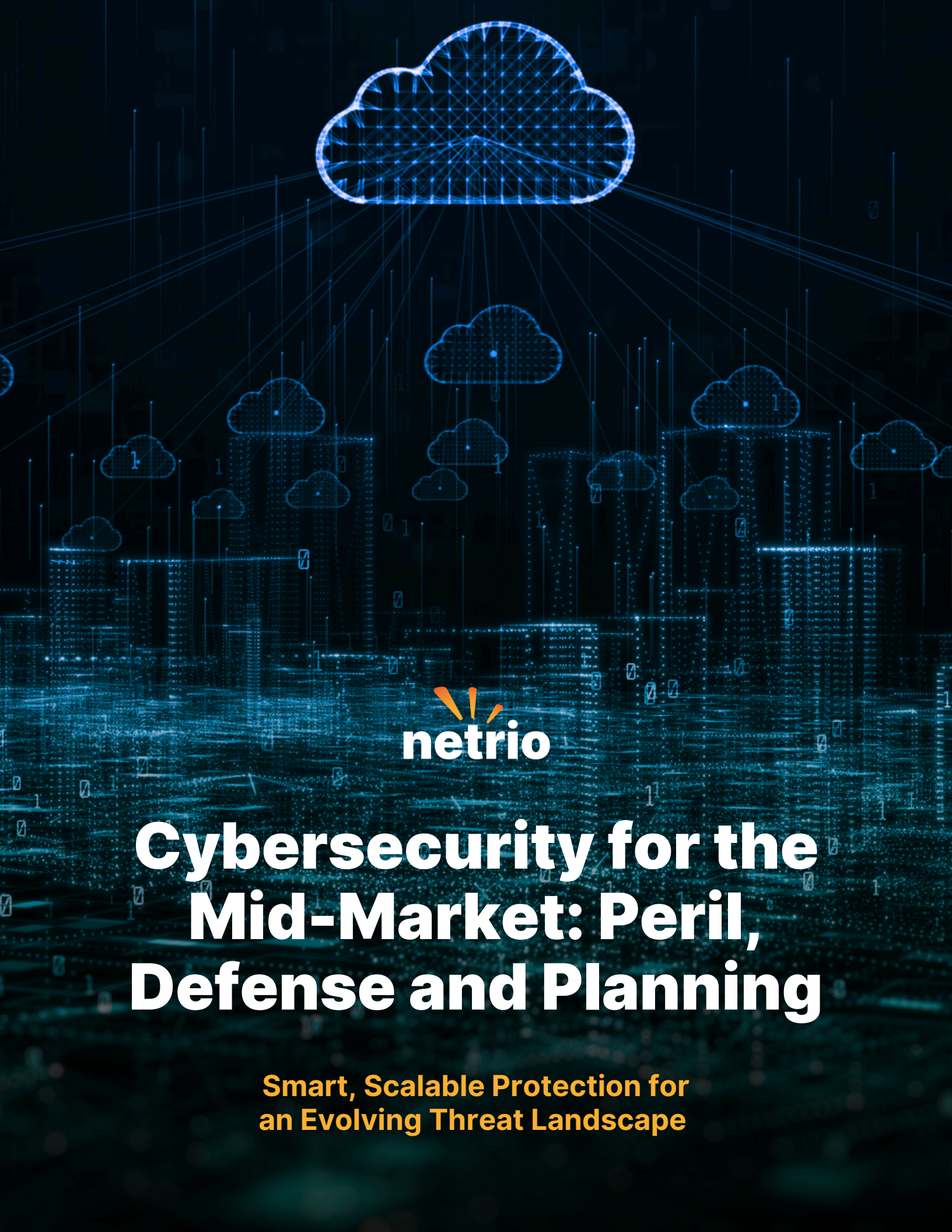


netrio

Cybersecurity for the Mid-Market: Peril, Defense and Planning

Smart, Scalable Protection for an Evolving Threat Landscape

Table of Contents

Introduction 3

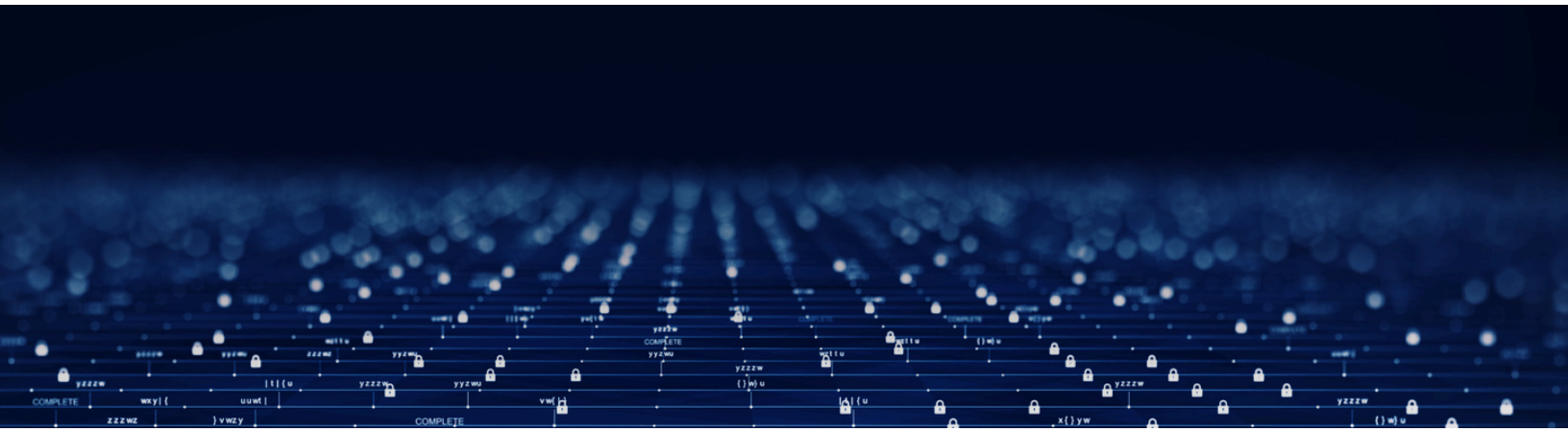
Shifting Threats and Evolving Cybersecurity Needs 4

Common Vulnerabilities Among Small and Mid-Sized Businesses 5

Affordable, Effective Strategies for Stronger Cyber Defense 7

The Role of a Managed Service Provider like Netrio 9

Is Your Business Secure? A Checklist 10



No business wants to imagine it: the moment you've feared has finally come. It started with an email from one of your vendors, a trusted partner, with an attachment an unwitting employee opened. Unfortunately, your business isn't equipped with multi-factor authentication (MFA) or an incident response plan, and your thinly spread IT team has been dealing with an onslaught of patching and updates.

Now your system is down. For days. Aside from lost revenue, you've had to shell out thousands to recover from the cyber breach. Not to mention potential reputational fallout. And the problem? Today's attackers don't require CIA-grade, tried-and-true tools. They just need little oversights in your system to allow them in.

To avoid the above scenario, it's important to consider that the breakneck pace of technological change can leave companies, often small- and mid-market enterprises, less equipped with the latest tools, from AI companions to top-notch security defenses. Systems are dating more quickly, allowing cybercriminals easier workarounds to penetrate lacking defenses.

And small and mid-sized businesses are prime targets. Why? Because without the deep pockets of large enterprises and the abundance of human capital to unleash on a cyberthreat, many small and mid-sized businesses have their hands tied. And many are waiting for the shoe to drop.

At Netrio, We've Got This.

Our solutions, from SOC-as-a-Service, Endpoint Detection and Response, and Rapid Incident Response, are tailored to meet evolving threats head-on.

We take an approach tailored to your business, bolstering your defenses to ensure smooth sailing—so you can focus on what you do best, and we can focus on stopping cybercriminals. Our goal is to help organizations manage and secure their technology environment. We offer a unique combination of in-house solutions, experienced executives, and extensive networking, cloud, and comprehensive managed services.

In this eBook, we'll explore the shifting sands of cyberthreats and how your small or mid-sized business can prepare for the worst to keep doing your best.

Shifting Threats and Evolving Cybersecurity Needs

The world of cyberthreats evolves alongside technological advancements, meaning your business's defenses need to upgrade just as quickly. Because mid-market enterprises live in the "sweet spot" for attackers (valuable enough to hold sensitive data but under-resourced in cybersecurity), they are often the victims of cyberthreats. With many lacking a full-time security team or formal response plan, they're easier prey for phishing, ransomware, and supply chain compromise.

Sophisticated Phishing and Ransomware-as-a-Service (RaaS)

Phishing has been and remains the most common access point for attackers, comprising 36% of system breaches. Meanwhile, Ransomware-as-a-Service (RaaS) has risen in popularity as a cybercrime business model, effectively democratizing ransomware and lowering the technical bar for launching devastating attacks. If the services are purchased, operators can build software for their clients to breach a business's system.

Supply Chain Attacks & Remote Work Vulnerabilities

Small and mid-sized businesses that work with larger supply chains are now part of the domino fall of targets that negative actors are seeking to compromise. By breaching such businesses' security defenses, cybercriminals are able to disrupt larger supply chain networks.

Additionally, with remote work, the attack surface has widened, from personal devices to unsecured home networks and cloud misconfiguration continuing to pose risks and provide challenges to mid-market enterprises with employees around the country or the globe.

At Netrio, we understand that your cybersecurity strategy must evolve as your digital environment expands. Our services secure the modern attack surfaces that many mid-market companies now rely on, such as cloud-based platforms, IoT devices, mobile endpoints, and hybrid infrastructure. These vectors can present significant risks if unmanaged. Netrio's layered defenses turn those vulnerabilities into strengths.

Regulatory Pressures and Compliance

Whether governed by HIPAA, PCI-DSS, SOX, or state-level laws such as California's CPRA, regulatory bodies are tightening boundaries. Fines for non-compliance can exceed hundreds of thousands of dollars—often enough to cripple a small- or mid-market enterprise's financial standing. Staying up to date with regulations helps to keep your business compliant and secure.

Common Vulnerabilities Among Small and Mid-Sized Businesses

Both small and mid-sized businesses suffer from similar vulnerabilities that can create and leave open gaps in their cybersecurity efforts, such as:

1 Lack of Dedicated Security Resources:

Many SMBs function with either dedicated security staff or a small, overworked team and a strapped budget. According to a CrowdStrike survey, only 7% of SMBs believe their budget for cybersecurity is sufficient, leaving the vast majority underserved.

2 Poor Visibility into Devices & Endpoints

Without centralized visibility, IT teams aren't able to detect rogue devices or early warning signs of compromise. As with any potential cyber issue, being on top of it before it occurs is key. Without strong visibility, issues can fall through the cracks. Such problems can be exacerbated when SMBs operate in hybrid or remote setups.

3 Unpatched or Legacy Systems

According to the Cybersecurity & Infrastructure Security Agency (CISA), many successful breaches exploit *known vulnerabilities* for which patches already exist. Ofttimes, due to lean IT teams and budget constraints, SMBs aren't up to date to fix potentially compromising issues in their legacy systems.

4 Weak Access Management

Weak or reused passwords, a lack of multi-factor authentication (MFA), and stale credentials are major culprits in system breaches. In general, reusing passwords or letting previous credentials sit, go unused, and never be updated provides leverage for attackers to gain access to multiple accounts, giving them the opportunity to breach deeper into systems.

5 No Incident Response Plan

According to the Ponemon Institute, many small- and mid-market enterprises do not have a formal incident response plan to combat potential cybersecurity compromises. Without clear roles and procedures in place, response times lengthen, allowing cybercriminals prolonged access to a business's systems and ballooning potential recovery costs.

Affordable, Effective Strategies for Stronger Cyber Defense

Zero Trust Architecture

Zero Trust Architecture (ZTA) isn't only a solution for large enterprises. Its core principles, such as continuous authentication and least privilege access, can be implemented using existing tools. Microsoft reports that companies that adopt ZTA reduce the average impact of breaches by 50%.

24/7 Threat Monitoring & Detection (SOC-as-a-Service)

Outsourced security operations centers (SOCs) offer round-the-clock monitoring without requiring internal headcount. Netrio's SOC-as-a-Service delivers real-time threat monitoring and escalation without the cost of a fully staffed in-house SOC.

Managed Detection and Response (MDR)

Beyond monitoring, many small- and mid-sized businesses benefit from deeper security operations integration, such as Managed Detection and Response (MDR), which provides expert-led monitoring and threat response. This service combines cutting-edge technology with experienced analysts to proactively detect, investigate, and remediate threats before they cause lasting damage. MDR ensures that your systems are always under a watchful, skilled eye, 24/7/365.

Extended Detection and Response (XDR)

As the number of tools and attack vectors increases, it becomes difficult for small- and mid-sized businesses to manage threat intelligence across disparate systems. Extended Detection and Response (XDR) brings together security data from endpoints, servers, email, cloud services, and networks into one unified view, allowing for streamlined detection and enabling faster, more accurate incident response.

Employee Training and Phishing Simulations

Human error remains a leading access point for attackers, according to IBM. Regular employee training reduces phishing click rates, helping users to understand potentially harmful emails and bad-acting attempts to access your system. Keeping your employees up to date helps them stay vigilant and exercise caution.

Multi-Factor Authentication (MFA) and Access Controls

Implementing MFA can block over 99.9% of credential-based attacks, according to Microsoft (2019). Layered access, particularly for administrative accounts and sensitive data, is essential in bolstering defenses.

Regular Patching, Updates, and Backups

Automated patch management tools reduce the burden on overworked IT teams while addressing vulnerabilities. The Cybersecurity & Infrastructure Security Agency (CISA) emphasizes that most exploited vulnerabilities are already known and patchable.

Disaster Recovery and Business Continuity Planning

Cybersecurity isn't simply about prevention; it's also about resilience. Although reinforcing all forms of cybersecurity to protect your systems is crucial, having a plan in case of a breach is also necessary. Most hackers lack the skills to break into sophisticated cybersecurity systems. Still, it does happen. In the event that your organization were to suffer a sustained breach, a clear recovery plan, supported by tested backups, can slash downtime from days or weeks to hours.

The Role of a Managed Service Provider like Netrio

Many businesses, and most small- and mid-market organizations, attempt to cobble together solutions and rely on overloaded IT teams, but that approach isn't sustainable. Cyber threats evolve too quickly for part-time attention.

The role of an MSP like Netrio is to provide full-time, round-the-clock attention to your organization's cyber defenses. Benefits of such a close, tailored partnership include:

- Access to top-tier security tools without large enterprise pricing
- Dedicated expertise
- 24/7/365 support
- Faster detection and response
- Simplified compliance and reporting
- Scalable services that grow alongside your organization

Is Your Business Secure? A Checklist:

We know that each business's cybersecurity standing is unique, and that where you want to be depends on where you're starting. At Netrio, We've Got This, and we'll start by asking you:

- [ ] Do you use MFA for email, VPNs, and admin accounts?
- [ ] Is patching automated and applied regularly across all systems?
- [ ] Do you conduct employee training and phishing simulations monthly, quarterly, yearly, etc.?
- [ ] Are backups isolated, encrypted, and tested? If so, how often?
- [ ] Do you have Endpoint Detection and Response (EDR) tools deployed and monitored 24/7?
- [ ] Are vendors and third-party tools reviewed for security risks?
- [ ] Is your disaster recovery plan documented and tested?
- [ ] Do you follow least privilege access principles?
- [ ] Have you conducted a cybersecurity risk assessment in the last 12 months?

We've Got This.

Ready to strengthen your security today to prepare for the threats of tomorrow?

Those who partner with us know that We've Got This, that we're the go-to for cybersecurity needs, and that we meet our partners where they are to take them where they want to be.

Interested in learning more? Reach out today to secure your organization so the business can thrive.