4 Cybersecurity Trends to Watch in 2022

Navigate an evolving security landscape with advanced solutions.

Insight®

Future-proof your business.

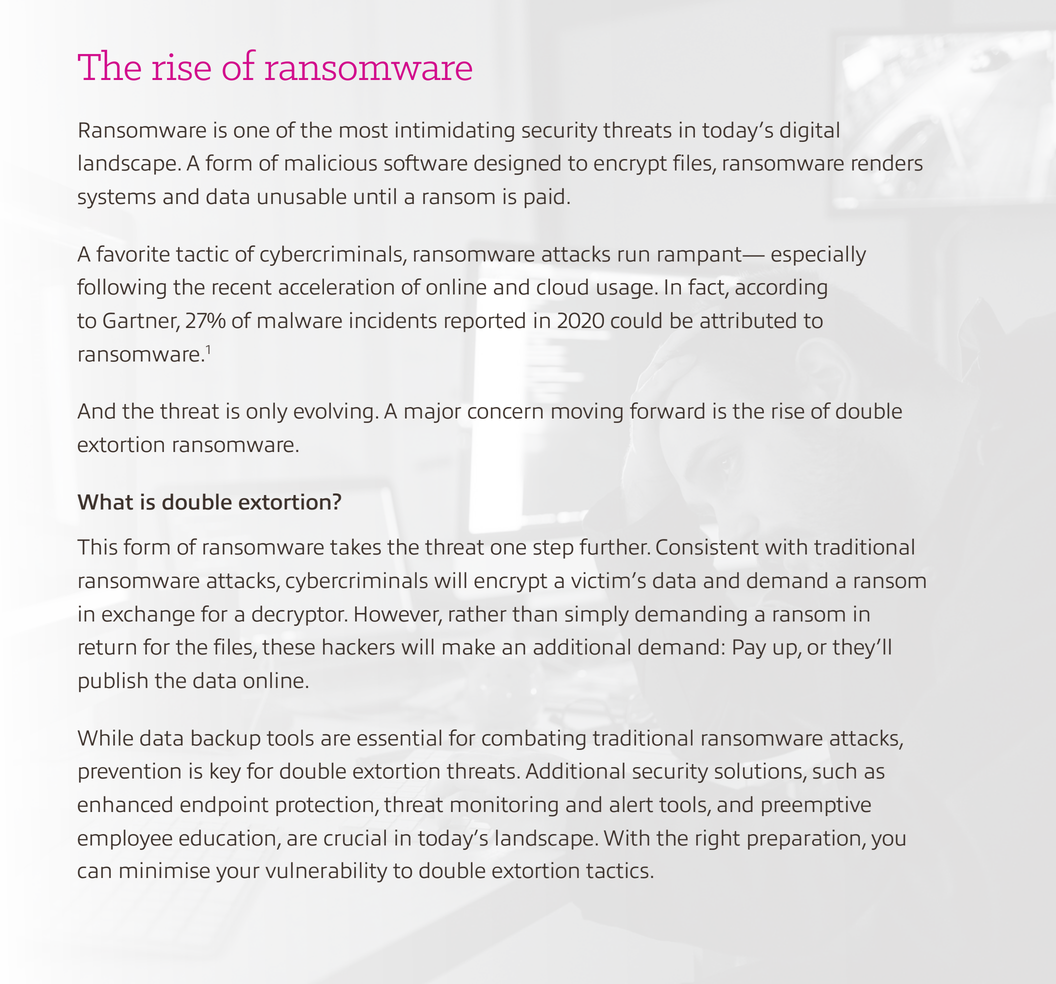
To thrive in a new threat landscape, you'll need future-ready security solutions.

With the rapid acceleration of cloud usage and digitised systems, a host of new security concerns are likely to emerge in the new year. Growing threats around network defence, data protection and multicloud strategies are dominating the security conversation, while cybercriminals have become faster, smarter and more discreet than ever before. It's crucial that businesses stay mindful of the latest predictions.

Here are four key security trends to monitor in 2022:

1. **Evolving ransomware**
2. **Hybrid workforce targeting**
3. **Impending data regulations**
4. **Proactive cloud protection**

Let's take a deeper look at each topic and explore advanced solutions to safeguard your organisation.



The rise of ransomware

Ransomware is one of the most intimidating security threats in today's digital landscape. A form of malicious software designed to encrypt files, ransomware renders systems and data unusable until a ransom is paid.

A favorite tactic of cybercriminals, ransomware attacks run rampant— especially following the recent acceleration of online and cloud usage. In fact, according to Gartner, 27% of malware incidents reported in 2020 could be attributed to ransomware.[1]

And the threat is only evolving. A major concern moving forward is the rise of double extortion ransomware.

What is double extortion?

This form of ransomware takes the threat one step further. Consistent with traditional ransomware attacks, cybercriminals will encrypt a victim's data and demand a ransom in exchange for a decryptor. However, rather than simply demanding a ransom in return for the files, these hackers will make an additional demand: Pay up, or they'll publish the data online.

While data backup tools are essential for combating traditional ransomware attacks, prevention is key for double extortion threats. Additional security solutions, such as enhanced endpoint protection, threat monitoring and alert tools, and preemptive employee education, are crucial in today's landscape. With the right preparation, you can minimise your vulnerability to double extortion tactics.

Protecting your hybrid workforce

As a dispersed workforce becomes the new normal, organisations must consider numerous issues — including the security impact of hybrid workers. When teammates access their organisation's servers from multiple locations and multiple devices, vulnerabilities are inevitable. Endpoint, email, and Identity and Access Management (IAM) solutions are crucial to your organisation's protection.

When ushering in a new era of long-term hybrid work, companies should stay vigilant around application and network security. As workers begin to return to the office, cybercriminals may target laptops and mobile devices with malware designed to infect corporate systems when reconnected to the network. Multi-layered security can help monitor and detect these threats.

- **Strong application security** will provide account authentication, in-app activity records and encryption for cloud-based data.
- **Network and infrastructure security** apply solutions such as firewalls and Virtual Private Networks (VPNs) to limit intrusions.

Cybersecurity training

While workers move between home, public and office networks, frequent employee education can shore up your cyber defence. As mentioned above, VPNs establish a point-to-point connection between your office server and a remote device, encrypting data before it is sent through the link. However, employees often bypass or avoid VPNs due to slow network speed or dropped connections. With proactive educational sessions, your team will know the importance of a VPN — and the risks of disconnecting.

Preparing for new data regulations

As the world and businesses become more digitised, we'll continue to see a higher demand for data protection. In their 2020 projections for the future of privacy[2], Gartner predicted that 65% of the world's population will have their personal information covered under modern privacy regulations by 2023, up from 10% today. The company also predicted that by year's end 2022, more than one million organisations will have appointed a privacy officer (or data protection officer).[2]

In a digital-first world, stricter protections on data privacy are inevitable, and the majority of consumers desire a protection standard. A 2021 survey by Morning Consult found that 83% of American support the idea that Congress should create a national standard for data privacy in the U.S.[3]

To maintain business continuity, it's crucial to stay aware of new developments in data regulations.

A team of experts on your side

With a technology partner like Insight, you'll have a team of dedicated experts to guide you through data protection changes — and to provide leading solutions for securing your data now. Our deep catalogue of trusted solutions for encryption, access, tokenisation and more will help keep your most critical information protected, compliant and uncorrupted.

Upgraded cloud security

Rapid cloud migration has been a key focus of the past two years, and even more new cloud strategies will take centre stage in 2022. With multicloud environments, enhanced Artificial Intelligence (AI) capabilities and an increased demand for cloud-to-edge applications, defending your cloud services against threats boosts your overall business protection.

Key cloud security trends to watch include:

- Proactive data protection
- Zero Trust model security
- Cloud Security Posture Management (CSPM)
- IAM tools
- Centralised platforms

To combat advanced threats, you'll need modern, sophisticated tools. Brute-force attacks and configuration errors are common cloud entry points for hackers, but with smart solutions from Insight — including email, data, network and infrastructure security software — you'll defend against modern attacks.

Secure your IT environment against sophisticated threats.

Cyberattacks are always evolving, which can make securing your organisation feel daunting. That's where a technology partner comes in. At Insight, our experts will guide you from end to end, leading to improved efficiency, effectiveness and strategic alignment.

With security solutions from Insight, you'll benefit from:

- Optimised costs
- Improved accuracy for entitlements
- Better future forecasting
- Increased readiness for internal and external audits
- Modernised data center with comprehensive protection
- Consistent compliance
- And more

Insight's deep partnerships with leading brands provide a robust catalogue of enterprise security solutions to protect your business. Our skilled team will help find, deploy and manage these services to keep you confident and secure.

Discover, mitigate and avert risk with advanced cybersecurity. Talk with an Insight expert today.

About Insight

Today, every business is a technology business.

Insight Enterprises Inc. empowers organisations of all sizes with Insight Intelligent Technology Solutions™ and services to maximise the business value of IT. As a Fortune 500-ranked global provider of Digital Innovation, Cloud + Data Centre Transformation, Connected Workforce, and Supply Chain Optimisation solutions and services, we help clients successfully manage their IT today while transforming for tomorrow. From IT strategy and design to implementation and management, our 11,000 teammates help clients innovate and optimise their operations to run business smarter. Discover more at **uk.insight.com.**

0344 846 3333 | uk.insight.com

[1] Sakpal, M. (2021, Nov. 16). 6 Ways to Defend Against a Ransomware Attack. Gartner.

[2] Moore, S. (2020, Jan. 20). Gartner Predicts for the Future of Privacy 2020. Gartner.

[3] Sabin, S. (2021, April 27). States Are Moving on Privacy Bills. Over 4 in 5 Voters Want Congress to Prioritise Protection of Online Data. Morning Consult.