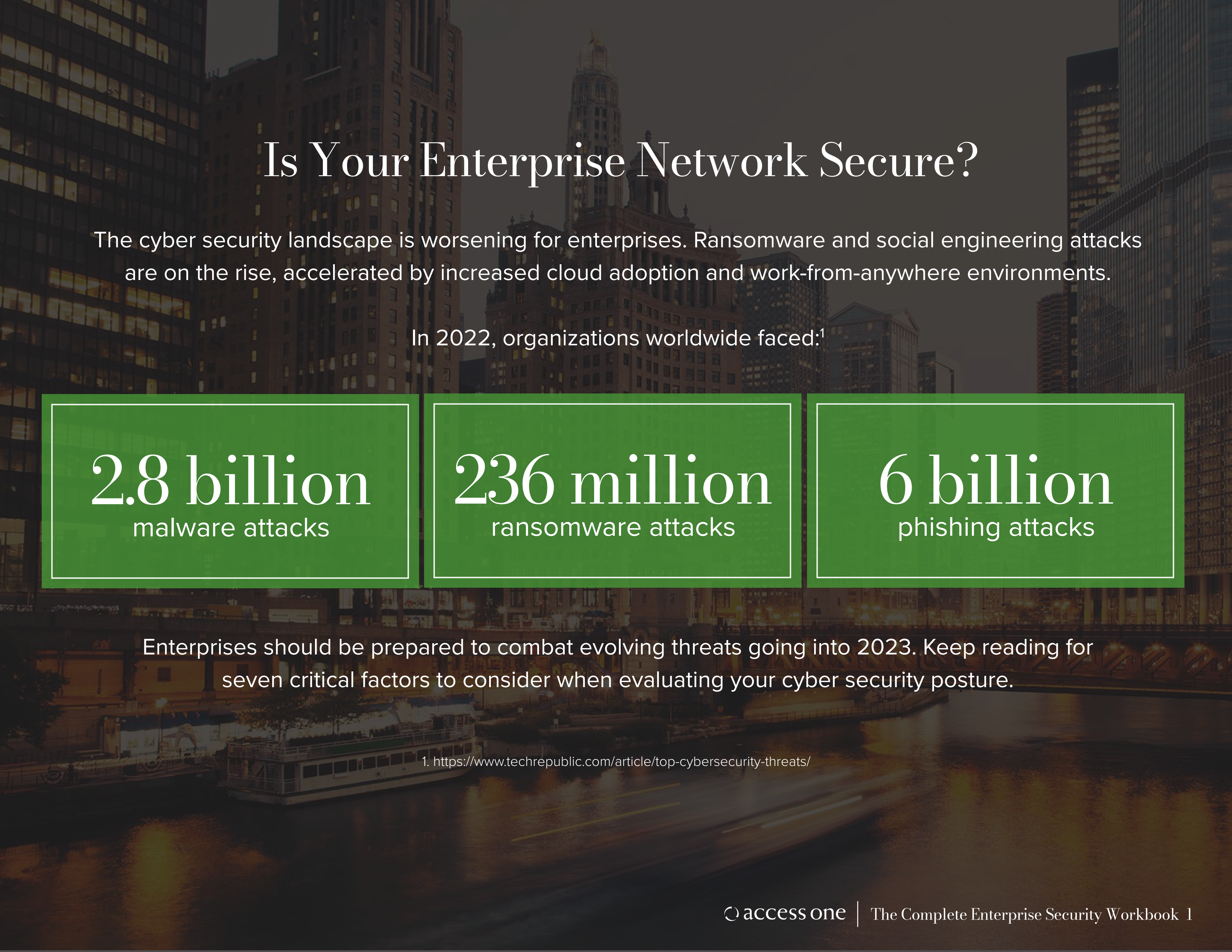
The Complete Enterprise Security Workbook

Strengthen Your Cyber Security Posture in 2023

access one

Table of Contents



Is Your Enterprise Network Secure?

The cyber security landscape is worsening for enterprises. Ransomware and social engineering attacks are on the rise, accelerated by increased cloud adoption and work-from-anywhere environments.

In 2022, organizations worldwide faced:[1]

2.8 billion
malware attacks

236 million
ransomware attacks

6 billion
phishing attacks

Enterprises should be prepared to combat evolving threats going into 2023. Keep reading for seven critical factors to consider when evaluating your cyber security posture.

[1] https://www.techrepublic.com/article/top-cybersecurity-threats/

Have You Implemented Measures To Protect Remote Workers?

Businesses embracing remote and hybrid work models face more cyber security risks than ever. Increased reliance on cloud apps and bring-your-own-device (BYOD) policies have resulted in an alarming rise in cyber attacks, with enterprise IT leaders reporting:[2]

56%
more network infections from web browsers.

54%
more attempted phishing attacks.

44%
of company-wide infections originating from personal devices.

Effective cyber security measures are a must if you're hoping to tackle these new vulnerabilities.

[2] https://threatresearch.ext.hp.com/hp-wolf-security-blurred-lines-blindspots-report-risky-remote-working/

Do You Have Early Warning Detection & Disaster Recovery in Place?

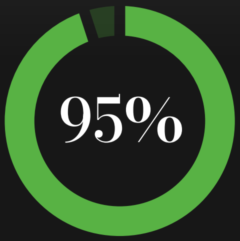
Because enterprise businesses manage massive amounts of sensitive data, detecting threats before they impact your network is critical. Early warning detection helps you quickly identify and contain threats, preventing hackers from wreaking havoc.

Similarly, having a solid disaster recovery strategy is key for preventing downtime and financial loss if disaster strikes. The average cost of a data breach in the U.S. is $9.44 million,[3] so you should consider developing a disaster recovery plan before issues arise.

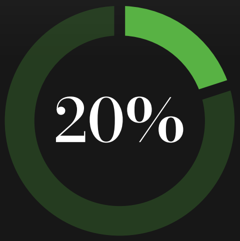
[3] https://www.ibm.com/reports/data-breach

Do You Provide Employees With Security Awareness Training?

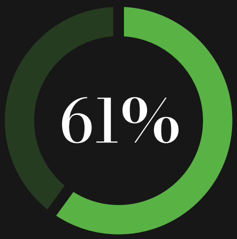
What's the weakest link in any organization's cyber security strategy? Poorly trained employees. Consider these statistics:[4]



of cyber security breaches result from human error.



An estimated **20%** of employees click on links in phishing emails.



of data breaches involve stolen or misused credentials.

Breaches cost **$1.07 million more** when remote work is a factor.

Comprehensive cyber security awareness training is essential for ensuring your employees can spot and avoid cyber threats.

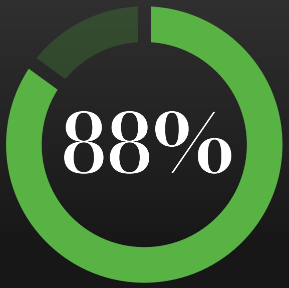
[4] https://www.cybertalk.org/2021/12/02/alarming-cyber-security-facts-to-know-for-2021-and-beyond/

Are You Using Real-Time Threat Detection Tools Effectively?

Cyber threats don't stick to traditional business hours. Your cyber security strategy should work 24/7/365, and real-time threat detection can make that happen.

Real-time threat detection refers to the continuous monitoring of company-wide network activity and system endpoints to help organizations prevent, identify, and respond to cyber threats at all times. By combining AI-powered threat detection with human intelligence and analysis, you can rest easy knowing your network is always safe.

Have You Implemented Physical Security Measures?



of business leaders have seen an increase in physical threat activity.[5]

Unmanaged physical threats can impact your IT team's ability to identify and combat cyber security threats, but joining your physical and cyber security services can help you:

- ✓ Prevent hackers from using physical security devices for attacks.
- ✓ Protect data accessed via poorly secured WiFi networks or IoT devices.
- ✓ Mitigate workplace violence masked by compromised security systems.
- ✓ Prevent hackers from introducing malware on physical equipment.

[5] https://ontic.co/wp-content/uploads/2022/01/2022-Ontic-State-of-Protective-Intelligence-Report.pdf

Do You Use Encryption To Help Prevent Data Breaches?

Enterprise businesses need to be proactive – not reactive – when it comes to cyber security. Encryption can help you thwart data breach attempts by converting plain text into an unreadable format so that any hacker who steals communications from your network can't gain access to confidential information.

By using encryption properly, you can protect your company's privacy, your employees' confidential information, and even your reputation.

Have You Completed a Risk Assessment?

Knowing your network risks is the first step toward building a smarter, more strategic cyber security strategy. Risk assessments can help you identify any vulnerabilities in your network and provide actionable tips to improve your company's cyber security posture.

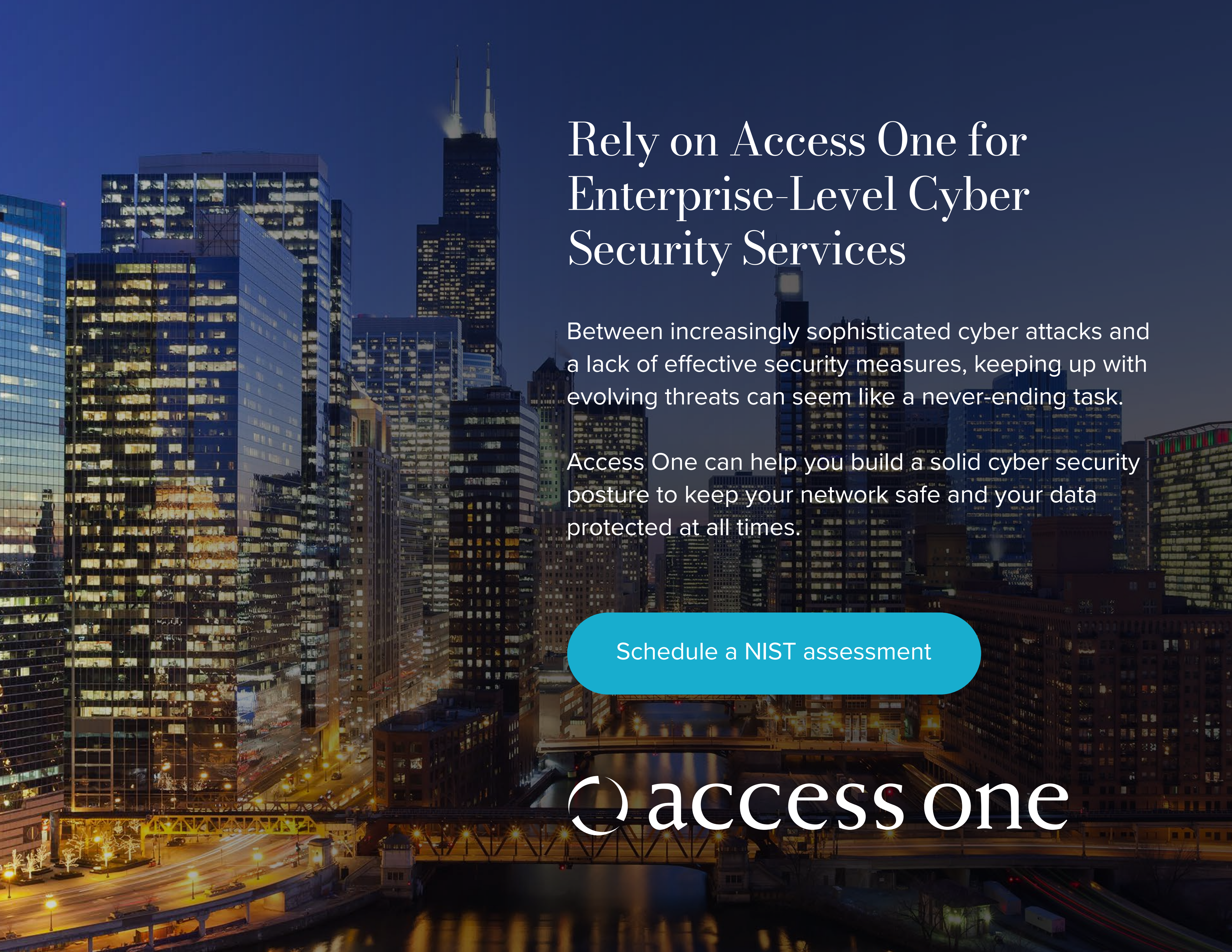
Ongoing risk assessments conducted by an expert in enterprise-level cyber security will help you uncover, protect, and fix vulnerabilities continuously.

Secure Your Enterprise With a NIST Assessment

Strengthen your security with a NIST risk assessment from Access One. We use powerful tools to analyze your devices, networks, and more and identify any vulnerabilities.

Here's what you get from an assessment:

- A network risk report to help you understand your level of vulnerability.
- A network management plan that lists vulnerable areas and remedies.
- An external vulnerability scan report based on a scan of 65,535 ports.
- A Microsoft cloud assessment that identifies risks in your cloud applications.



Rely on Access One for Enterprise-Level Cyber Security Services

Between increasingly sophisticated cyber attacks and a lack of effective security measures, keeping up with evolving threats can seem like a never-ending task.

Access One can help you build a solid cyber security posture to keep your network safe and your data protected at all times.

Schedule a NIST assessment

access one