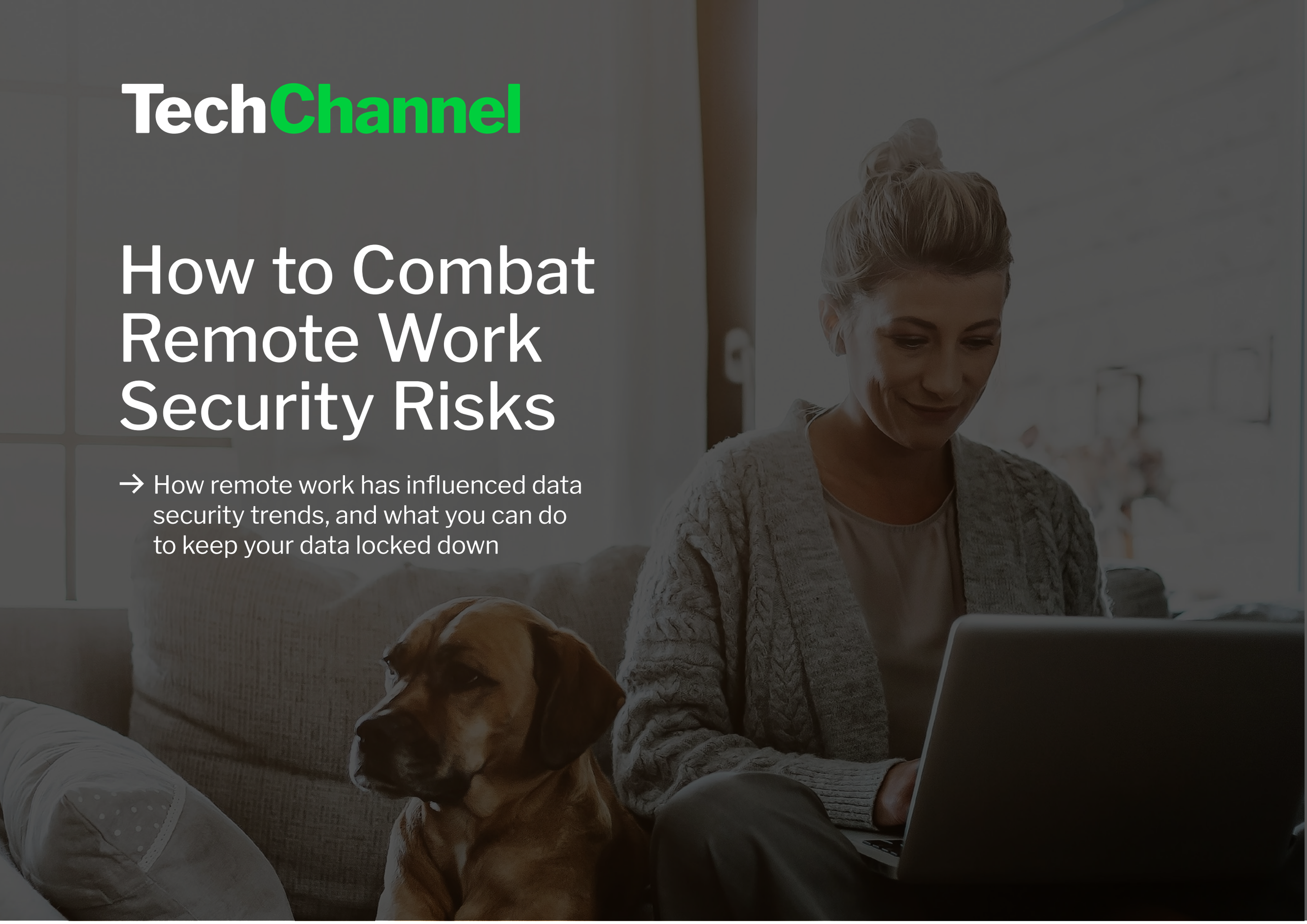
TechChannel

# How to Combat Remote Work Security Risks

→ How remote work has influenced data security trends, and what you can do to keep your data locked down

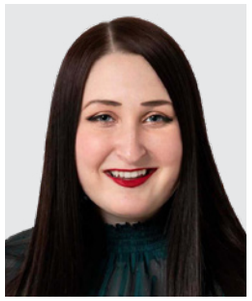


SPONSORED BY MICRO FOCUS®

contents



# How Remote Work Has Impacted Data Security Trends



Throughout this pandemic, many of us learned to effectively implement remote work strategies, fundamentally changing the way companies do business now and into the future. As we start to move closer to “normalcy,” it’s clear that remote work doesn’t seem to be going away.

While remote work offers clear advantages for flexibility and productivity, it does present at least one critical challenge: data security. With the introduction of private networks and personal devices, off-site working models introduce greater potential for stolen data and network compromise.

Luckily, organizations can take clear steps to reduce reduce the risk of remote work compromise—starting with implementing encryption strategies and developing an effective backup and recovery plan. In this e-book from TechChannel, learn how remote work has influenced data security trends and see what you can do to keep your data locked down.

**Keelia Estrada Moeller, Senior Editor**

# Encryption Software: A Key Cybersecurity Solution

Encryption solutions, used in combination with efficient key management, can deliver robust protection for sensitive data

BY SALONI WALIMBE

In the modern era, technology continues to spark worldwide advancements. From breakthroughs in healthcare to sophisticated transportation systems to rapid automation across the industrial landscape, technology has improved life in countless ways. With the rising significance of data in the industrial world, data security is becoming increasingly important, with the encryption software market emerging as a key contributor.

One of the main factors in this transformation is the growing amount of personal data being collated and managed online, in the cloud or on servers. From a business perspective, some form of personally identifiable information (PII), including names, birthdates, Social Security numbers and financial information, among others, is collected by organizations for their operations.

In fact, it's becoming increasingly difficult to carry out business activities without the storage and use of some type of personal data on business network systems. It's projected that the global **encryption software market** size could reach $20 billion in value by 2026.

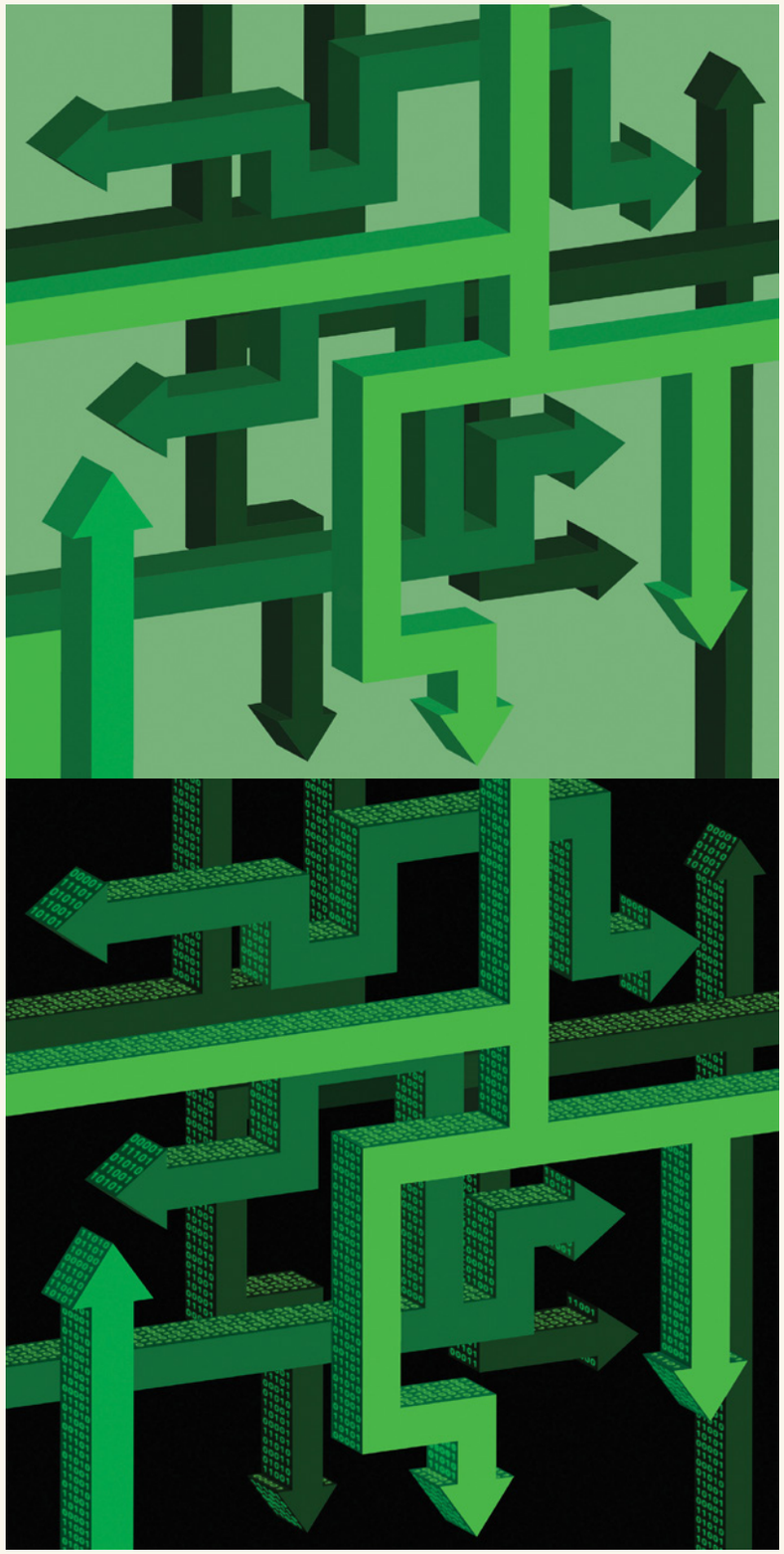
# What Is Encryption and Why Is It Essential?

In essence, encryption refers to the process of scrambling plain text, like emails or text messages, into an indecipherable format. This scrambled text, called ciphertext, helps in preserving the confidentiality of digital information stored on computers or transmitted via the internet and other networks. Once the message is delivered to the intended recipient, the data is translated or decrypted back into its original format.

The process involves the use of an encryption key, a collection of algorithms that can help scramble and unscramble the data, which is given to authorized senders and recipients.

Ensuring the security and privacy of that data is a priority for businesses in recent years, especially in light of evolving cyberthreats. According to a **2018 report from RiskBased Security**, over 5 billion records were exposed due to data breaches, while 2019 brought an onslaught of new threats, such as cross-site scripting attacks, AI botnets and formjacking.

As these threats continue to multiply in earnest, it isn't just consumers who are at risk of their data being compromised; companies can face significant setbacks due to loss of employee data. To protect the personal data of their customers and themselves, businesses need to be well-versed in various methods of data security, most notably encryption technology.



A majority of organizations use conventional safety protocols such as intrusion prevention, role-based access control applications and firewalls to protect their information. While these solutions do help prevent data breaches, if a breach does occur, data encryption software is considered to be a crucial last defense against the exposure or theft of private data.

Encryption solutions, when used in combination with efficient key management, can deliver robust protection for sensitive data, against modification, theft, disclosure or access by unauthorized parties, which is why they're often hailed as an integral part of any cybersecurity program. Data encryption is effective for data at rest (stored data), as well as data in motion (being transported or transmitted).

## The Rise of the Bring Your Own Device Trend

In recent years, bring your own device (BYOD) has gained rapid momentum. According to a **2014 Tech Pro survey**, over 74% of organizations were either planning to or were already allowing their employees to bring personal devices to work. In a **2016 Syntonic study**, it was observed that almost 87% of businesses were depending on employees using their own smartphones to gain access to business mobile applications.

More recently, in 2020, as the world bore witness to massive upheavals caused by the COVID-19 pandemic, the work-from-home culture began to emerge as a key survival tactic for businesses, making it essential for employees to utilize their own devices to access work-related data and applications.

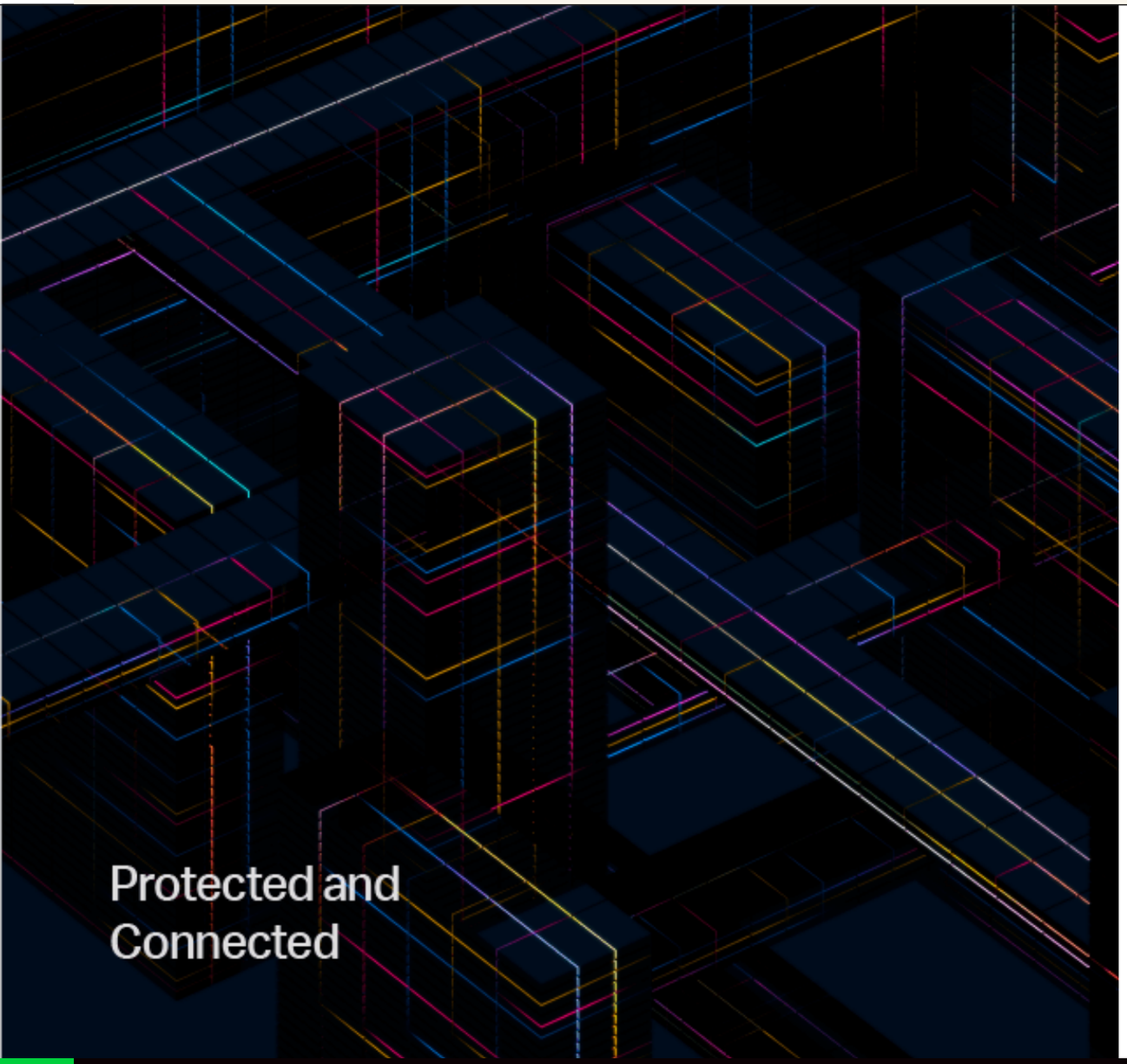
While the BYOD trend does bring many merits to the business world in terms of reduced software and hardware costs, it also adds considerable burden to the organization's IT department—which is commonly tasked with maintaining the devices as well as ensuring that the BYOD practice does not expose the company network or data to unauthorized access.

One of the major challenges blocking BYOD from reaching its true potential is the unauthorized use of personal devices by employees to carry out work-related tasks, irrespective of the company's BYOD policies. **According to Cisco**, for example, 95% of businesses allow employees to use their personal devices in the workplace.

Encryption software is emerging as a key solution in this scenario, making the execution of BYOD policies easier and ensuring a safer practice. Given that BYOD programs involve data access outside of the control of common business security measures, encryption solutions are essential for organizations to protect sensitive data both in transit and at rest.

Data encryption software helps organizations make sure that sensitive information is safeguarded even in worst-case situations like interception of traffic over unsecured networks or theft of devices.

For example, in March 2019, cybersecurity firm AppGuard introduced TRUSTICA Mobile, a communication app for mobile devices, equipped with military-grade security features, such as iris, fingerprint and facial biometrics for user authentication, as well as encryption keys modified for each interaction. The solution was designed to deliver encrypted file transfer and storage, voice and text messages, as well as video sessions. It was developed to strengthen BYOD policies for businesses and smaller companies and protect the privacy of employees.



## Encryption Technology Research and Development Efforts

With the solution beginning to gain rapid traction as a key part of cybersecurity, major encryption software market players are making significant strides in developing new encryption solutions designed to cater to evolving data security needs.

In December 2020, for instance, IBM Security introduced a new service designed to give companies the ability to explore the use of fully homomorphic encryption (FHE), an emerging technology that ensures data remains encrypted even while being analyzed or processed in third-party or cloud environments. The new solution, dubbed IBM Security Homomorphic Encryption Services, provides expert support and education to companies, as well as a testing environment for clients to build application prototypes that can leverage FHE.

Efforts to drive up the integration of encryption software in industrial applications are also seeing a rapid surge across developing economies. A notable example of this is the recent collaboration between the Data Security Council of India and India's Ashoka University, which resulted in the launch of the Coalition of India for a Progressive and Holistic Encryption Regime (CIPHER).

Consisting of like-minded individuals and establishments, the main objective behind the CIPHER coalition was to give policymakers a more nuanced and in-depth understanding of encryption. This in turn would allow them to create ideal crypto-based solutions for enhanced governance in the nation, as well as endorse the development of encryption technology and boost the start-up ecosystem in India.

## Looking Forward: EaaS Models

Cost optimization will also strengthen upcoming products in encryption software industry and serves as a focal point for business decisions. Encryption as a Service (EaaS) is one offering with the potential to transform security-related decision making. It has been estimated that the deployment of encryption services on the cloud will expand at over 25% CAGR up to 2026. EaaS models could be a significant driver of this growth, indicating a notable future trend in the industry.

**GET THE FULL REPORT**

Get the full GMI report on the growing encryption software market, and how remote work is influencing security trends.

**SALONI WALIMBE** is a senior research content developer for Global Market Insights, a global market research and consulting service provider offering clients actionable market data in key industries from technology, to renewable energy, to biotechnology and more.

# Defend Your Mainframe Data From Internal Threats

BY TREVOR EDDOLLS

Mainframe security was originally, quite sensibly, designed like a castle or fort. Companies had information to protect inside the castle. And there were lots of things outside the castle, some of which wanted to take the information you were protecting. That meant your walls needed to be strong and your gateway needed to restrict the flow of traffic, so you could check for bad guys trying to get in or your valuable possessions trying to get out.

These days, it seems that the threats are already inside the castle. The dark web is full of people's data—most of which has been stolen. It seems modern ransomware attacks involve exfiltrating data (e.g., getting it out past the guards on the gate), then corrupting the backups, and then encrypting the data.

On top of that, inside your metaphorical castle walls, you have disgruntled or pressurized staff, who may steal or corrupt your data. In truth, sometimes it's done in error or without realizing the consequences, but often it isn't.

So, we have people with stolen credentials gaining access to the castle, and we have disgruntled or unsuspecting trusted staff inside. In addition, we can't even see who anyone is because they are probably working remotely or they appear to be trusted personnel. What can we do to keep everything secure?

The answer would seem to be, don't trust anyone. Moving to Zero Trust Network Access not only makes it much harder for hackers to access a network, but seemingly authorized users can't access applications and data unless they meet pre-specified identity, device and application-based criteria. And that significantly reduces the attack surface for bad actors (hackers) to try to get through.

**Read the full article**

# Why Security and Backup and Recovery Are Increasingly Important

## 5 tips for developing a backup and recovery plan to reduce the risk of remote work compromise

BY JOANNA SOBRAN

Even as companies inch back toward some semblance of operational normalcy, the reality is that remote work will likely remain part of any reopening plan. This could mean some staff working from home full time, while others head into the office, or it could manifest as hybrid environments that see alternating at-home and in-office schedules.

No matter its eventual iteration, however, it's safe to say that working remotely has fundamentally changed the way companies do business—and will continue to do so for the foreseeable future.

Despite documented advantages for business productivity and staff flexibility, remote work also comes with a critical challenge: security. From privileged access to corporate networks on personal devices to the increased risks of phishing and business email compromise, the arms-length nature of off-site employee framework introduces the potential for lost assets, stolen data and even complete network compromise.

To deter downtime and reduce total risk, robust backup and disaster recovery services are more critical than ever for IT professionals to implement.

## Remote Work by the Numbers

While shifts toward remote work were ongoing before the pandemic, most companies opted for a slow and steady approach that saw only the minimum of access and applications offered to staff at home—and almost never full time.

COVID-19, however, changed everything. Overnight, enterprises that had virtually no experience with remote work were forced to design, deploy and integrate digital frameworks that allowed day-to-day processes to continue largely uninterrupted. All told, **88% of businesses** mandated or encouraged staff to work from home because of the pandemic, even as IT teams scrambled to connect cloud services and streamline mobile device adoption, according to a Gartner report.

The outcome was—and is—a work in progress as companies look to empower staff working from home without increasing overall risk. This is no easy task, and IT professionals are understandably worried about the impact of remote work on security at scale. In fact, a recent **OpenVPN survey** found that 54% of IT professionals believe remote workers pose a larger security risk than on-site staff.

## Potential Security Problems and Implications

It's one thing to worry about the abstract nature of remote work risk—it's another to recognize and prioritize the practical implications.

Consider the recent uptick of COVID-related phishing campaigns that target staff with fake messages supposedly from C-suite executives that demand urgent action or include malicious attachments that can infect user devices. Even prior to the pandemic, **28% of companies reported** corporate data loss and 19% said they had experienced at least one data breach in the last year, according to DataCore.

Employees also present potential problems for security: **Proofpoint** revealed that 50% don't they don't password-protect their home networks. What's more, 90% use corporate-issued devices for professional and personal activities. The result is an ideal environment for malicious actors—unprotected networks offer a shortcut to more critical corporate services, while connected devices provide a potential backdoor for privileged user access.

# 5 tips to Create a Backup and Recovery Plan That Reduces Security Risks

To reduce the risk of remote work compromise, it's worth creating a comprehensive backup and recovery plan that addresses common attack vectors and helps safeguard against more unlikely outcomes.

Top tips include:

1. **Consider current conditions:** While your recovery time objectives (RTOs) and recovery point objectives (RPOs) might make sense for pre-pandemic conditions, do they meet remote work requirements? Are they achievable given your current infrastructure? Consideration of your current RTO and RPO frameworks through the lens of remote initiatives can help identify the need for new partners or more robust technologies.

2. **Improve password protection:** Passwords remain the primary method of protection for most users—remote or on-site. They're also easily compromised, especially if staff select commonly used passwords, use them across multiple apps and leave them unchanged for months at a time. As a result, it's critical to create robust requirements that prevent the use of too-simple passwords and mandate the creation of new passwords every few months.

3. **Regulate remote work:** Remote work management is critical to ensure systems are secure, backed up and operating within normal parameters. Comprehensive managed services from trusted providers offer a streamlined way for companies to gain real-time views of remote networks, automate network backups and monitor infrastructure anytime, anywhere.

4. **Create secondary connections:** What happens if primary connections fail and users can no longer access corporate servers from home? Despite improved infrastructure, even massive cloud providers occasionally experience downtime or are victimized by cyberattacks. In a best-case scenario, connections are down for a few hours and tasks must be pushed back or paused. Worst case, productivity stalls for days as critical infrastructure is repaired. That said, it's a good

**The operational rewards—and increased risks—of remote work are here to stay. For many organizations, this means finding a middle ground between empowering at-home users and making sure they don't accidentally create avenues of compromise.**

idea to establish secondary connection protocols—such as the use of business-issued mobile devices as hotspots for VPNs—to get business back on track.

5. **Leverage multiple locations:** Natural disasters or cyberattacks can strike anywhere, anytime. To ensure remote workers don't suddenly find themselves facing days of lost work and the prospect of starting complex data-driven tasks over again, it's worth backing up your data in multiple locations—such as on-site and in the cloud—and implementing backup and disaster recovery solutions that automatically perform backups every few minutes to minimize potential data loss.

## Navigating Remote Realities

The operational rewards—and increased risks—of remote work are here to stay. For many organizations, this means finding a middle ground between empowering at-home users and making sure they don't accidentally create avenues of compromise.

In practice, building a remote balance requires robust backup and data recovery processes that define critical needs; boost password protection; regulate remote networks; support secondary connections; and leverage multiple storage locations to minimize the impact of malicious breaches; reduce the risk of accidental compromises; and limit data loss due to natural disasters.

**JOANNA SOBRAN** is president and CEO of MXOtech.

# Insights on the Growing Cybersecurity Market

BY LAUREN BORCHART

According to **a 2020 report from Global Market Insights** (GMI), the cybersecurity market has been flourishing in recent years. It surpassed $150 billion in 2019 and is expected to exceed $400 billion and grow at over 15% Compound Annual Growth Rate (CAGR) between 2020 and 2026. As organizations migrate their main businesses to digital platforms, the need for cybersecurity policies has grown.

This growth is largely due to the rising demand for secure networks and safe data accessibility. And, during the COVID-19 quarantine, forms of cybercrimes like phishing and hacking increased rapidly as internet use rose.

Recent emphasis on monitoring and safeguarding important cyber assets, and an increased interest in cybersecurity in general, have also helped the market grow. As big industries like finance, healthcare and small and medium-sized businesses (SMBs) have gone digital, data breaches have gained more attention. This has created the desire for major industries to invest in cybersecurity protocols and has led to the growth of the market.

While the demand for cybersecurity is growing across the world, the market is getting increasingly competitive as new cybersecurity products launch, and more major providers form partnerships. Some of the major players in the market include Cisco Systems Inc., Hewlett Packard Enterprise Development LP, IBM and Intel Corporation. The field has become so saturated recently that many large companies have been acquiring smaller companies and start-ups to diversify the products they offer and gain power in the cybersecurity industry.

**Read the full article**

This e-book was published by

TechChannel

901 N. 3rd St., Suite 195, Minneapolis, MN 55401 // (612) 339-7571

## Staff list

TechChannel

TechChannel.com is home to a variety of content to help you get started on your data security journey.

Learn more about data security