

10 Security predictions for 2023

Do what matters for your security. Avanade's experts predict the biggest security trends you need to know in 2023

Medium impact

1. Phishing emails will get more human

Conversational language tools such as GPT-3 and GPT Chat will be used to write phishing emails that sound more human and more clickable, making phishing attacks harder to spot and manage.

Danilo Benedetti, Cyber Architect

2. Practical security will trump compliance

Businesses will focus on improving their own practical security in addition to third-party compliance requirements. This will see a rise in demand for integrated solutions over best-of-breed.

Ben Warriner, Cyber Architect

Medium impact

3. DIDs will enter the mainstream

Decentralized Identifiers (DIDs) verify a user through an identity wallet that holds information about the user such as ID cards and qualifications. IDaaS platforms will drive business adoption of DIDs, enabling businesses to implement more effective zero-trust security policies and improve remote worker experiences.

Darren Robinson, Digital Identity Lead

4. Security expansion will be needed for remote working

As cyberattacks on remote workers become more advanced, companies will be forced to move from their traditional centralized security model to a secure service access method that extends security beyond the perimeter.

Andi Hudson, EU Cyber Centre of Excellence Lead

5. It's time for the security platform era

Vendors will accelerate their consolidation of security services and products, supporting the shift from niche best-of-breed solutions to flexible best-of-platform options.

Rajiv Sagar, Avanade Cybersecurity Lead

6. Look out for the talent gap

The security skills gap will increase over the next year. Businesses must rely on trusted security partners to help them through the next set of challenges, while governments and education will rely on the private sector to improve skills and support new talent.

Andi Hudson, EU Cyber Centre of Excellence Lead

High impact

7. Manufacturers will seek onshore stability

Recent economic events will trigger businesses to consider bringing their manufacturing and production lines back onshore in search of stability. However, reshoring businesses will need to rethink the security of their supply chain technology due to intellectual property risks and cyberthreats.

Uche Ishionwu, IoT/OT Security Architect

8. The dawn of Internet of Everything

The integration of IoT, AI and distributed ledger technologies (such as blockchain) will form the next-generation Internet of Everything (IoE). IoE will support digital identities, trust, transparency and decentralized automation – increasing efficiency and security across all industries.

Uche Ishionwu, IoT/OT Security Architect

High impact

9. Cyberwarfare will disrupt supply chains

Nation-against-nation cyberwarfare will increase, destabilizing governments, economies and populations. These cyberwarfare campaigns will disrupt supply chains and resource production leading to further increases in consumer prices.

Jason Revill, Cybersecurity Centre of Excellence Lead

10. Trust in automation

Automation will continue to be the primary force in security monitoring and protection. Using a SOAR platform to automate security response will enable organizations to protect a larger data surface and allow defenders to respond to adversaries earlier and more effectively. Automation will also become increasingly aligned to industry use cases to support collaboration on industry-specific threats.

Anand Manoharan, Growth Markets Security Lead

Avanade can help you make sense of tomorrow's security challenges, so you can focus on prioritizing what matters for your organization's security.

Get in touch with one of our team to learn how.

Contact us 