat for laptops, tablets, and mobile phones that can access the network	• **One in ten laptops are stolen in their lifetime, and 98% of those laptops are never recovered[8]** • Technology research firm Gartner has found that a laptop is stolen every 53 seconds • 86 percent of IT practitioners report that someone in their organization has had a laptop lost or stolen, with 56 percent of them reporting that this resulted in a data breach[9]
Malware and Hacking End-users often leave their devices unattended while traveling, hoteling, attending meetings, and desk sharing	• 61% of organizations report that one of their primary concerns around data protection and security is users leaving sensitive information on their hard drives[7]
Visual Hacking End-users are often unaware of this effective hacker method of capturing sensitive and confidential information Visual hacking is more prevalent in office spaces with open-floor plans and desk sharing environments While traveling, visual hacking occurs on planes and trains and in event conference rooms, hotel lobbies, and business centers	• 52% of sensitive information is captured by observing unprotected employee computer screens while in the office[10] • **51% of organizations report that one of their primary concerns around data protection is with users who don't cover their laptop, tablet or phone screens when "out and about"[7]**

Security gaps in end-user controlled devices leave networks exposed to controllable vulnerabilities. A 2018 survey around physical locking technology asked IT decision-makers to share examples of data loss resulting from unsecured end-user devices[11]:

> **"Social Security numbers for all employees on stolen laptop for no good reason. No encryption. Made local news ... IT management has still not corrected the issue."**

> **"Somebody walked into the office looking very presentable, said they were going to a meeting and they knew their way, so he was let in. The person just walked around looking for unattended laptops and grabbed a few."**

> **"An employee left their computer bag in the back seat of her car and she went shopping after work. A thief broke into her car and took the entire laptop bag and contents."**

> **"We had one of our sales representatives lose her laptop while travelling to a potential client. On her laptop was proprietary information that was vital to our company."**

Organizations Need to Implement Reasonable Endpoint Security Measures

IT professionals are now incentivized more than ever to implement endpoint security measures. Privacy regulations such as the GDPR and CCPA require companies to provide "reasonable security" to protect customers' personal information against loss or exposure. To avoid regulatory fines, companies must demonstrate that policies are in place to minimize the chances of data loss. **For companies that fail to comply with certain GDPR requirements, fines may be up to 2% or 4% of total global annual revenue or €10m or €20m, whichever is greater**.[12] According to CSO Online, "Sizable fines assessed for data breaches in 2019 suggest that regulators are getting more serious about organizations that don't properly protect consumer data. In the UK, British Airways was hit with a record $230 million penalty, followed shortly by a $124 million fine for Marriott, while in the US Equifax agreed to pay a minimum of $575 million for its 2017 breach."[13]

In addition to steep regulatory fines, the need to avoid reputation damage cannot be overlooked. Many organizations have come to realize that data exposure is brand exposure and that consumer confidence in a company is tantamount to brand confidence. Regardless of industry, the blowback of data exposure has steep and often costly consequences for brands.

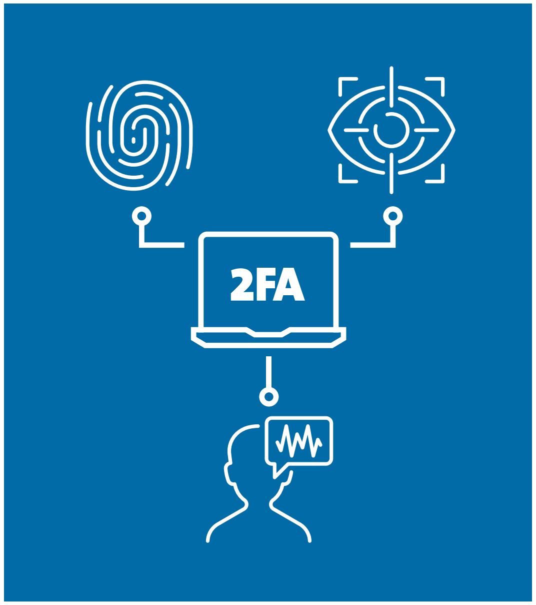
Common Challenges for Endpoint Security and How to Resolve Them

Endpoint security is complicated by a number of factors, including the expanding list of devices connecting to the network, an increase in BYOD programs, desk sharing and mobile/remote workforces, employee non-compliance with data protection policies, and inadequate IT resources to manage remote deployments. Add the complexities of remote connections to the network, with many unwittingly using unsecured Wi-Fi networks, and these challenges can overwhelm even the most sophisticated IT teams. Different layers of protection should be adopted to address each of these challenges.

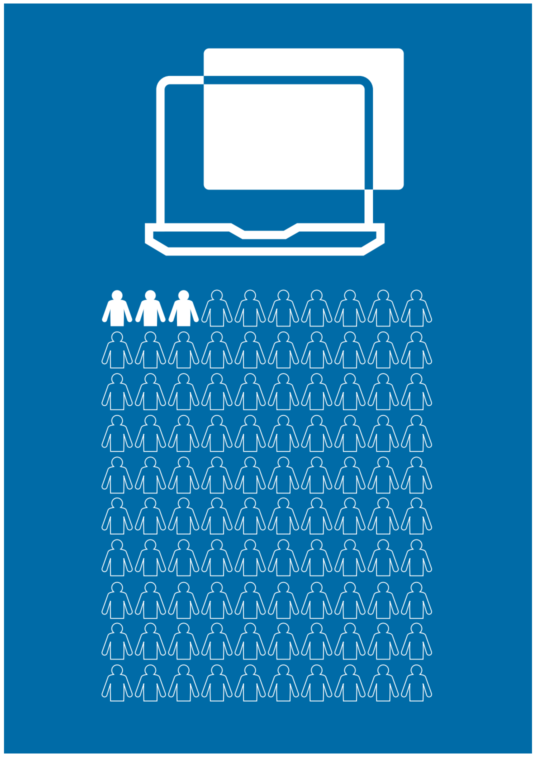
Expanding List of Devices Connecting to the Network

Addressing the security challenges associated with the expanding list of devices connecting to the network can seem daunting when attempting to address the security threat of every laptop, tablet, external hard drive, and mobile phone. According to the Kensington Global Data Protection Study, **52% of organizations report budget constraints as the biggest challenge related to implementing and deploying a physical device security policy for portable devices**. The key to addressing these endpoints is breaking the need down by device and then providing layers of cost-effective protection.

For laptops, tablets, and mobile phones, network security should include biometric, VPN, data encryption, and remote wipe capabilities. A 2019 survey projected that **90% of businesses will utilize some form of 2-factor authentication (2FA) that includes biometrics by the end of this year**.[14] Biometric authentication is on the rise for these devices for good reason. According to the Kensington Global Data Protection Study, 28% of companies said they use fingerprint authentication for enhanced, safer security; 24% said they used it for improved accountability and accuracy; and 17% said they used it because the technology was faster, more convenient, and easier to use. Additionally, visual and physical security should be considered for laptops and tablets. Cost-effective solutions include privacy screens for visual security; and laptop, tablet, and port locks for physical security.



External hard drives should also be secured. Data encryption should be used to address network security. Physical locks or locking kits for external hard drives without security slots can be used to prevent the theft of these devices since they are small enough to be easily stolen and can expose highly sensitive information.



Increase in BYOD, Desk Sharing, and Mobile/Remote Workforces

The Kensington Global Data Protection Study found that 56% of organizations currently allow employees to bring their own computer (BYOC) and 57% require desk sharing. 88% of organizations report that **less than 3% of employees use privacy screens while on the road or out of the office**[7] The key to addressing the security challenges associated with the increase in BYOD, desk sharing, and mobile/remote workforces is helping end-users understand, through training and/or certification programs, that data protection requirements are the same in and out of the office. Devices must be protected from theft, malware, and visual hacking whether they are on a desk within the office or on an airplane tray table.

Employee Non-Compliance with Data Protection Policies

You are not alone if employee non-compliance with data protection policies is a core endpoint security challenge. **Only 9% of organizations report full compliance with company security policies, and only 35% report 77–99% compliance**. Only 17% report that employees use physical locks more than 3% of the time when away from the office.[7]

Understanding what causes non-compliance can be the key to eliminating the challenge. 30% of organizations report that users are non-compliant with portable device security policies due to inconvenience, 21% attributed non-compliance to a lack of corporate oversight, and 20% to apathy.[7] It is critical to help employees understand the importance of compliance as it relates to current applicable regulations, certification requirements, fines, and what a breach could mean to the organization's brand image.

Remote Connections

Allowing employees to work from home comes with additional cybersecurity risks. Employees may lack the necessary knowledge to set up secure Internet connections. Many home Wi-Fi routers are still using old WEP encryption and the original factory password — both of which are easy to crack. Additionally, the MAC address filtering that can be enabled on a home router is vulnerable to hackers using a wireless packet sniffer. For security and speed, using a wired Ethernet connection is a smart idea for home connections accessing the network.

Employees working from other remote locations, including airports, trains, or cafés need to be mindful of the hidden dangers of public Wi-Fi and what they should do to avoid the risks. Cybercriminals use unsecured public Wi-Fi channels to gain access to important emails, encrypted messages, and unsecured logins. This information can make it possible for potential data thieves to hack into an organization'sn network. Several steps can be taken to ensure the network is protected. IT should ensure that company websites and applications are using HTTPS protocols and that employee devices are covered by antimalware software that includes anti-sniffing protection. Remote workers should be required to log in to the VPN and have a firewall enabled on devices at all times. Using a mobile hotspot provided through the organization's mobile carrier, or tethering laptops to a mobile device is a good way to avoid using public Wi-Fi.

It is important to set up policies regarding remote connections and periodically educate employees so they understand the risks and the importance of taking protective actions.

COMMON CHALLENGES FOR ENDPOINT SECURITY AND COST-EFFECTIVE SOLUTIONS

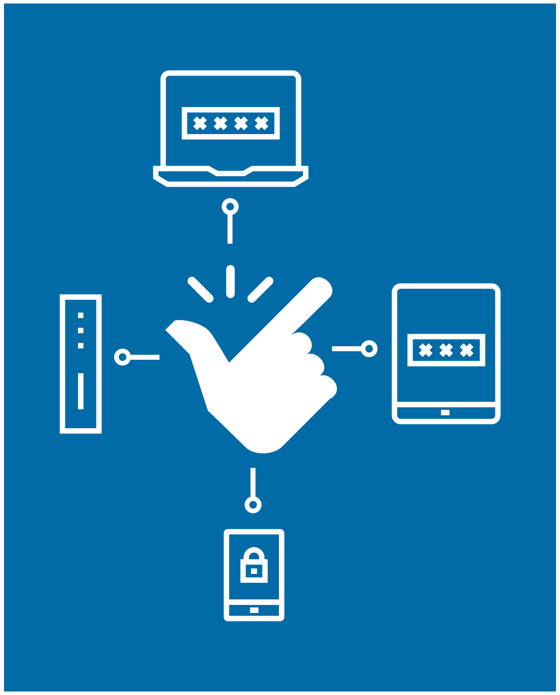
CHALLENGE	SOLUTION(S)
Expanding List of Devices Connecting to the Network	**Laptops, tablets, and mobile phones** Utilize biometrics, VPN, data encryption, remote wipe capabilities, privacy screens, device locks, and port locks **External hard drives** Utilize data encryption and physical locks (use locking kits for external drives without security slots)
Increase in BYOD, Desk Sharing, and Mobile/Remote Workforces	**Employee Training** Employees must understand that data protection requirements are the same whether in or out of the office
Employee Non-Compliance with Data Protection Policies	**Employee Training** Help employees understand the importance of compliance as it relates to current applicable regulations, certification requirements, and what a breach could mean to the organization's brand image
Remote Connections (Home and Public)	**Home Connections** Employees who work from home should either use a wired Ethernet connection or work with IT to ensure Wi-Fi modems are set up properly to meet security standards **Public Connections** Company websites and applications should use HTTPS protocols All employee devices should be covered by anti-malware software that includes anti-sniffing protection Remote workers should be required to log in to the VPN and have a firewall enabled on devices at all times Use a mobile hotspot provided through the organization's mobile carrier, or tether laptops to the mobile device to avoid using public Wi-Fi **Employee Training** It is important to set up policies regarding remote connections and periodically educate employees so they understand the risks and the importance of taking protective actions

Best Practices for Solving Common Challenges with Endpoint Security

The most important advice is to get started. All efforts to enhance endpoint security can be immediately documented to support claims that the organization is making efforts to protect data. Should a breach occur while the organization is making improvements, some leniency may be granted if efforts are underway for continuous process improvement. A few best practices for solving the most common challenges associated with implementing endpoint security include:

Deploy Physical Device Security for All Portable Devices

Simply put, it is much more difficult to hack a network without an entry point. Physical device security is cost-effective, simple to deploy, and serves as a first line of defense for all portable devices. Locking stations, laptop locks, tablet locks, and locking kits continue to evolve to meet the demands of a multi-device world. Streamlined solutions can include custom keyed locks, combination locks, desktop locks, portable locks, and lock and anchor points. Employees must be provided with a means to secure their devices in and out of the office, and this may require different protection to meet varying needs. Employees should certify that they are responsible for securing their devices and have been trained how to do so in different environments. To simplify implementation, work with an experienced hardware security partner to help you identify your needs and the most cost-effective way to secure and manage all of your organization's portable devices.

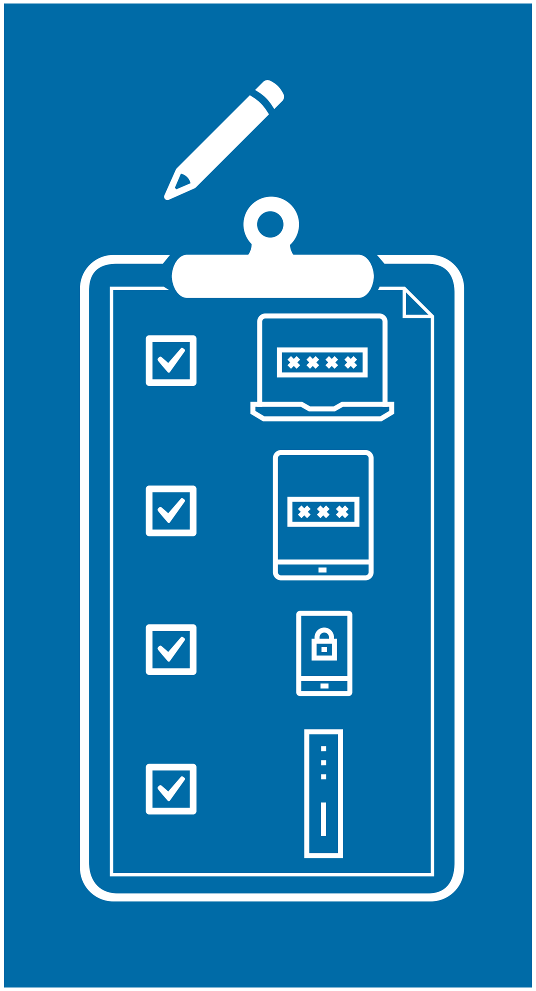


Utilize Simple Solutions for End-Users

30% of organizations report that users are non-compliant with portable device security policies due to inconvenience.[7] To support compliance, **it is important to focus on end-user convenience**. For office employees, physical device security could be as simple as a centralized desktop locking solution for all peripherals. For mobile employees, it could be physical security that is lightweight, compact, and easy to implement. It is important to remember that different employee sectors use their devices differently, and thus have different endpoint security needs. Privacy screens are simple, and prevent visual hacking. They should be required for managers, human resources, executive teams, and any employee with sensitive information on their computer both while in the office and while traveling or working remotely. When evaluating endpoint security options, remember to let simplicity drive some of the decision, since compliance with the solution is the only true path to data protection.

Implement 2nd-Factor or Multi-Factor Authentication

Improving authentication methods to prevent unauthorized access to lost or stolen devices is an important step in data protection. Universal 2nd-factor authentication enhances data protection policies, is simple for end-users, and forces cyber compliance. It is important to note that not all 2nd-factor authentication options are created equal. For example, text-based authentication is not as secure as biometric authentication. Fingerprint-based security is simple, fast, easy to deploy in Windows environments, and works well for in-office and mobile workforces. **Best-in-class 2nd-factor authentication options include advanced biometric technology, FIDO U2F or FIDO2 CTAP1 certification, and broad integration and compatibility**. An experienced 2nd-factor authentication partner can help with training and education needs, for a seamless deployment.



Train, Track, Certify and Enforce Compliance

Data protection plans are only as strong as their weakest link. Employees must be trained on how to utilize the organization's endpoint security solutions in and out of the office, why endpoint security matters to the organization, and what steps should be taken to minimize the chances of data loss when a device is lost, stolen or retired. To ensure ongoing compliance, **training should be tracked and offered with each deployed device**, and employee self-certification of understanding should accompany the deployment of every device. Additionally, data protection training intervals of no less than every 18 months will help enforce compliance, as well as force an internal review of compliance with the latest regulations.

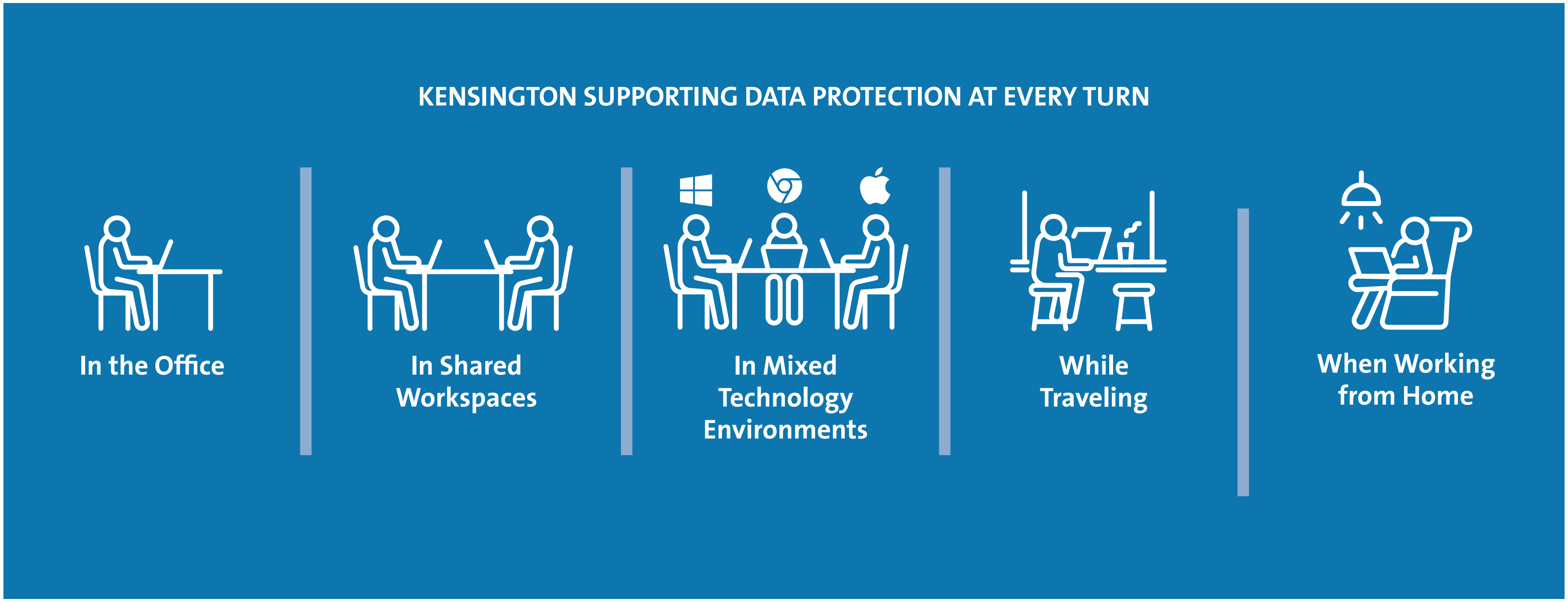
Seek Additional Cost-Effective Ways to Protect Data

There are many ways to improve data protection plans. Some require us to step outside the realm of popular thought. Consider this fact — **56% of organizations report that one of their primary endpoint security concerns is users printing out sensitive data and leaving it in unsecured areas**.[7] While laptops are the biggest source of exposure, data breaches can also occur from the careless disposal of printed paper containing confidential information. It is worth noting that **privacy regulations relate to paper-based data as well as electronic data**, so it is important that organizations handle personal data carefully to avoid fines and legal action due to non-compliance. Paper shredders provide a cost-effective solution for protecting printed data and should be part of every data protection plan. Shredders offer varying levels of protection and shredder security levels are referenced by a protection rating (P-rating). The P-rating refers to the number of pieces a document is shredded into. The higher the P-rating, the more pieces a document is shredded into and the higher the level of security it provides.

Conclusion and Kensington’s Recommendation

Endpoint security solutions help protect confidential business and personal data, protect customer and client data, comply with privacy legislation; and help organizations evade the reputation damage, negative publicity, and costly expenses that can result from a data breach. Many endpoint security solutions are cost-effective and simple to deploy. From physical device locks, to privacy screens, to fingerprint-based authentication keys, to paper shredders, **the simplest forms of protection can be the most effective**.

As the standard in device security for more than 35 years, Kensington has expanded our expertise to include the data protection demands of a multi-device world. To us, security is about more than saving a physical device from theft — it is also about saving data from falling into the wrong hands, which could be far more costly than simply replacing the device. That is why our security solutions are tough, innovative, and easy to use.



KENSINGTON SUPPORTING DATA PROTECTION AT EVERY TURN

In the Office

In Shared Workspaces

In Mixed Technology Environments

While Traveling

When Working from Home

If you need support implementing endpoint security solutions or are struggling with users not adopting policy or best practices, visit **kensington.com/security-solutions** to see how we can help.

Sources

1. The Economic Impact of Cybercrime — No Slowing Down, McAfee, February 2018
2. The Connected World: The Internet Economy in the G20, The Boston Consulting Group, 2012
3. Symantec Internet Security Threat Report, Symantec, January 2020
4. 1 in 3 CISOs Feel Biggest Challenge of Endpoint Solution is its Complexity, CISO MAG, November 2019
5. A Guide to Endpoint Privilege Management, Beyond Trust, January 2020
6. The Biggest Data Breach Fines and Penalties, CSO Online, January 2020
7. Applied Marketing Research, Inc.,Kensington Global Data Protection Study, February 2020
8. Laptop and Mobile Device Theft Awareness, University of Pittsburgh, accessed via https://www.technology.pitt.edu/security/laptop-theft, March 2020
9. 7 Shocking Statistics that Prove Just How Important Laptop Security Is, Security Boulevard, September 2018
10. Global Visual Hacking Experiment Whitepaper, 3M, 2016
11. SpiceWorks, Kensington Locking Survey, February 2018
12. What are the GDPR Fines?, GDPR.EU, accessed via https://gdpr.eu/fines, March 2020
13. The Biggest Data Breach Fines, Penalties and Settlements So Far, CSO Online, January 2020
14. Spiceworks Study Reveals Nearly 90 Percent of Businesses Will Use Biometric Authentication Technology, accessed via https://www.spiceworks.com/press/releases/spiceworks-study-reveals-nearly-90-percent-businesses-will-use-biometric-authentication-technology-2020, March 2020

Kensington
The Professionals' Choice™

FOR MORE INFORMATION CONTACT: 1-855-692-0054 | sales@kensington.com