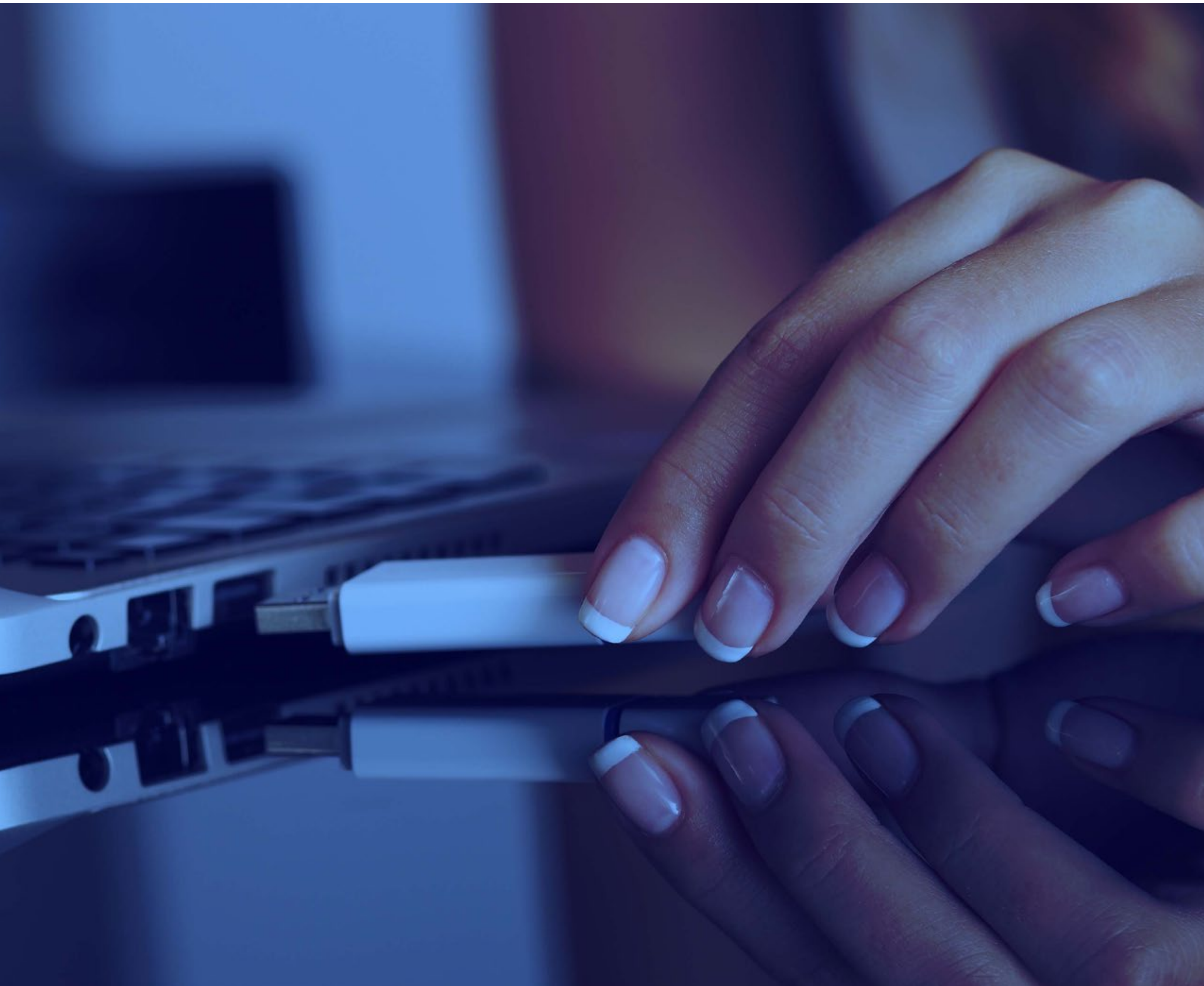
WINZIP™

Protecting Sensitive Data in Today's Hybrid, Distributed Workplaces

A guide to the new data security and privacy challenges that healthcare, financial, and government sectors face—and how organizations can overcome them.

White Paper | WinZip Enterprise



Introduction: Today's Evolving Workplace

Dramatic workplace changes have impacted nearly every vertical as a result of the COVID-19 pandemic. The emerging models for hybrid, distributed workforces are changing the way organizations operate. Employers are recognizing that employees don't have to be at the office to produce results—and as a result, they're empowering them to work and collaborate from anywhere.

For the healthcare, government, and financial sectors, this new dynamic brings tremendous opportunity to improve business continuity, boost resilience, fuel business growth, and optimize operations.

Employers are recognizing that employees don't have to be at the office to produce results—and as a result, they're empowering them to work and collaborate from anywhere.

But this shift in the workplace raises a new critical question: How can organizations ensure their sensitive data remains secure across remote, distributed teams?

Globally, 80% of surveyed organizations said they accelerated at least some of their digital transformation programs in 2020. The top two most accelerated programs were to strengthen cybersecurity defenses and to implement wider capabilities for remote work. The top two barriers to these initiatives? Data privacy and security concerns.

Remote work risks are top of mind. Asked about their concerns related to cyber exposure in 2021, the two that risk management experts across the globe ranked at the top were data breaches and IT vulnerabilities stemming from increased remote work.

There are several key reasons why organizations see cybersecurity in remote environments as a challenge:

- **The growth of sensitive digital data**, along with the increased number of data touchpoints, exponentially increases the attack surface—and with it, the exposure to cyber threats.
- **Employees are now accessing files and data on multiple devices**—often via unsecured connections. This means that simply protecting your company's network and corporate endpoints is often no longer effective.
- **The proliferation of cloud applications and services** adds new risks due to lack of visibility and consistent control across a multi-cloud infrastructure.
- **The new complexity of increasingly digital work environments**, which must be maintained by IT teams, is adding pressure on resources that are already stretched thin. Placing additional security burdens on them is not sustainable long-term.

This white paper examines how evolving, increasingly distributed workforces increases the need for data privacy and security for healthcare, government and financial organizations—and how leaders in these verticals can address these challenges by using technology to secure sensitive data.

Data Security and Privacy Challenges in Remote Environments

The remote work trend has been growing for some time. But in recent years, the accelerated adoption of digital technologies, the digitalization of business processes, and the growth of cloud computing have made remote workplaces feasible at scale. And in response to the global pandemic, 2020 saw an explosion in the number of people working from home.

Many organizations made a hasty shift to remote work because they had no other choice due to strict lockdowns that forced them to send workers home on short notice.

This created vulnerabilities that many organizations didn't address strategically, either because they didn't have the time or were unaware of the full extent of the risks caused by the shift to remote work.

It's thus not surprising that 47% of organizations report that the inability to control risks in the homes of remote workers is a significant concern. This presented cybercriminals with a ripe opportunity. As remote work shifted into high gear, attackers targeted the IT resources and systems that enabled employees and contractors to work from home, including:

- **Email servers:** With more sensitive and confidential information shared electronically in a distributed environment, email servers became a prime target.
- **Virtual private networks (VPNs)**: The surge in VPN use made them attractive to cyber actors, who exploited several publicly known VPN vulnerabilities to gain access to corporate networks.
- **Remote Desktop Protocol (RDP):** The rapid shift to remote work increased reliance on this proprietary protocol for remote access to Windows servers and workstations, and security researchers observed a substantial increase in attempted RDP attacks.
- **Collaboration and communication tools:** As organizations quickly turned their focus to cloud-based collaboration and communication tools such as Microsoft 365, Slack and Zoom, so did malicious actors, exploiting those apps for phishing and malware attacks.

The Impact of Remote Work on Data Breaches

A UK survey of IT decision makers found that 35% of remote workers have knowingly put corporate data at risk of a breach.

A separate study found that the average cost of data breaches for organizations with remote workers was $8.64 million in 2020, compared to an average of $8.19 million for those organizations without remote workers, and to $7.3 million overall in 2019.

Researchers in this study attributed the higher remote work costs to "the difficulty in detecting and responding to attacks aimed at devices used outside corporate networks."

Top Trends Impacting the Hybrid Workplace

Now that both employers and employees have experienced the benefits of remote work, hybrid workplace models are emerging as the "workplace of the future" for knowledge workers. This shift comes at a time when several other trends are converging to have a profound impact on data privacy and security:

- **The rising information tide:** Organizations create, collect, process, and store massive (and growing) quantities of data. A 2020 survey found that organizations were managing 40% more data than a year before. The spread of this data across your on-premises, cloud, and/or multi-cloud ecosystem can weaken your company's security controls.
- **Increased information sensitivity:** From January to October 2020 alone, 730 publicly disclosed data breaches exposed a total of 22 billion records in the US. Valuable intellectual property (IP), personally identifiable information (PII), electronic protected health information (ePHI), financial accounts, and other types of data have become an increasingly inherent part of digital file content. This data is highly valuable not only to your organization, but also to cybercriminals.
- **Expanding regulations:** Noncompliance has costly consequences, especially in the highly regulated government, healthcare, financial, and insurance sectors. But meeting regulatory requirements in a multi-cloud environment, for example, is a tough challenge, especially since the public cloud's shared responsibility model complicates security.
- **Talent shortage:** The estimated 3.1 million gap in global cybersecurity talent has resulted in 64% of organizations experiencing personnel shortages. The growing complexity of digital work environments and the proliferation of security tools put further burdens on IT and security teams that are already stretched thin.

Spotlight: Insider Threat

People are your weakest link: 85% of breaches involve a human element. Yet protecting against insider threats in a hybrid environment is a difficult task. Organizations saw a 60% increase in malicious insider attacks since the onset of COVID-19.

Fortunately, you can use technology to prevent many insider-related incidents. For example, 88% of all data breachers are caused by employee mistakes. Take advantage of security tools and controls to mitigate human-driven risks, such as sharing or storing sensitive files without securing them.

Data Protection in Healthcare, Government, and Finance

Healthcare, government, and financial sectors commonly rank at the top industries targeted by cyberattacks. Hybrid workforces make organizations in these sectors more vulnerable to attacks by further complicating their IT operations and compounding the data security risks.

Before we discuss what steps you can take to protect your data, let's look at the specific threats and risks that these sectors face.

Healthcare

Protected health information (PHI) is more valuable on the dark web than many other types of data, which attracts cybercriminals to healthcare providers and insurance carriers. It comes as no surprise then that healthcare has had the highest cost of data breaches for 11 consecutive years. In 2020, the average for healthcare was $9.23 million, compared to $4.24 million across all sectors.

One aspect that drives up cost is noncompliance with regulations such as the US Healthcare Information Portability and Accountability Act (HIPAA). In 2020, the US Department of Health and Human Services Office of Civil Rights levied a total of more than $13.5 million in fines for violations—more than in any previous year of enforcement.

Two of the biggest sources of breaches in healthcare include the following.

- **Ransomware:** This was by far the biggest threat to the healthcare industry in 2020 (identified in 46% of breaches), prompting INTERPOL to issue a warning to hospitals and other providers.

  Especially troubling is the rise of so-called double-extortion schemes, where attackers not only encrypt files but also threaten to leak stolen data—and sometimes even following through on this.

- **Hacking:** Whereas lost and stolen devices were the main culprit behind healthcare data breaches in the past, hacking and IT incidents by outside actors are now responsible for most of those incidents. The top two locations of breached ePHI are network servers and email.

The Cost of Healthcare Data Breaches

- In 2020, healthcare reported the highest number of data breaches (accounting for 484 out of 3,257 total breaches, followed by 429 in the information sector and 382 in finance and insurance).
- The average cost of a data breach in healthcare rose from $7.13 million in 2020 to $9.23 million 2021—more than double the 2021 average of $4.24 million across all sectors globally.

Government

The massive supply chain attack on networking company SolarWinds compromised a broad range of US government agencies, illustrating the vulnerability of the public sector in general.

As a result, in May 2021, President Joseph R. Biden issued an executive order aimed at strengthening national cybersecurity. The order has broad implications for modernizing the government's cybersecurity and implementing a variety of controls. The US is only one example—governments around the world face serious security threats.

Two of the biggest sources of breaches in the government sector include:

- **Ransomware and data theft.** These were the most common types of attacks on government agencies in 2020. Nation-state actors often go after IP and other confidential documents, both for monetization and espionage purposes.
- **Threat actors.** Malicious individuals or entities such as nation-states that try to carry out cyberattacks, known as threat actors, are adapting their tactics to remote environments. For example, Emotet, an advanced banking Trojan that has evolved to steal sensitive data, made a strong comeback in 2020 globally. According to the US Cybersecurity Infrastructure and Security Agency (CISA), this threat is "among the most costly and destructive malware affecting state, local, tribal, and territorial governments," with each incident costing an average of $1 million to remediate. One of Emotet's latest tricks is to infect unsecure Wi-Fi networks, along with the devices connected to them, which is a big concern for companies with remote employees.

Government is Among the Most-Targeted Sectors

- Government agencies experienced **more than twice the number of malware attacks** compared to other sectors in 2020. In March 2020 alone, each government agency globally saw an average of 12,725 malware attacks, **or about one every 17 hours.**
- In the first 10 months of 2020, the US government had the third-most number of publicly reported breaches, accounting for 12.5% (for comparison, healthcare accounted for 24.5% and the technology sector, for 15.5%).

Real-World Example: US Department of Veterans Affairs

Malicious hackers used social engineering and exploited authentication protocols to gain unauthorized access to the US Department of Veterans Affairs' (VA) Financial Services Center's online application in 2020.

The data breach compromised PII such as Social Security numbers, affecting 46,000 military veterans. The VA said the hackers' objective was to change information on the application to divert payments that the VA makes to private physicians. The agency did not disclose whether those attempts succeeded.

Finance

Although threat actors often target the financial sector to steal money, data theft is just as big a problem: 83% of data compromised in confirmed breaches of financial and insurance firms is personal data.

Yet more than a quarter of the surveyed financial institutions say they didn't accelerate their adoption of cloud security measures despite pivoting to remote work. These organizations also noted that the shift to distributed environments created challenges related to endpoint security, including patching of employees' personal devices.

Two of the biggest sources of breaches in the financial sector include:

- **The move to cloud-based email services.** This escalated the risk of business email compromise (BEC) attacks, which saw a 67% increase from 2019 to 2020. Among Coalition insurance policyholders, for example, the top BEC-related claims came from financial services.

  And BEC doesn't only create financial risk: Overall, BEC was the initial point of entry for 60% of Coalitions' claims, resulting in data breaches, among other incidents.

- **Bring your own device (BYOD) policies**. Surveyed government executives noted that BYOD and remote worker policies "posed particular challenges for their digital security." Additionally, security staff shortages made it difficult to manage worker risks such as the use of unsecure cloud-storage apps.

Financial Sector Risks and Cost of Data Breaches

- After healthcare, the financial sector has the highest cost of data breaches—an average of $5.72 million.
- On average, each employee in banking, insurance, and investment companies has access to nearly 11 million files and nearly 777,777 folders.
- Nearly two-thirds of those companies have more than 1,000 sensitive files accessible by each employee, putting them at risk of noncompliance with regulations such as General Data Protection Regulation and Sarbanes-Oxley.

Real-World Example: Desjardins Credit Union, Canada

A June 2019 breach of Desjardins Credit Union compromised PII such as customer names, social insurance numbers, and the addresses of close to 9.7 million individuals in Canada and abroad.

The credit union did not become aware of the breach for two years. An investigation found that the breach was due to poor access controls to folders, which enabled an employee to exfiltrate the data over a 26-month period by copying it to a personal USB drive. The breach cost the company at least $53 million.

How Data Is Compromised

Before providing concrete steps that you can take to protect your data, it's first important to understand how unauthorized access can occur.

Effective data protection follows three tenets: confidentiality, integrity, and availability (often referred to as the CIA triad). Some of the ways that this triad can be compromised in a digital, distributed environment include:

- **At the endpoint:** Cybercriminals can gain access to employee devices by deploying malware, hacking, using backdoors, exploiting vulnerabilities, and so on. The risk is higher in BYOD and hybrid work environments because IT has less visibility into and control over what personal devices employees use.
- **DNS tunneling:** This method exfiltrates data by sending it over DNS protocol (often through shared internet hotspots, such as public Wi-Fi). DNS tunneling bypasses firewalls and other network security by setting up a direct communication channel with a computer, infecting it with malware and enabling the attacker to control it.
- **Application-based attacks:** An example of an application-based attack is "consent phishing," where attackers obtain access to sensitive data through permissions. The attack starts with a phishing email with a malicious link to a lookalike login page—for example, to Office 365—but rather than stealing credentials, the threat actor tricks the employee into granting Office 365 access to a malicious app.
- **At the application point:** Some cloud-based applications don't use multi-factor or two-factor authentication (e.g., the Pro or Business versions of Smartsheet). Cybercriminals could gain access to the data stored in the app through brute-force attacks or via stolen credentials.
- **In transit:** Threat actors use malware, "man in the middle" attacks, DNS spoofing, and other methods to "sniff" data or "eavesdrop" as it travels across networks, to and from the cloud, or between devices. Unsecure protocols (e.g., FTP, HTTP, POP3) and unsecure connections (e.g., public Wi-Fi) both create risk.

Real-World Example: University Hospital New Jersey

In September 2020, a phishing scam resulted in a compromised network and a ransomware attack at University Hospital New Jersey. Cybercriminals reportedly stole 240 GB of data, then leaked 1.7 GB—48,000 documents that included information such as names, Social Security numbers, and patient release forms.

In an effort to prevent further data leaks, the hospital contacted the attackers, who initially demanded a $1.7 million ransom. Following negotiations, the ransomware operators eventually settled for 61.9 bitcoin, (which translates to $672,744).

Five Steps For Protecting Your Sensitive Data

While different industries face unique risks, common best practices for protecting data apply across the board, whether you store, access, or share PII, ePHI, intellectual property, or other sensitive data.

Like your network and other types of cyber-security, you need multiple layers of data protection. A layered approach adds extra barriers of entry for malicious actors. In addition to fortifying defenses with technology controls, consider a holistic strategy that strengthens both processes and the knowledge of your employees, so they know what to look out for and what steps to take to help ensure data security.

NOTE: *The steps below are only some of the recommended best practices, rather than an exhaustive list. Use them as a starting point for basic steps as you begin to build out your security layers and overall strategy.*

1. Encrypt sensitive data in transit and at rest

Encryption turns plaintext (readable) data into ciphertext (nonreadable) through complex mathematical algorithms, and only authorized users who have a decryption key can “unscramble” it.

Many organizations today are moving to what some refer to as “military-grade” encryption, which uses a 256-bit key size and is more secure compared to the legacy 128-bit algorithm.

Certain regulations, such as the Federal Information Security Management Act (FISMA) also require adherence to specific cryptographic requirements, such as Federal Information Processing Standards (FIPS).

When a malicious actor hacks an endpoint such as a computer or server (where data is “at rest”) or intercepts it in transit (also called “in flight”), encryption renders the file unusable, protecting the confidentiality and integrity of the data and helping you maintain compliance.

Not all your data needs the same level of encryption—for example, you may have different policies for data that's publicly available than for confidential data. A first step is to classify your data based on sensitivity level, then determine which type should always be encrypted and which encryption can be optional.

When determining your strategy, ensure that you cover not only employee computers and laptops but all types of storage media, including servers, smartphones, and removable or external storage devices.

Additionally, consider deploying encryption at the file point, which secures the data regardless of where it's stored or how it's shared and transmitted. For example, with WinZip® Enterprise, files are placed in virtual containers that are surrounded by a layer of encryption and compression. A file can only be opened if the user has the correct password, or if an IT administrator has an enterprise-wide key to decrypt it.

2. Centralize policy controls and enforcement
In a hybrid, distributed environment, employees and contractors store and access data in numerous locations. This often results in inconsistent data security policy enforcement.

For example, if your organization has adopted multiple public clouds, your IT teams may lack visibility into the cloud data and applications and struggle to manage access controls in a unified manner.

A variety of solutions can enable centralized policy controls and enforcement, including:

- Identity and access management.
- File management utility applications.
- A cloud access security broker, or CASB (for cloud apps).

These solutions work in different ways to provide policy controls to IT administrators. They can enable actions such as disabling specific applications, preventing employees from storing or sharing sensitive files through unsecure apps, or restricting access to apps and other resources.

It's important to note that these solutions are not mutually exclusive; some can be used in combination with the others to provide additional security.

Centralizing control enables your IT or security team to manage access to all your applications in a single pane of glass. This not only improves your security posture but also simplifies management, saving IT admins valuable time.

3. Create multiple forms of data backups
Best practices for data backups follow the so-called 3-2-1 rule, which is all about redundancy. This rule recommends keeping at least three copies of data (one primary and two backups), storing the copies on at least two different media and keeping at least one copy off-site. This applies to all your data, whether you store your original locally, at the data center, or in the cloud.

The 3-2-1 approach helps you restore data in the event of an incident such as a cyberattack. Ransomware often encrypts not only the primary data source but also local backups, which is why cloud backup has an advantage.

Back up your data regularly and often. There's no rule of thumb for how frequent your backups should be—it often depends on the amount of data you handle. Some experts recommend daily backups for critical data (and at least weekly for nonessential files), while others recommend every few minutes if your business has vast amounts of highly sensitive data.

Ideally, companies should look for solutions that automate and simplify the process to make it easy for both admins and end-users to create backups.

4. Require strong authentication
Stolen credentials are available in abundance for sale and lease on the dark web. One group of researchers also found 15 billion credentials from more than 100,000 breaches offered for free.

Knowing that many people reuse usernames and passwords, hackers attempt access to other systems and applications with these stolen credentials. Other techniques at their disposal include brute-force attacks and credential theft through phishing. More than 60% of confirmed data breaches involve credentials in one form or another.

Password management best practices (such as using a password manager) and multi-factor authentication (MFA) add another barrier to unauthorized data access. Leverage built-in MFA tools offered by many applications, such as Office 365, or consider implementing unified authentication and authorization across your environment.

The Implications of the "Executive Order on Improving the Nation's Cybersecurity"

US President Biden's May 2021 Executive Order (EO) establishes broad new requirements for the federal government, including best practices such as encryption, MFA, endpoint detection and response, and zero-trust security.

When fully implemented, this EO will have ripple effects not only on compliance for government agencies but also for the private sector.

The National Institute for Standards and Technology (NIST), which will develop the new standards under the EO, has a lot of weight both in the public and private sectors.

NIST also developed the FIPS standards, HIPAA Security Rule implementation guidelines, and the NIST Cybersecurity Framework, and many businesses across all industries adopted the Cybersecurity Framework as a best practice.

IT leaders in the government, healthcare, and financial sectors should be watchful of this EO's developments and understand how it may impact their organizations in the future.

Additionally, consider supplementing your strong authentication practices with other security measures, such as implementing account lockout policies (locking an account after a set number of failed login attempts) and configuring accounts to be automatically disabled (e.g., after an account is inactive for a set amount of time).

One area that companies may overlook is the authentication recovery mechanism. If you have a weak process, attackers could gain unauthorized access to your systems by simply resetting a password.

For example, using a recovery process that relies entirely on knowledge-based answers poses a risk because an attacker may be able to guess the answer or find personal information that people use for common questions.

5. Educate your hybrid workforce
Creating a strong cybersecurity culture is critical in the hybrid workplace. You need buy-in both from your executive leadership and your workforce. One survey found that 43% percent of businesses changed their cybersecurity approach to focus more on education following the transition to remote work.

Many employers emphasize phishing awareness, and for good reason—57% of organizations experienced a successful phishing attack in 2020, and data loss occurred in 60% of those attacks.

But phishing is only one component. Your security education and training program should consider all potential security risks, which may include anything from weak passwords and risky internet browsing to remote access and BYOD.

Additionally, different roles within your organization may require different types and levels of training. Segment your program to include not only general awareness and training for all workers, but also additional curriculum for roles such as managers, employees with privileged access, and specialized job categories such as those that handle sensitive data.

The National Initiative for Cybersecurity Education (NICE) offers several free and low-cost employee education programs. Many HR software vendors also offer security training modules as part of their onboarding and continuing education offerings.

Online training modules are popular, but it's important to think beyond them—your employees learn in different ways. Use a variety of communication channels, based on your corporate culture and communication tools (online and offline), to disseminate information, updates, and security messaging.

Secure and Protect Your Sensitive Data With WinZip Enterprise

The ability to collaborate and communicate from anywhere is instrumental in a hybrid workplace—and security shouldn't be a barrier. As you evaluate your security stack to harden data protections in a distributed workplace, consider tools not only for protecting your network and devices, but also for ensuring secure collaboration.

WinZip® Enterprise solves many of the data security challenges that government, healthcare, and financial sectors face by:

- **Delivering military-grade file point encryption**, which aims to ensure your files remain secure regardless of where they are stored.
- **Preventing leakage of sensitive files** that employees send through email attachments or unsecure cloud apps by enabling safe information sharing through some of the most popular business collaboration tools available, including Microsoft 365, Google Drive, Box, and Dropbox.
- **Providing centralized IT admin control** of the entire application and its policies, including those for password, backups and more.
- **Offering a lightweight, encrypted endpoint backup capability**, which automatically backs up files from anywhere to anywhere, e.g., the cloud, on-premises, and endpoints.
- **Enabling secure file management**, including automatic file deletion from the recycle bin, download folder, and temporary folders, ensuring that sensitive data is not stored in unsecure folders.
- **Supporting secure collaboration** through additional features, such as integration with Slack, Microsoft Teams, and SharePoint. Employees can also easily create PDFs from multiple file formats and add security features such as watermarks or set expiration dates when sharing links to sensitive files.

WinZip Enterprise is also Federal Information Processing Standards (FIPS) 140-2 validated and FIPS 197 certified and trusted for Defense Federal Acquisition Regulation (DFAR).

Other key benefits of WinZip Enterprise include:

- Scalability for small and large teams.
- Complete customization to meet the needs of your IT team and your end users.
- Improved productivity and optimized use of your IT resources, including data storage.

WinZip Enterprise helps safeguard your organization while improving productivity for your IT admins and your employees—removing the barriers to secure collaboration and fueling business growth.

Conclusion: Embrace Distributed Workplaces Without Compromising Security

There's no reverting to the workplaces of yore. Employees today expect flexibility, which means if your organization wants to effectively compete for talent in this new business climate, you need to embrace a hybrid workplace model.

But this shift comes with new risks. Addressing the unique vulnerabilities and threats of the remote workplace requires a different approach. Your security strategies, tools, processes, and even your employee knowledge must adapt.

Embracing the workplace of the future doesn't mean trading flexibility for cybersecurity. Instead, reevaluate your risk through the new lens of a hybrid workplace and take the necessary steps to fill in the vulnerability gaps.

As your digital footprint and your amount of data continue to grow—and your business evolves—so will your risks. To empower secure collaboration and communication from anywhere, adjust your strategies dynamically to ensure your defenses are keeping up.

Learn how WinZip Enterprise can protect your organization's data.

winzip.com/enterprise