



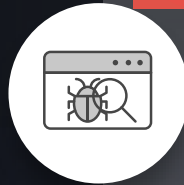
Aligning Business Objectives with the Cybersecurity Landscape

Jack Chan

Vice President Product Management | Field CTO APAC



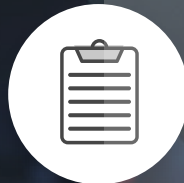
Agenda



The Big Picture – Business & Cybersecurity



Evolution of Networks and Threats



Mitigation Strategies



Useful Resources



CONFIDENTIAL

Access Limited to Authorized Personnel

“There are only
two types
of companies:

Those that **have** been hacked,
And those that **will be.**”

Robert Mueller
FBI Director, 2001-2013





The Big Picture – Business Factors



DIGITAL EVOLUTION

Digital innovation is creating tremendous opportunity, but more risk



TECHNOLOGY DISRUPTION

More companies are rapidly implementing AI to transform business operations



ECONOMIC HEADWINDS

Budget changes and skills shortage are resulting in more delays and more risk



SKILLS SHORTAGE

With 3.4M unfilled jobs, the struggle to recruit and retain cybersecurity talent creates additional cyber risks



ENVIRONMENTAL, SOCIAL & GOVERNANCE

Consumers and boards are putting more pressure to deliver on ESG initiatives



REGULATORY AND COMPLIANCE

Companies are reacting to more frequent reporting and regulatory changes



THREAT LANDSCAPE

Attacks are growing in sophistication and frequency

Long-lived Exploits
Industrial Ransomware
Supply Chain Attacks
Cloud Risks
APT Threat Actors
New Vulnerabilities
Targeted Attacks On The Rise
Insider Risk



The Business Risks Are Obvious

Recent Examples



Blue Screen of Death



Supply Chain Attacks

You cannot protect what you don't know....





The Business Risks Are Obvious

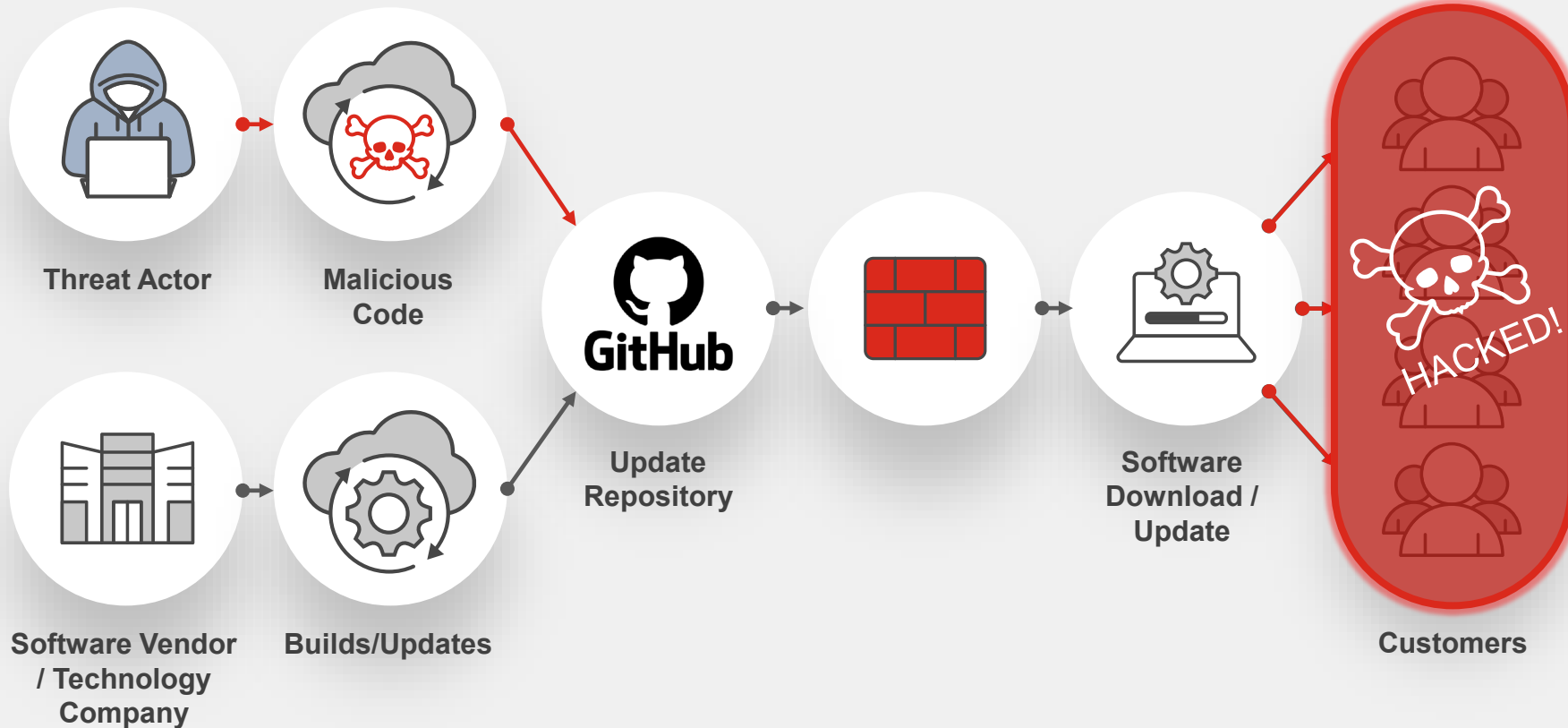
Recent Examples



Blue Screen of Death



Supply Chain Attacks



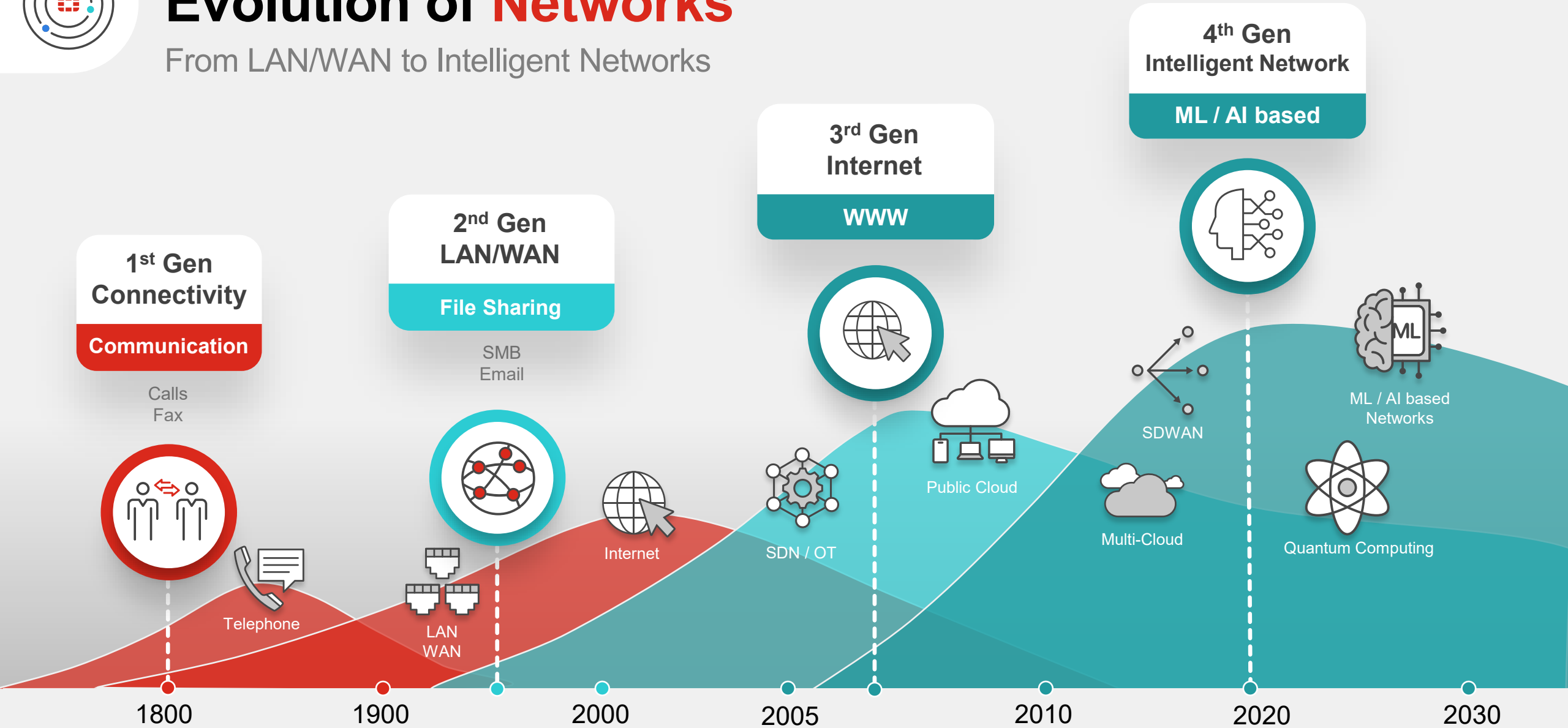
You cannot protect what you don't know....





Evolution of Networks

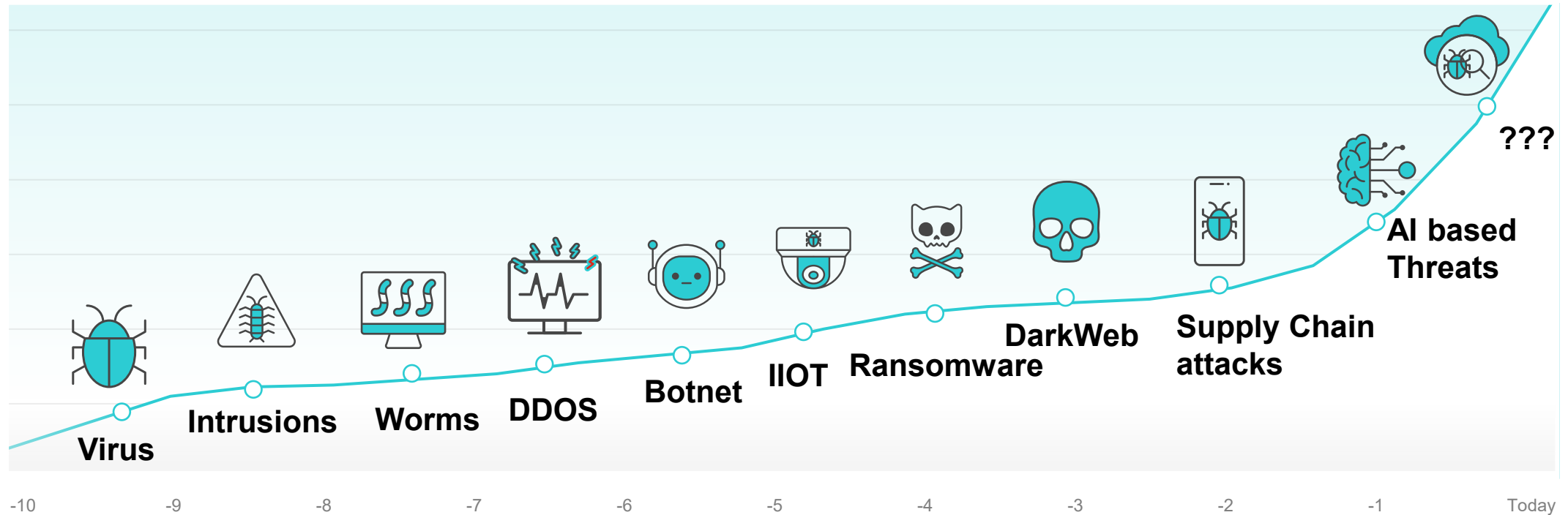
From LAN/WAN to Intelligent Networks





Evolution of Threats

Threat Landscape Changes



2014

10 Years

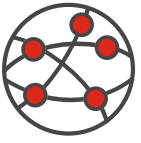
2024



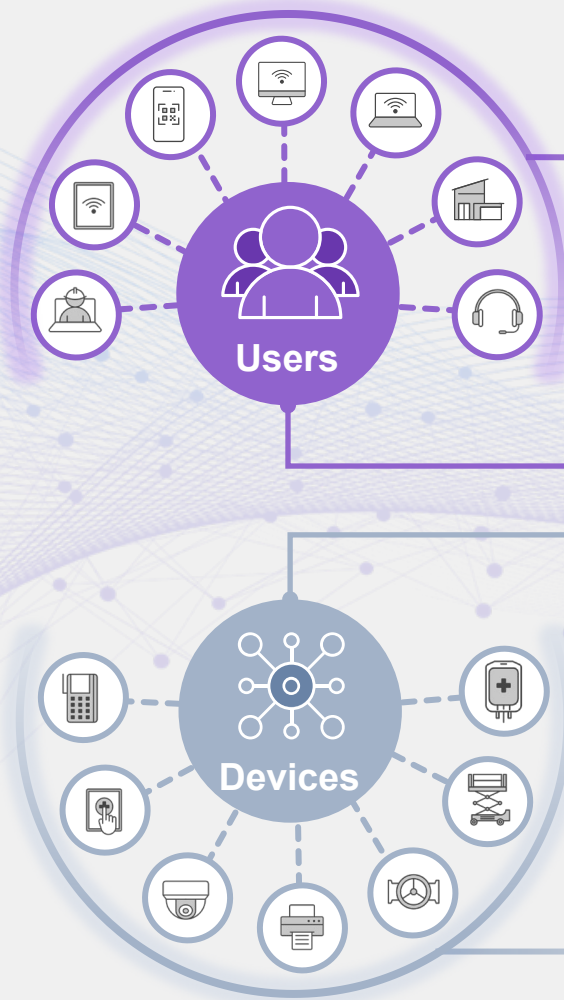
This content is shared exclusively with the **CTO Office** and **Product Management** teams and is considered void if transferred to (or presented by) anyone outside of this group. The contents are for individual use and should not be copied, transferred, uploaded or shared to anyone without written consent. © Fortinet Inc. All Rights Reserved.

CONFIDENTIAL

Access Limited to Authorized Personnel



The 20th Century of Networking



84%

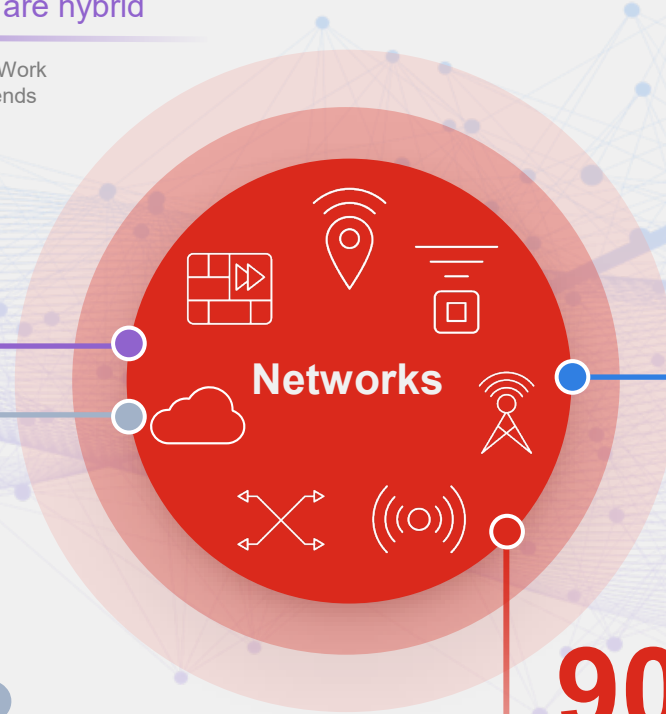
Companies are hybrid

Forbes: Remote Work Statistics and Trends

42B

IoT devices

IDC: World-Wide IDC Forecast



Networks

125+
Distributed applications
used by enterprise

2022 Gartner: Market Guide for SaaS Management Platforms



Apps

90%

Of enterprises will have experienced a security incident related to the edge network by 2026

2022 Gartner: 2022 Strategic Roadmap for Edge (IoT) Networking





The Real Question is...

“What are we trying to
PROTECT?”

“Where is the
VALUABLE information?”



The Threat Landscape is More Complex Than Ever



**LONG-LIVED
EXPLOITS**



**EXPANDING ATTACK
SURFACE**



**TARGETED ATTACKS
ON THE RISE**



APT THREAT ACTORS



**ABUNDANT 0-DAY
MALWARE**



**INDUSTRIAL
RANSOMWARE**



CLOUD RISKS GROW



**SUPPLY CHAIN
ATTACKS**



INSIDER RISK



**RIISING CRITICAL
THREATS**

Source: 2H 2023 Global Threat Landscape Report, Outbreak Alerts Annual Report 2023 & The 2024 Cloud Security Report

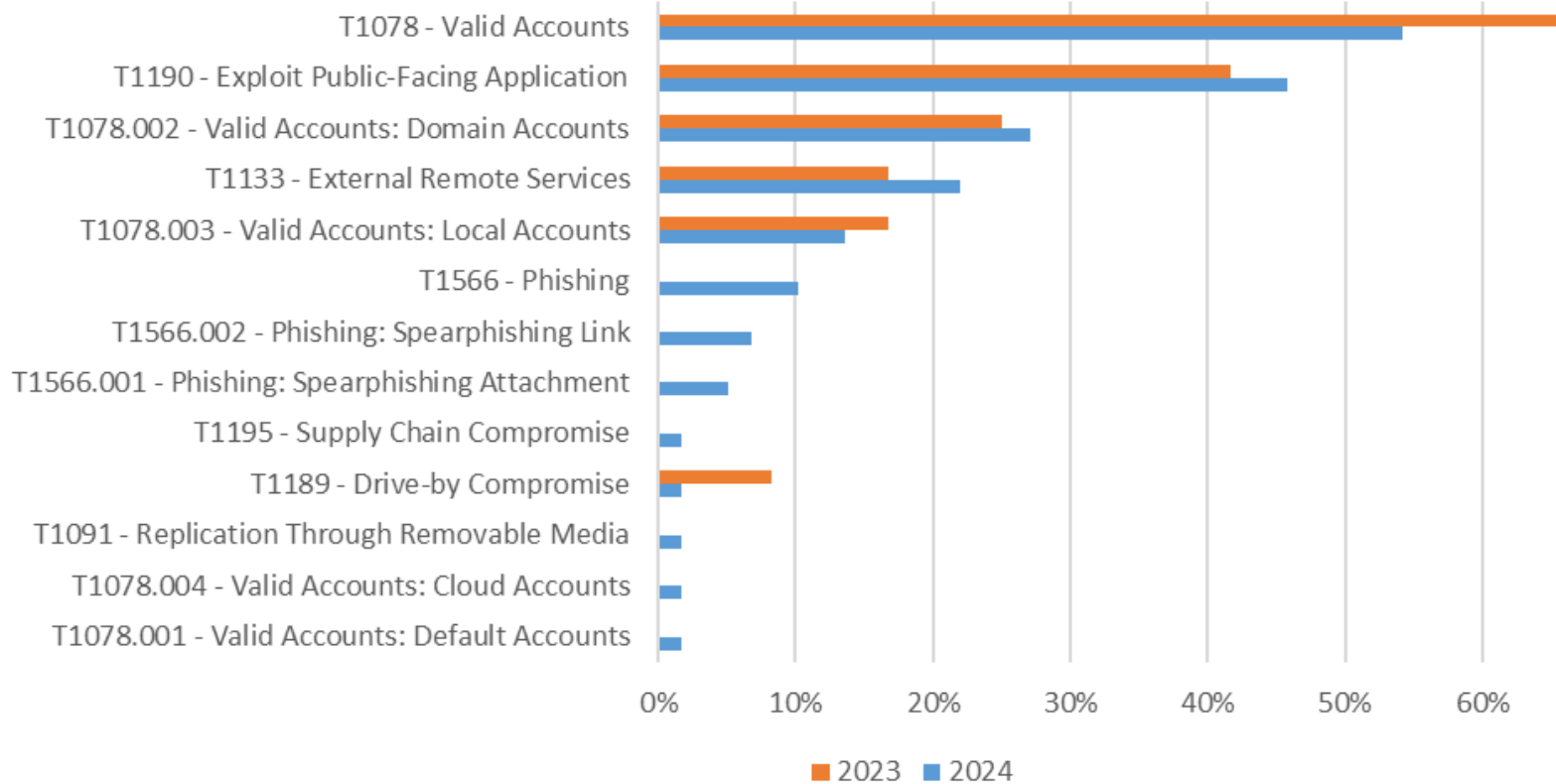




Insights – Tactics, Techniques and Procedures

FortiGuard Labs Research 2023 - 2024

Observed Initial Access Techniques





The Moving Goalpost?





The Moving Goalpost?



How
do I
Keep Up?



Who
can I
Trust?



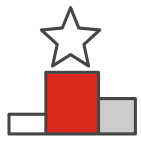
What
can I
Trust?



How
do I build
a Capable
Team?



Which
risks do I
Outsource /
Accept?



Mitigation



Strategies

SCAN ME!



Source:
<https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf>





Useful Resources

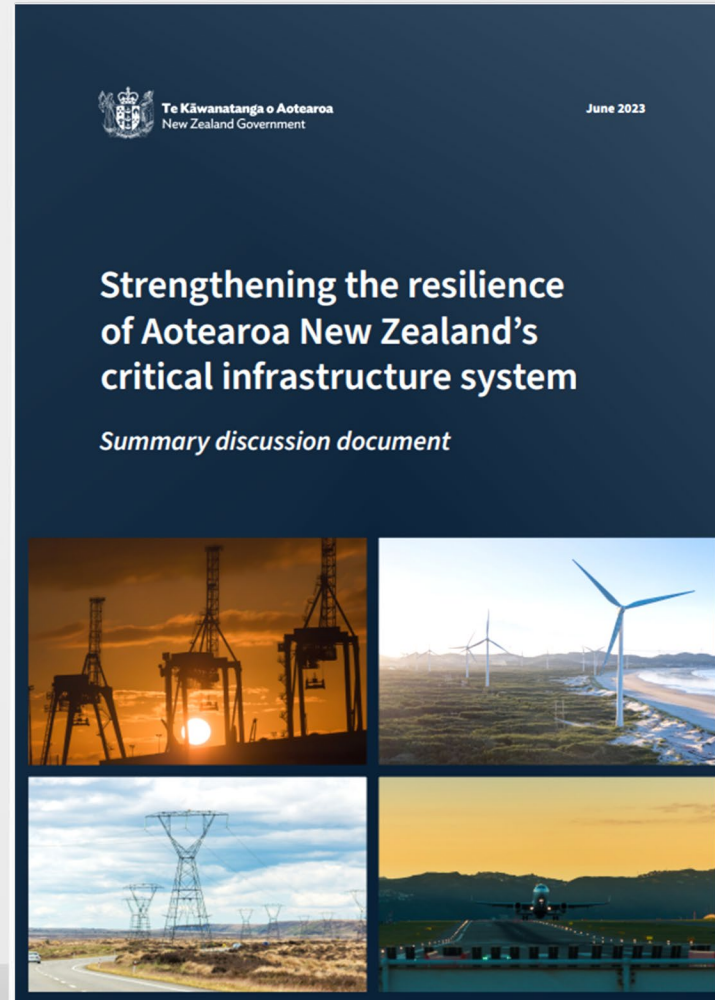




Cybersecurity Focus in NZ

5 million Internet users presents opportunities and risks

Figure 1: Simplified overview of New Zealand's regulatory approach to infrastructure resilience



SCAN ME!



AU Institute of Company Directors - Checklist



Australian Institute of Company Directors

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

SME and NFP Director Checklist

	Document where possible who has responsibility for cyber security
1. Set clear roles and responsibilities	Appoint a cyber champion to promote cyber resilience and respond to questions
	Consider whether a director, or group of directors, should have a more active role in overseeing cyber security
	Collect data where possible on the effectiveness of cyber risk practices
	Utilise the ACSC Cyber Security Assessment Tool to identify the cyber security strengths of the organisation and understand areas for improvement
2. Develop, implement and evolve a comprehensive cyber strategy	Assess whether utilising reputable external providers will enhance cyber resilience over managing in-house
	Assess whether there is certain data (e.g. employee or customer data) that does not need to be collected
	Establish an Access Control System to determine who should have access to what
	Regularly repeat cyber security training and awareness amongst all employees
	Promote strong email hygiene
	Patch and update applications and anti-virus software
3. Embed cyber security in existing risk management practices	Configure Microsoft Office macro settings (e.g. only macros from trusted locations enabled)
	User application hardening - limit interaction between internet applications and business systems
	Limit or restrict access to social media and external email accounts
	Restrict use of USBs or external hard drives
	Restrict operating system and software administrative privileges
	Implement multi-factor authentication
	Maintain offline backups of key data
	Ensure that departing employees or volunteers no longer have access to systems and passwords

1

Key Takeaways:

- Clear **Roles & Responsibilities**
- Develop a **Comprehensive Cyber Strategy**
- Embed Cybersecurity in **Business Risk Management Practices**



FortiGuard Outbreak Alerts

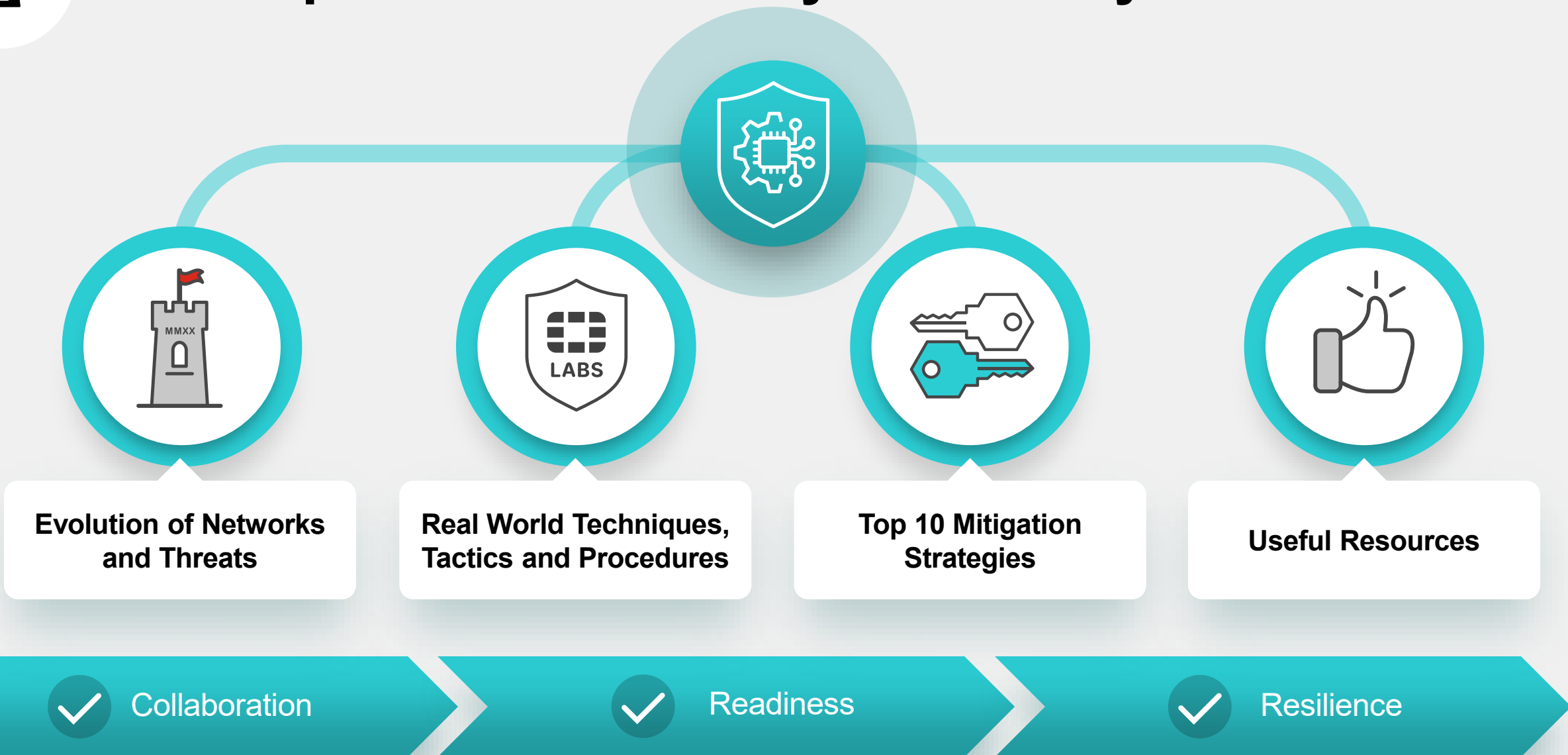
Subscribe today

Keep up to date with all the latest outbreaks by subscribing to FortiGuard Outbreak Alerts today!





A Recap of Business & Cybersecurity Risk



The background features a grid of dark gray squares and semi-circles. A red horizontal bar is at the top left. Another red horizontal bar is positioned above the 'O' in 'FORTINET'. A red horizontal bar is at the bottom left. In the bottom right, there is a grid of small white dots and a vertical gray bar.

FORTINET