CYBERSECURITY TRENDS TO WATCH IN 2023

Explore the impacts of hybrid work, ransomware, cloud security and data regulation.

Insight

The future of cybersecurity

Cyberattacks are growing more common — and more sophisticated — by the day. In today's threat landscape, no business can afford to relax their security measures or fall behind in having the latest security tools.

In this ebook, we'll explore four top trends shaping cybersecurity today and the technology you need to stay secure. We'll look closely at:

Hybrid work: This new workforce structure is here to stay, and cybercriminals are taking advantage. Identity and access management, endpoint security and user awareness are vital.

Ransomware and phishing: These threats remain a top security concern due to their low cost and high profit model. It's crucial that your organization takes appropriate steps to defend data, systems and people.

Cloud security: Cloud applications and data are popular targets for cybercriminals, but smart technology can bolster your defense.

Data protection: Analytics are evolving, and privacy laws are changing the way we view data security. We'll cover tools that help protect your most sensitive information.

Hybrid workforce security

Many companies are shifting to a permanent hybrid work model. In fact:

74% of U.S. companies are using or plan to implement a permanent hybrid work model.[1]

When teammates access servers from multiple locations and devices, vulnerabilities are inevitable — but powerful security can defend employees and data in the home, on mobile devices and in the office.

Identity and Access Management (IAM) technology expands visibility and control over users across your network.

When your business depends on applications for productivity and engagement, you need powerful post-deployment protection. **Application security** software minimizes the risk of threats, breaches and code hijacking.

Minimize vulnerabilities across your IT environment with **network and infrastructure security**, such as firewalls and Virtual Private Networks (VPNs).

Employee awareness training

Don't dismiss the importance of user training. For instance, employees often bypass or avoid VPNs due to slow network speeds or dropped connections. Proactive educational sessions educate your team on the importance of a VPN — and the risks of disconnecting.

Ransomware and phishing: IT's biggest concern?

Ransomware remains one of the most concerning security threats in today's digital landscape. Ransomware is a form of malicious software designed to encrypt files and render systems and data unusable until a ransom is paid.

The 2022 Mid-Year Cyberthreat Report by Acronis[2] called ransomware the number-one threat to large and medium-sized businesses. The report estimates that global damages related to ransomware attacks will top $30 billion by 2023.

Unfortunately, phishing and malicious emails are a preferred method of cybercriminals. And, even with security training, many employees struggle to recognize a phishing attempt.

The good news? Strong email security can mitigate the risk of targeted ransomware. Email security software delivers a robust defense against malicious messages, including vital tools such as firewalls, encryption and filtering to make it harder for bad actors to enter your internal systems. Antivirus protection and Artificial Intelligence (AI)-powered predictive analysis will also shore up your defense against this evolving danger.

Additional preventative measures include regular system updated, strong IAM security, restricted permission and limited network access, and automated data backup tools.

Advanced cloud protection

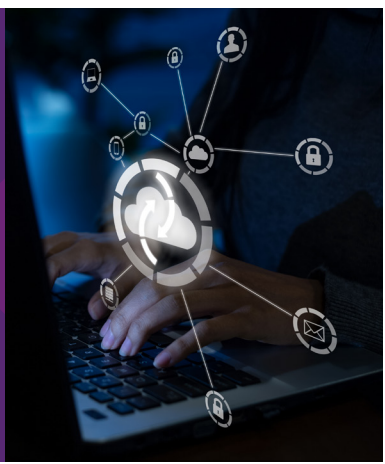
Cloud migration has rapidly increased with the permanence of hybrid work. In fact, the foundation of remote work relies on the effective adoption of cloud computing. This shift has resulted in multi-cloud environments, enhanced AI capabilities, machine learning and increased demand for cloud-to-edge applications. But successful use of the cloud requires ongoing management, tactical security decisions and knowledge of evolving cyberthreats.

Security for the cloud enables organizations to modernize and scale with confidence. Whether you've adopted a public, private or hybrid cloud model, Insight offers a host of cloud security offerings to boost visibility and protection.

With the right tools, you'll defend against sophisticated cloud attacks.

Advanced cloud security includes:

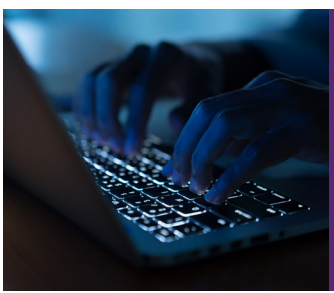
- Proactive data and application protection
- Cloud disaster recovery
- Zero Trust security
- Secure encryption
- Cloud Security Posture Management (CSPM)
- Risk monitoring and threat detection



The rise of data

Today's businesses rely on a constant flow of data — and the modern consumer will sever ties with companies they don't trust with their information. While data breaches are a top concern, new and evolving regulations are just as important a factor in structuring your cybersecurity ecosystem.

On May 25, 2018, the General Data Protection Regulation (GDPR), a privacy policy that sets guidelines for collecting and processing personal information in the European Union (EU), came into effect. The GDPR has affected businesses worldwide, and the regulation enlists severe fines against violators.



Gartner predicts that by the end of 2023, 65% of the world's population will have their personal data covered under a data privacy regulation. In comparison, this percentage was 10% in 2019.[3]

As our world becomes more digitized, it's vital to have a finger on the pulse of privacy laws. Preparation for future privacy laws can make an enormous difference in how you navigate upcoming regulations. So, how can you stay up to date with all the information?

With Insight on your side, you'll have a team of committed experts to walk you through every step of privacy changes, endpoint vulnerabilities, user access control and leading security for data protection.

Prevent.
Detect. Defend.

When it comes to a cyberattack, it's not an if — it's a when. And, in the face of evolving threats, securing your organization can seem like an impossible task.

Insight is here to help.

Our skilled security experts are standing by to guide you from end to end. We'll help you implement cybersecurity technology to improve efficiency, effectiveness and strategic alignment.

With Insight as your technology partner, you'll enjoy a robust catalog of cybersecurity technology from leading brands to keep you confident and secure.

Your business will benefit from:

- Optimized costs
- Improved accuracy for entitlements
- Better future forecasting
- Increased readiness for internal and external audits
- Consistent compliance
- And more

Gain visibility and control over your IT environment.

Talk with an Insight expert today.

About Insight

Insight Enterprises, Inc. is a Fortune 500 solutions integrator helping organizations accelerate their digital journey to modernize their business and maximize the value of technology. Insight's technical expertise spans cloud and edge-based transformation solutions, with global scale and optimization built on 34 years of deep partnerships with the world's leading and emerging technology providers.

Insight

1.800.INSIGHT | insight.com

[1] McCain, A. (2022, Sept. 22). 30 Essential Hybrid Work Statistics [2022]: The Future Of Work. Zippia.

[2] Acronis. (2022). Mid-Year Cyberthreats Report 2022.

[3] Gartner. (2020, Sept 14). Gartner Says By 2023, 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations.