COMPUGEN
Innovate. Inspire. Impact.

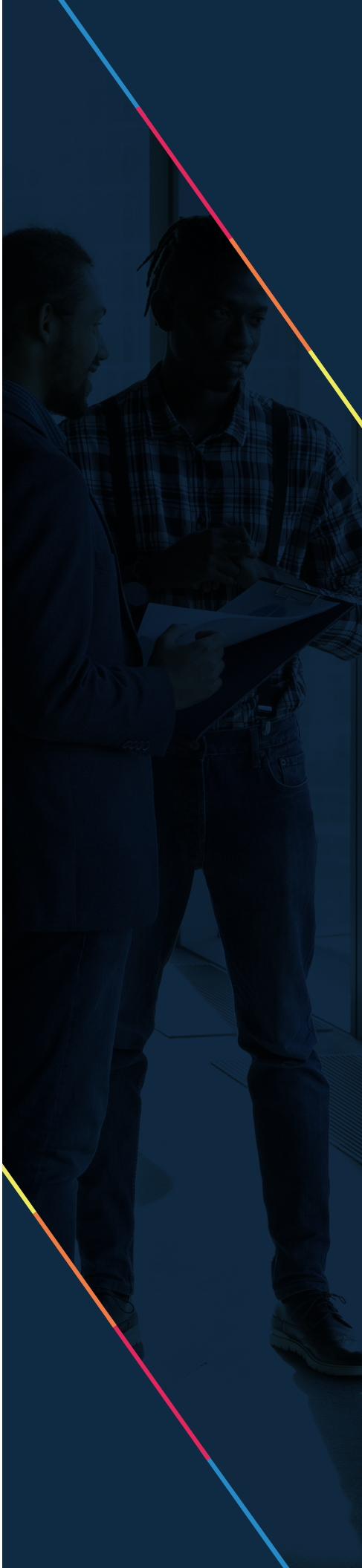
DELL EMC

2023 Cyber Security Trends + How Companies Practice Resilience

Explore critical Dell Security features as you catch up on key cybersecurity trends. Here's what you should know with essential stats and tips.

Dell Security, cybersecurity trends

Table of Contents

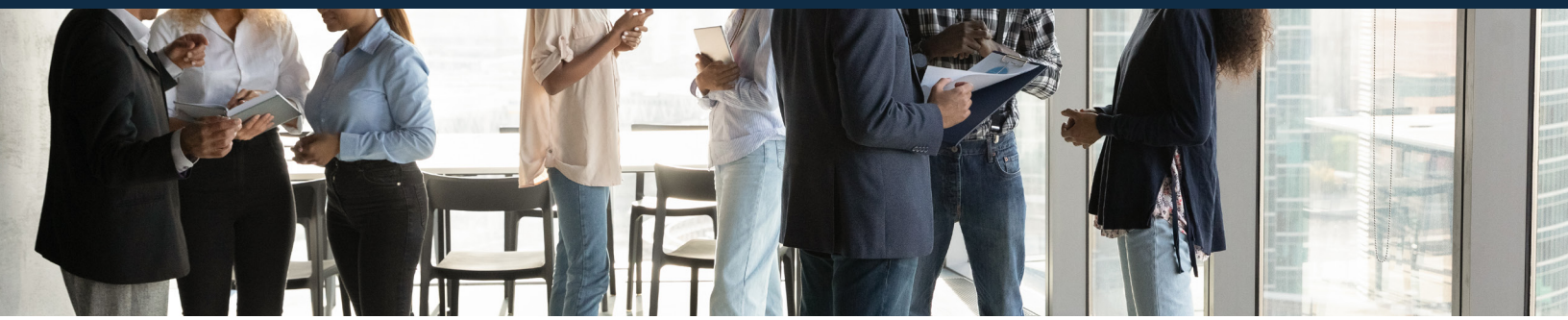


Businesses are racing to keep pace with the evolving complexity and sophistication of cyber threats, resulting in organizations doubling down on cybersecurity investments over the last two decades. Cybercrime increased by 600% during the pandemic, with the highest losses in the inancial sector. But, businesses around the globe spent an estimated $6 trillion on cybercrime damages in one year alone.

Today, organizations that rely on data are increasingly vulnerable to ransomware attacks and cyberattacks. Even a single cyber threat or attack could easily cost millions of dollars, and its effects can be ongoing due to the destructive nature of these attacks. In addition, there are many types of cyber threats, and attackers use multiple platforms and techniques to attack.

With cyber-attacks happening every 11 seconds, it's no longer a matter of if hackers or cyber criminals will attack your company. Instead, it's a matter of when it will happen and how expensive and damaging it will be. On average, companies spend $13 million for IT budgets to prevent cyberattacks and ransomware threats.

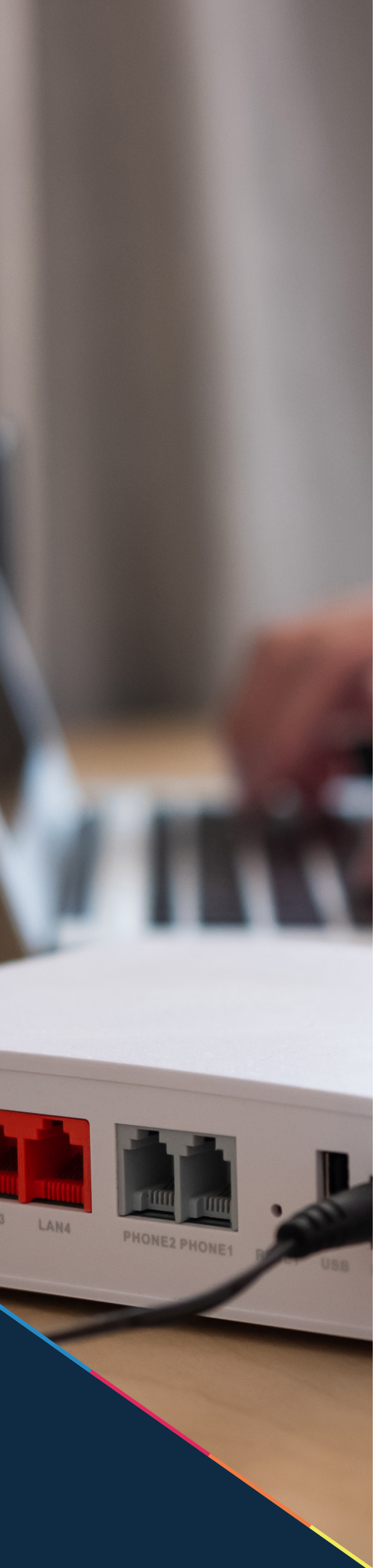
That's a relatively small price to pay, considering what could happen if you experience a hacker compromising your data and potentially bringing your company's operations to a standstill. The numbers are scary, but cybersecurity is not all bad news. Here are the top trends to watch.



Top 8 Cybersecurity Trends to Help Your Company Become Resilient

As part of its mission, Dell Technologies strives to create a connected, secure, and trusted world. As a result, Dell naturally builds cyber resilience and security into every solution, service, and product as part of their end-to-end approach to customer security, data, organization, and network.

As we look at the top cybersecurity trends that will help your company build and maintain resilience, it's essential to keep Dell's myriad of cyber resiliency and security solutions in mind. As new threats emerge, Dell helps you maintain a secure and resilient organization with Dell Endpoint Security and VMware Carbon Black Cloud, as well as Cyber Recovery services.



1. Connected New Technologies

The Internet of Things (IoT) will be online and connected by 41 billion devices by 2027. As the prime targets Because of their growing status as prime targets for cyber attacks, the IoT industry is searching for new ways to protect their devices. Unfortunately, hackers continue to develop techniques to circumvent cybersecurity tools almost as fast as the cybersecurity industry releases new security tools.

Since those trends are already well established, there's no reason to think they will continue to evolve. Increasingly, cybercriminals are targeting Multifactor Authentication (MFA) and Endpoint Detection and Response (EDR), which are now sometimes considered surefire protection against all cyberattacks and ransomware breaches.

You, too, may already rely on non-phishing-resistant multifactor authentication, but some hackers have already circumvented that. Similar techniques have been developed for evading EDRs, which will mean a massive spike in the availability and sale of EDRs soon.

Dell introduced CloudIQ, a cybersecurity machine intelligence solution to address these evolving cybersecurity issues. So, while you might identify specific factors that contribute to infrastructure health, you may still need an approach that will perform continuous health checks.

This evolving software solution aims to identify conditions that impact infrastructure health. Then, it offers recommendations for remediation. Beyond saving your organization time and money, CloudIQ cybersecurity features deliver infrastructure efficiencies. So, you're also better able to protect your company and prevent data breaches.

2. Escalated Credential Thievery

There will continue to be a devastating effect from cybercriminals leveraging large caches of leaked/stolen credentials. As a result, you may be adopting passwordless devices, password managers, and hardware identity tokens for your business and personal devices.

While most people reuse credentials between environments, systems, or sites, some variations of credentials are being reused. Attacks against traditional multifactor authentication will continue. As cyber criminals capture authentication tokens more often, you'll continue to see spikes in phishing, breaches, and other malicious activity. The greater success hackers have, the more of these threats you'll likely experience and be forced to mitigate in your business.

As these threats continue to escalate, it's critical to remain hyper-vigilant and clearly understand the strategies and skills you can deploy to protect your company and employees. Dells' Secureworks® TaegisTM XDR provides advanced analytics, critical and evolving expertise, and threat intelligence. So you're able to detect and respond to cyberattacks and ransomware threats quickly.

---

3. Expanded Metaverse Implications

You've likely noticed the upsurge of interest lately in the concept of the Metaverse. Even though many of the ideas are not new, it's exciting to think about how you and your company can connect with your clients and visitors in new, more immersive, mixed-reality environments.

As the Metaverse continues to grow, there are very real cybersecurity concerns you must watch and be aware of for interactions with the Metaverse. For example, you'll increasingly need to verify the identities of people and companies you think you're interacting with. And, as the Metaverse expands and AI fakes become more prevalent, you could open yourself and your company up for attacks or other malicious activity without processes in place to verify identities and authentication.

With the latest evolving technology, you can verify identities and virtual transactions via digital certificates built on blockchain technology. Dell's mission is to develop technologies that drive and support human progress. It's exciting to see and experience more of the world as we break down all those barriers.

With Dell's ecosystem and open standards, they'll continue to develop and be a part of advances that make game-changing experiences a reality. It's all about improving and expanding how you interact with the world, but you also must make security your top concern. Dell offers the layers of cyber protection you need to keep your data and identities safe in the myriad of environments you may find yourself.

4. Risks from Remote Work

It is estimated that by 2025, nearly 41 million Americans will work remotely. That's an increase of 87% compared with the number of remote workers before the pandemic. Unfortunately, the high number of remote workers also puts your organization at greater risk of cyberattacks, ransomware, and other malicious activities.

Hackers make phishing attempts on email, text, voice, and even third-party applications because they are easy targets, mainly when some remote workers haphazardly manage them. In addition, those hybrid or fully remote employees may be less protected by the same level of security and infrastructure in their home office or hybrid space.

As mobile and remote working continues to grow exponentially, Dell SafeData and Dell SafeGuard help to protect you from cyber breaches. Dell SafeID separates the operating environment from memory and critical data in protecting your secure operations. By executing operations and securely storing credentials, SafeID keeps credentials locked down. So, you can protect your data better while preventing hackers from modifying or accessing your templates and encryption keys.

This level of security and protection is exactly what you need for the evolving modern work environments. It may be invisible, but it's also smarter, faster, and even seamless. So, you can keep your remote employees collaborating and working at peak efficiency. All the while, you're abiding by compliance regulations and key security protocols to maintain safety and protection against cyberattacks and ransomware.

Protecting against targeted cyber-attacks requires proactive management of your organization's cybersecurity maturity. Your organization can prepare proactively and deal with the next security event successfully by establishing mature, robust security controls, and understanding prevention alone isn't enough.

5. Increased Cloud Service Attacks

Since the advent of cloud-based computing a few years ago, many businesses have moved away from physical infrastructure to access software applications, data storage, and other services on the internet. Reducing operational costs and increasing efficiency are two benefits of embracing this technology.

Cloud security leaders will face a challenge in 2023 in hiring the talent they need. Due to the need for specialized and niche professionals, one of the biggest challenges is finding skilled professionals to support your evolving cybersecurity requirements.

In an era when so many organizations are turning to the cloud for their business needs and where cybersecurity skills are in increasing demand, cybersecurity generalists are the answer. In order to build internal teams, organizations will reskill specialists back to generalists and recruit more generalists with proven track records.

6. Normalized Zero Trust

The concept of zero trust in cybersecurity is relatively new, but it represents a shift in how companies handle user onboarding and management. With this method, you must authenticate all users and constantly validate their access to your systems. As part of the process, your users will be required to prove their identities and authorized permissions before they can access the data on your servers.

The zero trust method contrasts with the more traditional user onboarding practice of requiring users to log in once and giving them access to all your content. As remote workers continue to be more vulnerable, zero trust makes it more difficult for hackers to damage or take over your system once they've gained rudimentary access via a targeted user.

That's why businesses are increasingly moving toward accepting the ideas around and adopting the zero-trust methodology. While it may seem paranoid or even overly restrictive, zero-trust protocols protect your company against ransomware and malware activities and damages.

7. Reduced Downtime + Core Functionality with AI

Both cybercriminals and cybersecurity professionals will use artificial intelligence (AI) to gain an advantage. As you adopt AI-based security controls and response mechanisms, you can better protect your data and reduce downtime from attacks or malicious activities.

The Dell Technologies AIOps application for Dell EMC IT infrastructure products, Dell EMC CloudIQ, recently introduced cybersecurity features as part of its cyber resilience and security solutions. With this approach, the company simplified and automated IT processes while making cybersecurity robust and flexible.

Using artificial intelligence, your company can detect cyberattacks more easily. With machine learning, you're able to learn as it can learn what the typical network should look like. So you can better flag activity and breaches immediately instead of waiting for more widespread damage or lock-outs. With that level of automation and self-sufficient, machine-learning functionality, it's no longer just a nicety. AI is now a vital component to achieving the success you need for your organization.

---

8. Rise in Hackers in the Recession

The recession means hackers have more reasons to delve into previously unexplored realms of cyber criminality. Even newbie, less technical criminals will attempt malicious attacks and ransomware breaches out of desperation when faced with their currently bleak prospects. That's bad news for your company, even if you think you're prepared for cyberattacks and ransomware.

It's also so much easier for hackers to find the tools and even gain backing for what could be easy profits. Cybercriminals have become more motivated to commit cybercrimes in pursuit of monetary gain because of this trend, making it difficult to track and identify them. Consequently, you and your cybersecurity professionals must implement strategies to prevent these attacks and protect your company from evolving threats in the future.

Organizations or industries that are on the brink of collapse are targeted by cyber criminals to tip them over. Manufacturing - the backbone of supply chains - suffered from this last year. Ransomware attacks are expected to spike in 2023 as a global recession looms. After spending time and money fighting back against ransomware, more prominent organizations in heavily impacted regions are the best prepared for this new wave.

Designed to protect data against ransomware and other sophisticated threats, Dell's PowerProtect Cyber Recovery solution isolates vital information from threats. Using machine learning, you can detect suspicious activity and recover known good data to resume normal business operations. Ransomware and sophisticated cyber threats can threaten your critical data if they are not protected and isolated. Machine learning can identify suspicious activity so that data can be recovered and normal operations can be resumed.

Cyber attacks and ransomware target the data that drives your business - PowerProtect Cyber Recovery protects it. Data is isolated from the attack surface by automation and intelligent security. PowerProtect Cyber Recovery gives you the confidence that your data and business are protected, encrypting it and storing it immutably within a dedicated cyber vault.

Dell ensures cyber resilience and business continuity on-premises and in multiple cloud environments. To protect US financial institutions from cyber threats like ransomware, PowerProtect Cyber Recovery was the first and only solution that received endorsement from Sheltered Harbor for complying with all requirements.

Why Dell's Cyber Recovery is Important?

In cyberattacks, your valuable data (including backups) is often stolen, destroyed, or otherwise compromised. That's not something you can easily recover from when you experience that level of loss and destruction. Restoring normal business operations post-attack requires protecting and recovering critical data with assured integrity. So, what are the chances of your business surviving?

As part of Dell Technologies Services, Dell EMC PowerProtect Cyber Recovery helps ensure your data protection vault is air-gapped and increases confidence in your ability to recover from a cyberattack. Two primary focus areas for Dell's Cyber Recovery services are advisory and implementation.

Your organization can benefit from Dell Technologies' assistance in improving its current rating. For organizations of all sizes, intrinsic security is essential for safeguarding their digital lives. It's a comprehensive cyber resilience strategy. It safeguards digital lives and protects your organization's entire digital ecosystem. So you'll know that your data is safe from cyberattacks and ransomware. Given that level of safety and security, you'll be able to achieve your goals.

How Compugen Can Help

As we've discussed, organizations are doubling down on defense strategies as security threats become more sophisticated and targeted. The pandemic dramatically affected the growth and efficacy of cybercrime and hackers, as cybercriminals have exploited less secure networks. But the upsurge in cybercrime and ransomware is still a top priority even as the pandemic's effects have somewhat lessened.

As one of Canada's largest privately owned and operated IT services providers and PC systems integrators, Compugen can help you design the modern workspace of your dreams without the stress or heavy lifting associated with doing it on your own. Developed from internally recognized industry frameworks and standards, Compugen's Cybersecurity Lifecycle Framework (CLF) offers layered security solutions and services.

As a result, information security threats can be detected and prevented. You can also analyze the data to ensure that your future response and protection strategies continue to evolve in productive and compliant ways for the safety and security of your company. So the response is not only immediate and practical but also ongoing.

We guarantee compliance, enhanced security expertise, and business continuity regardless of whether you choose Compugen's managed or professional services. Our mission is to provide customers with unique human experiences every day, using technology-based solutions. In addition, our mission is to create a positive and ripple effect in the world by developing technology solutions as a service.

COMPUGEN
Innovate. Inspire. Impact.

DELL EMC

Schedule a Modern Workspace Audit with Compugen to bring the right level of foresight and insight to your team.

From better collaboration and communication to easier changeover and security management, Microsoft Modern Workspace promises to ease employees' and IT teams' respective jobs. What's more, every subsequent update can be readily provided through the Cloud to ensure your software systems remain updated. As your modern IT Partner, we help you implement innovative technology-based solutions, turning the unreachable into the achievable.

Book Audit