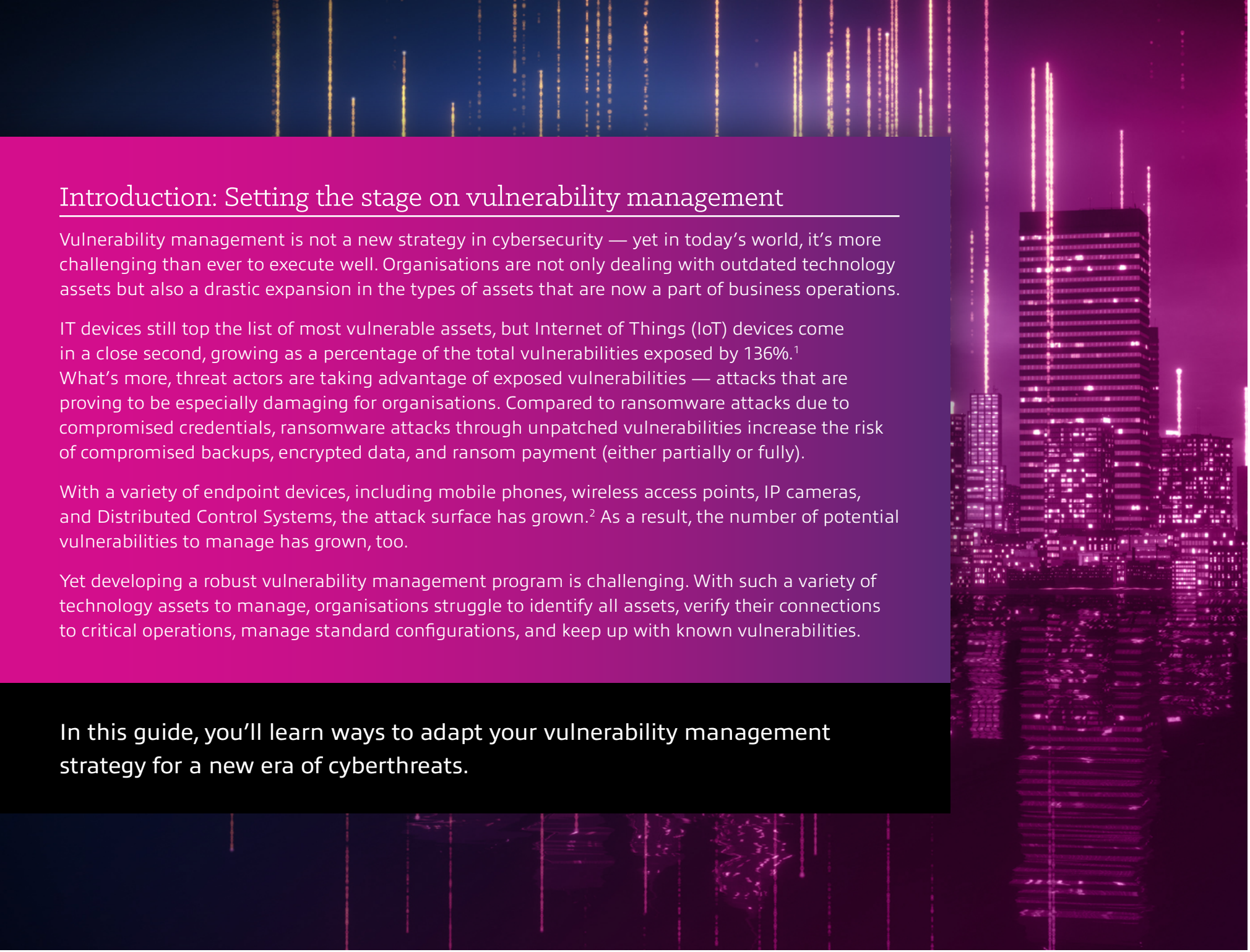
Beyond the Critical: Redefining Vulnerability Management

How advanced technologies & architecture can improve enterprise security

Insight®



Introduction: Setting the stage on vulnerability management

Vulnerability management is not a new strategy in cybersecurity — yet in today's world, it's more challenging than ever to execute well. Organisations are not only dealing with outdated technology assets but also a drastic expansion in the types of assets that are now a part of business operations.

IT devices still top the list of most vulnerable assets, but Internet of Things (IoT) devices come in a close second, growing as a percentage of the total vulnerabilities exposed by 136%.[1] What's more, threat actors are taking advantage of exposed vulnerabilities — attacks that are proving to be especially damaging for organisations. Compared to ransomware attacks due to compromised credentials, ransomware attacks through unpatched vulnerabilities increase the risk of compromised backups, encrypted data, and ransom payment (either partially or fully).

With a variety of endpoint devices, including mobile phones, wireless access points, IP cameras, and Distributed Control Systems, the attack surface has grown.[2] As a result, the number of potential vulnerabilities to manage has grown, too.

Yet developing a robust vulnerability management program is challenging. With such a variety of technology assets to manage, organisations struggle to identify all assets, verify their connections to critical operations, manage standard configurations, and keep up with known vulnerabilities.

In this guide, you'll learn ways to adapt your vulnerability management strategy for a new era of cyberthreats.

Risks of poor vulnerability management

Protecting anything of value — whether it resides in a home or a business — requires securing any entry point that might be exploited by a criminal. This is the essence of vulnerability management. Imagine a band of robbers walking through a neighborhood and checking every single door for the one that's unlocked.

When devices and other assets go unpatched, unmanaged, or even unknown, an easy entry point for hackers emerges to access your environment.

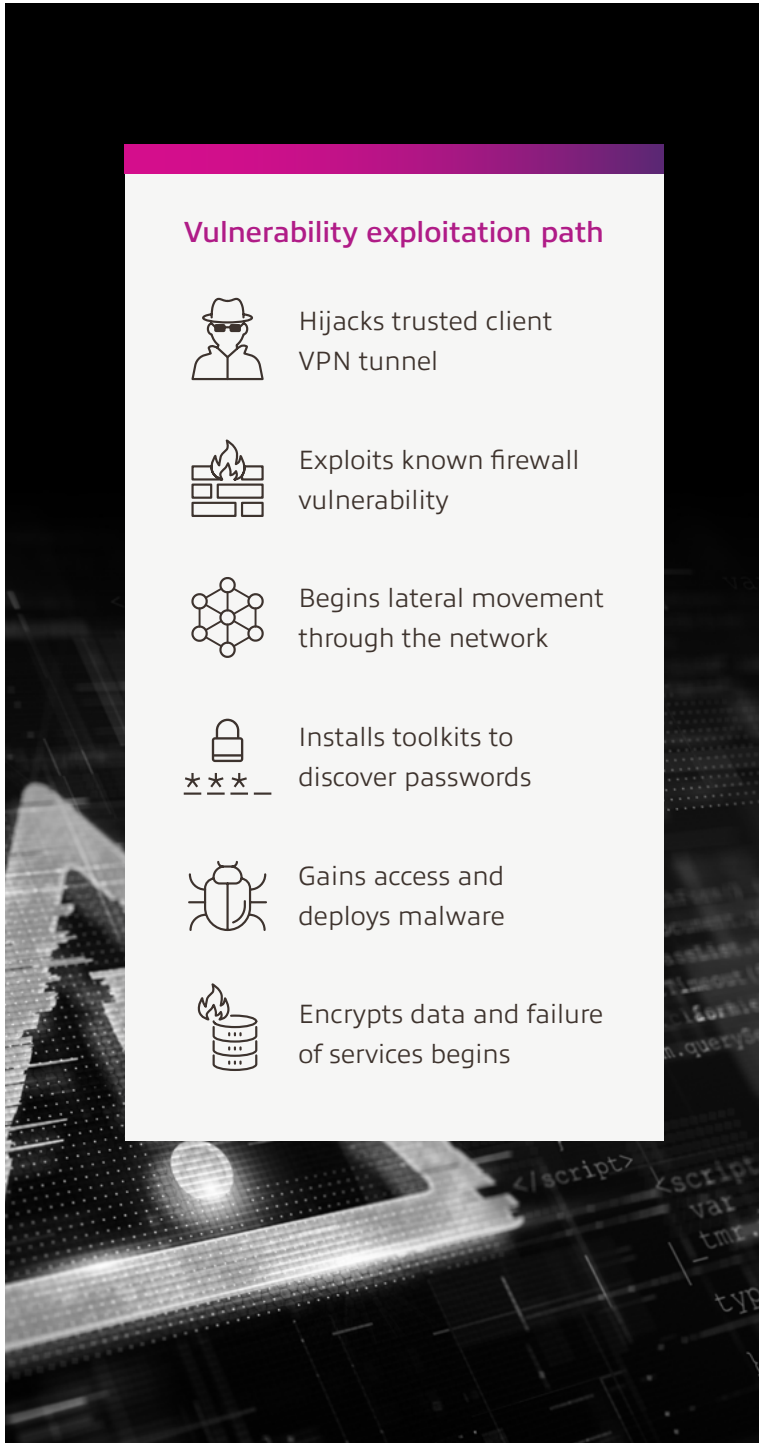
Over the years, unpatched systems consistently make up a third of all initial attack vectors and provide an easy avenue of entry into an organisation.[3]

Attackers often rely on automated scanning to discover unpatched systems. They target web applications, public-facing applications, network devices, remote access services, and VPN provider software.

Once an attacker identifies a vulnerability, this can lead to:

- Ransomware attacks
- System outages
- Data loss
- Denial of service
- Increased cost of recovery

Not only was vulnerability exploitation the most common way for attackers to gain initial access in 2023, these attacks also had more severe outcomes than those based on compromised credentials.[4]



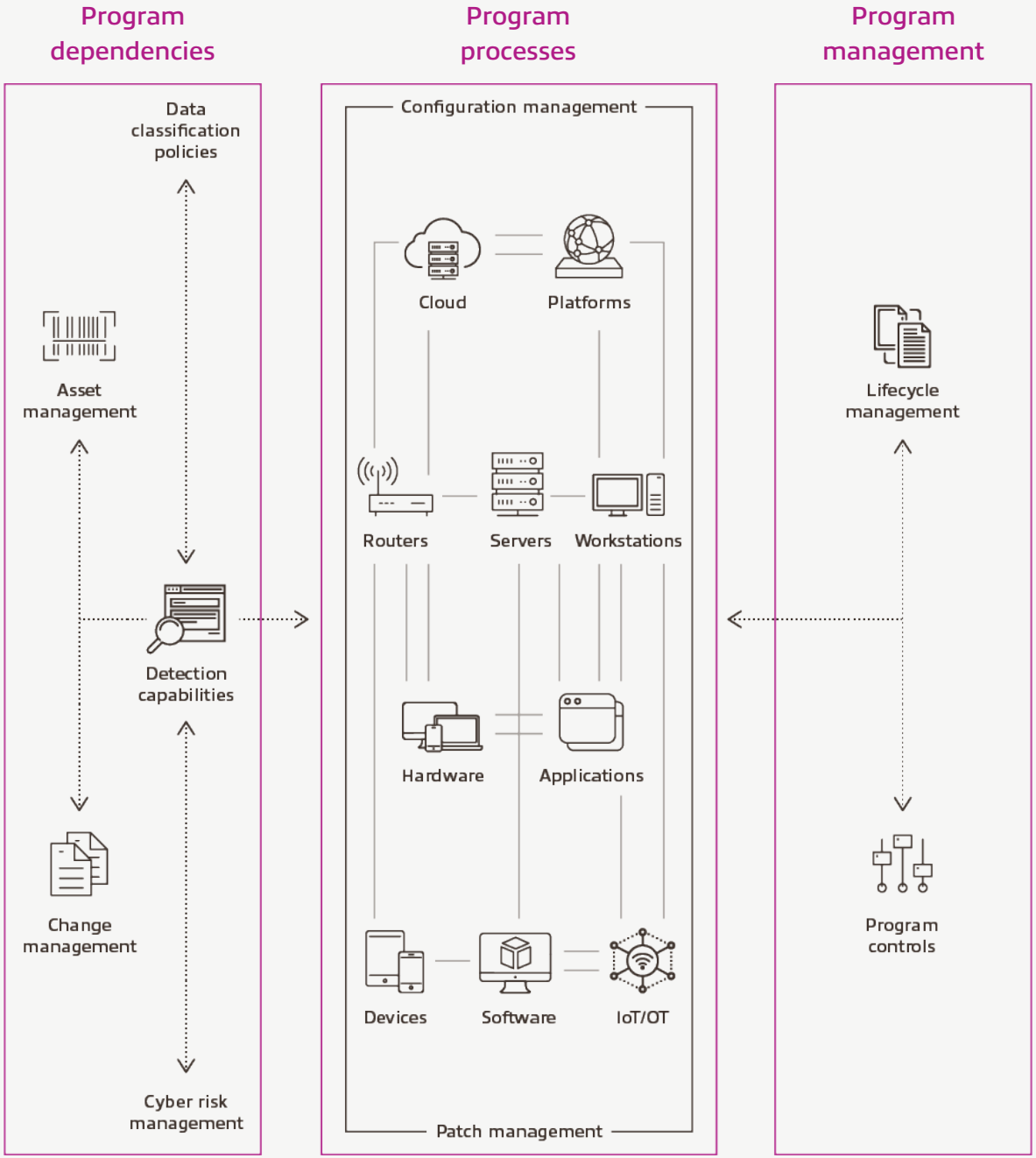
Enter: A modern vulnerability management program

To mitigate threats, a sound program architecture for managing vulnerabilities is key. There are three pillars for success to consider:

- **Program dependencies** such as asset management and data classification policies are often overlooked but are key components of the full vulnerability management program, establishing policies and capabilities.
- **Program processes**, including configuration management and patch management, provide configuration and vulnerability patch baseline policies, procedures, audits, and remediation activities.
- **Program management** measures and supports program effectiveness, governance, and adoption through lifecycle management and program controls.

80%–90%

of all successful ransomware compromises originate through unmanaged devices.[5]



How vulnerability management is evolving: The latest advances

Fortunately, technology advances have ushered in built-in capabilities that streamline the process to capture technology assets (along with relevant asset details), identify misconfigurations and vulnerabilities, and provide automated responses or recommendations for remediation.

Attack Surface Management (ASM)

ASM provides visibility across all assets and monitors threat vectors associated with each type of asset from the attacker's view. ASM tools can automate the process of asset discovery and classification, vulnerability scanning, threat modeling, and risk prioritisation across platforms such as multicloud environments. Tools including **Microsoft® Defender, CrowdStrike® Falcon Surface®**, and **Tenable® One** provide ASM functionality.

Continuous Threat Exposure Management (CTEM) and Risk-Based Vulnerability Management (RBVM)

CTEM and RBVM are new approaches to vulnerability management that integrate threat exposure and risk prioritisation. CTEM uses threat intelligence feeds and continuous scanning to pinpoint vulnerabilities, while RBVM uses multiple data points such as risk and exposure prioritisation to focus on the riskiest assets and the potential business impact. RBVM helps security teams prioritise assets with the greatest risk exposure instead of having to patch all vulnerable assets.

Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR)

SIEM and SOAR technologies use AI to track and automate the remediation process. SOAR can provide automated responses or recommendations for misconfigured assets or known vulnerabilities. Advances in AI can help detect, prioritise, and automate patching of vulnerable systems. Products like **Qualys TruRisk™ AI** are showing promise in delivering predictive, automated, and autonomous vulnerability management solutions.

Why risk-based vulnerability management?

RBVM is a proactive and focused approach to assess and reduce the risk of vulnerabilities in your assets, using machine learning and threat intelligence. It works to assess threat context and business impact.

RBVM helps you reduce risk by focusing on the most critical vulnerabilities, optimise resources by automating tasks, and improve visibility by assessing both traditional and modern assets.

By using CISA Known Exploited Vulnerabilities (KEV) catalog and Exploit Prediction Scoring System (EPSS), teams can focus on vulnerabilities that are known to be exploited in the wild — and prioritise those with a high likelihood of exploitation.

Steps to consider

While vulnerability management should be a proactive approach to preventing cybersecurity attacks, equally important is strengthening cybersecurity posture to minimise the impact of a threat, and to be prepared in the event of a breach.

1

A critical first step is to review your asset management process and policies — and identify your prioritised business assets. Unknown assets cannot be protected and may be an entry point for attackers to gain access to sensitive data or critical systems.

2

Gain an understanding of the vulnerabilities in your environment. Run a vulnerability scan (ideally, this is something that is done continuously). This will provide you with the number of critical vulnerabilities in your identified technology assets.

3

Given the number of critical vulnerabilities that arise on an almost daily basis, strengthening your security posture with a Zero Trust architecture is a crucial step. Following a "never trust, always verify" approach to security has been shown to help minimise the impact of a breach.

4

Ensure you have a plan in the event of a disaster, including internal and external communications, internal resources, and backup-restore processes. Review, update, and test your recovery plan, ensuring key stakeholders understand their roles and responsibilities.

About Insight

Insight Enterprises, Inc., is a Fortune 500 Solutions Integrator with 13,000 teammates worldwide helping organisations accelerate their digital journey to modernise their business and maximise the value of technology. We enable secure end-to-end transformation and meet the needs of our clients through a comprehensive portfolio of solutions, far-reaching partnerships and 35 years of broad IT expertise. Rated as a Forbes World's Best Employer and certified as a Great Place to Work, we amplify our solutions and services with global scale, local expertise and a world-class eCommerce experience, realising the digital ambitions of our clients at every opportunity.

Insight®

1800 189 888
au.insight.com

0800 933 111
nz.insight.com

65 6438 2995
sg.insight.com

852 2972 8200
hk.insight.com

Sources:

[1]Forescout Research. (2024, June 10). The Riskiest Connected Devices in 2024.

[2]Sophos. (April 2024). Unpatched Vulnerabilities: The Most Brutal Ransomware Attack Vector.

[3]Ibid.

[4]Ibid.

[5]Microsoft. (October 2023). Microsoft Digital Defense Report 2023: Building and improving cyber resilience.