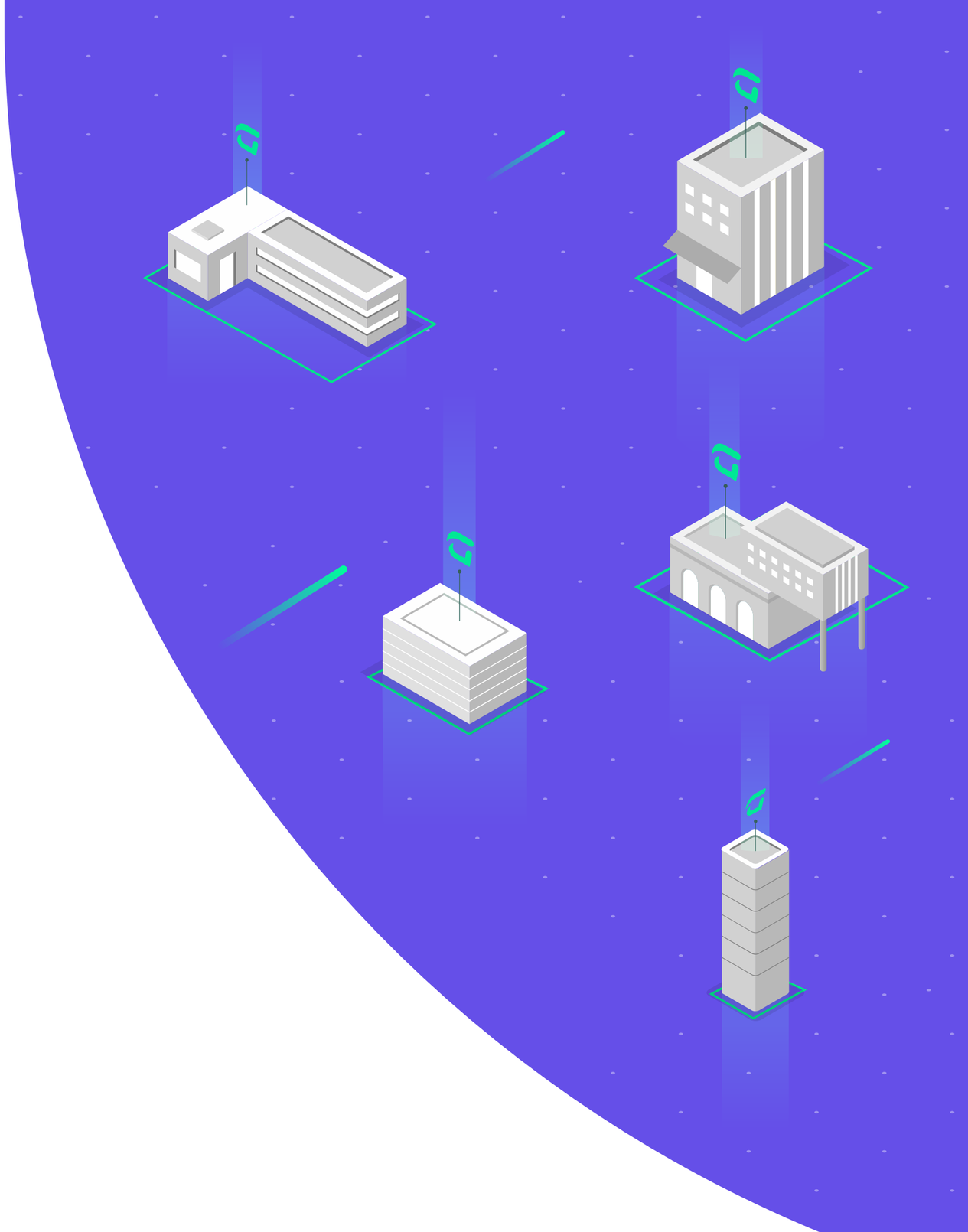
Guardz.



Mastering Cybersecurity to Drive MSP Growth.

Agenda

Chapter 1 | The Traditional Security Stack

- Understanding the Siloed Nature of Point Solutions
- Issues Arising from Disconnected Security Measures
- MSPs Diving into Cybersecurity

Chapter 2 | How Enterprises Address Security Issues

- How Enterprises Address Security Issues
- Understanding MSPs Limitations
- Key Principles for Bridging the Cyber Gap

Chapter 3 | Understanding the New Cybersecurity Landscape

- The Evolving Attack Landscape
- The Expansion of Threat Landscapes and the Escalating Hacker Toolkit
- Emerging Threats: Beyond Ransomware and Phishing

Chapter 4 | It's All About Consolidation

- The Depth of protection against Multi-Vector Attacks: Following Enterprise Trends
- The Unique Relationship Between MSPs and Business Owners: Why Traditional Security Tools Fall Short
- Best Practices for Security Stack Consolidation

Chapter 5 | A Data-Driven Approach to Improve Cyber Risk

- Solid Security and Eligibility for Risk Transfer to Insurance Carriers
- The Importance of Cyber Insurance and its Role in Driving Small Business Success
- Insursec and the Importance of Knowing Your Risks in Real-Time

Chapter 6 | Level Up Your Cybersecurity Game with AI

- Meet Guardz: The Power of One Cybersecurity Platform for MSPs
- What Sets Guardz Apart
- Guardz Key Benefits for MSPs
- What MSPs are saying about Guardz

Chapter 1

The Traditional Security Stack

Understanding the Siloed Nature of Point Solutions

The acceleration of digital transformation in recent years has led to a rapidly evolving digital landscape, making robust security measures more critical than ever. Consequently, MSPs face an ongoing challenge to safeguard their clients' networks and data against diverse threats.

A traditional security stack is often the first line of defense for many MSPs, but this approach has several limitations.

The siloed nature of a traditional security stack can be attributed to the fact that individual security technologies have been developed independently over time. Each technology was built to address a specific issue, such as email protection, data loss prevention, antivirus software, and awareness tools, so they do not communicate or collaborate effectively.

As the collection of disjointed solutions continues to grow, it becomes increasingly unsustainable for security personnel to switch between multiple threat defense tools, leaving room for vulnerabilities to slip through the cracks.

Issues Arising from Disconnected Security Measures

Limited visibility

MSPs cannot get a clear picture of their client's overall security posture when the various technologies in the stack do not share information.

Inefficient response times

Lacking integration between security measures, MSPs may struggle to quickly identify and respond to threats, thus increasing the risk of a successful cyber attack.

Higher costs

Managing disparate security technologies can be time-consuming and resource-intensive, driving up the cost of managing and maintaining the security stack.

Security teams that operate over 50 tools are 8% **less effective at detecting an attack** and 7% less effective when responding to one.

MSPs Diving into Cybersecurity

Trend: MSPs are moving out of their comfort zones into a more robust security offering that they haven't offered in the past and that customers expect.

As MSPs recognize the limitations of the traditional security stack, they have begun to explore other security measures to protect their clients' data and networks more efficiently. Unfortunately, while device protection and backups are essential components of a robust security strategy, they do not offer the comprehensive protection needed to effectively combat the ever-evolving cyber threats across users, communication channels, SaaS applications, and data in the cloud.

Some MSPs have started adopting additional security measures, such as email security services and Cloud Application best practices. However, while these security measures can help MSPs to provide a more holistic approach to their clients' security, is it enough to reduce the risk of cyber-attacks and safeguard sensitive data?

To address the limitations of the traditional security stack, MSPs need to reconsider their reliance on point solutions. This means moving away from disjointed, siloed security solutions and towards an integrated security platform that addresses the numerous challenges MSPs face. Such a platform can provide the following:

- **Holistic protection, which covers the top attack vectors**
- **Improved visibility and management across multiple clients**
- **Scalable and efficient response times when threats arise**
- **Lower costs in both management and maintenance of the security infrastructure.**

Chapter 2

MSPs and the Small Business Challenge

How Enterprises Address Security Issues

Enterprises have long recognized the limitations of traditional point solutions and the need for a more comprehensive and integrated approach to address today's security challenges. As a result, many have taken the necessary steps toward building their security stacks and investing in advanced security tools like Security Information and Event Management (SIEM).

However, for most MSPs, providing and maintaining similar levels of security for their clients is challenging due to resource limitations and the inherent complexities of these solutions that are not designed for small businesses.

64% of MSPs report having insufficient resources to handle advanced security threats.

Understanding MSPs Limitations

MSPs often face limitations compared to the comprehensive solutions implemented by large enterprises. These limitations can arise from resource constraints, budget limitations, workforce size, and technological complexity. Understanding these limitations is crucial for MSPs to effectively address cybersecurity challenges for their clients.

Resource Constraints

MSPs typically operate with limited resources compared to large enterprises. This includes financial resources, infrastructure capabilities, and personnel. They may not have the same level of funding to invest in cutting-edge cybersecurity tools, infrastructure upgrades, or dedicated security teams. This limitation can impact the scope and depth of cybersecurity solutions that MSPs can offer to their clients.

Budget Limitations

With smaller cybersecurity budgets, SMEs pose a unique challenge for MSPs compared to large enterprises. MSPs must work within budget constraints while delivering effective security measures by finding cost-effective solutions. Prioritizing critical security controls based on SME clients' specific needs is crucial. MSPs could utilize open-source tools, cloud-based security services, or offer bundled security packages to cater to SME budgets and requirements.

Workforce Size

SMEs often lack specialized cybersecurity expertise compared to large enterprises with dedicated IT security teams. MSPs must consider this when designing cybersecurity solutions for SMEs, providing user-friendly, manageable options without demanding significant human resources. Achieving this may involve automation, centralized monitoring, and outsourcing specific security functions to external providers.

Technological Complexity

Large enterprises often have complex IT infrastructures, utilizing advanced security technologies like SOCs and SIEM systems. In contrast, MSPs work with SMEs that have simpler infrastructures. MSPs should offer security solutions tailored to SMEs' specific needs and capabilities, ensuring streamlined, scalable options fitting their infrastructure requirements.

Compliance Requirements

SMEs may face industry-specific compliance obligations like GDPR, HIPAA, or PCI DSS. MSPs must comprehend these requirements, assisting SMEs in meeting them through proper security measures. However, unlike large enterprises with dedicated compliance teams, MSPs may face challenges providing comprehensive compliance support due to limited resources and expertise.

Key Principles for Bridging the Cyber Gap

To create comprehensive cybersecurity solutions for SMEs, MSPs should consider the following six principles

MSPs aim for streamlined, **easy-to-manage security solutions designed for small businesses**, closing the resource gap.

Scalability

Look for security solutions that can quickly scale up or down according to the size and needs of your clients.

Flexibility

Adopt a holistic solution that allows you to tailor your security services to each specific client. Be prepared to understand your small business clients' unique needs and customize your offerings to their specific requirements.

Simplicity

Small businesses often lack the resources and budget.Therefore, leverage solutions that are easy to deploy, manage, and maintain while offering robust protection in a cost-effective way

Educate and Empower

Provide ongoing education and training to SME clients. This can include cybersecurity awareness training, best practices, and regular updates on their business security posture and emerging threats affecting their operation.

Stay Current

Invest in continuous research and development to stay ahead of the ever-evolving cybersecurity landscape. Regularly update your security solutions and processes to ensure optimal protection for your clients.

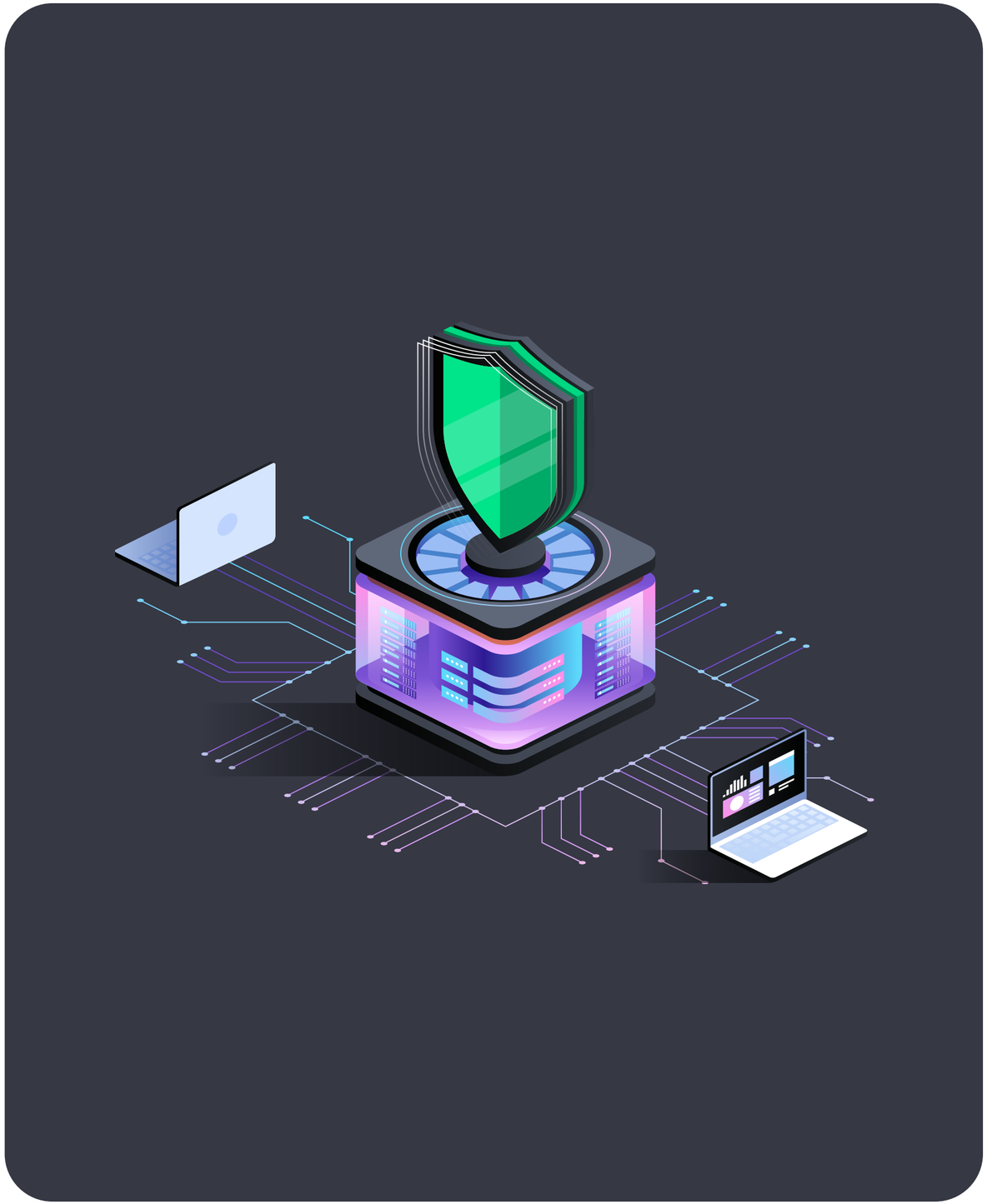
Chapter 3

Understanding the New Cybersecurity Landscape

Understanding the New Cybersecurity Landscape

The digital transformation sweeping across industries has shifted how businesses operate, with the move to the cloud playing a crucial role in this transition. Organizations embracing cloud technologies benefit from increased flexibility, scalability, and cost efficiency while streamlining their IT infrastructure.

Yet, this rapid evolution also presents unique challenges and vulnerabilities in cybersecurity, making it essential for businesses to adapt and bolster their defenses against emerging threats.



The Shift to Attack-As-A-Service

The cyber attack landscape has significantly transformed recently, with a notable shift toward Attack-As-A-Service. While large corporations and government entities were once the primary targets of cybercriminals, the availability of advanced cyber-attack tools and services has led hackers to focus on small businesses. These organizations often lack the resources and expertise to defend themselves against sophisticated attacks, making them prime targets.

Ransomware attacks against small businesses increased by **150% in the last two years.**

The ease of acquiring advanced cyber-attack tools on the dark web has enabled criminals to launch devastating attacks on unsuspecting businesses. This has led to the rise of cybercriminals offering hacking-as-a-service, allowing even less skilled individuals to launch complex attacks.

Some key factors contributing to the growing complexity of the attack landscape include

AI and ML in Cybercrime

Utilizing Artificial Intelligence (AI) and Machine Learning (ML) by cybercriminals to craft more targeted and efficient attacks.

IoT Device Vulnerabilities

The accelerated growth of Internet of Things (IoT) devices often lack proper security measures and can be used as entry points for hackers.

Rise of Attack-As-A-Service

The increasing prevalence of Attack-As-A-Service, makes sophisticated cyber-attacks accessible to a broader range of threat actors, regardless of their technical skills.

Emerging Threats:

Beyond Ransomware and Phishing

While ransomware and phishing attacks remain prevalent, MSPs must be aware of other emerging threats that can significantly impact their small business clients. Some of these threats include

Supply chain attacks

Cybercriminals target third-party vendors or suppliers with weaker security measures, enabling them to access their intended target's systems.

Spear phishing

Highly targeted phishing attacks aimed at specific individuals within an organization, often using personal information gathered through social engineering.

Social engineering

Using manipulation, employees reveal sensitive info or allow unauthorized access via methods like impersonating peers or IT support personnel.

Financial Fraud

Cybercriminals utilize BEC schemes, invoice fraud, and unauthorized transfers to trick businesses and individuals into disclosing financial info or sending funds to fake accounts.

Chapter 4

It’s All About Consolidation

Security stack consolidation has emerged as a popular trend in the cybersecurity landscape, providing a range of advantages for MSPs. This approach involves streamlining and integrating multiple security solutions into a unified, cohesive system, which simplifies management and maintenance while enhancing overall effectiveness.

The Depth of Protection Against Multi-Vector Attacks and the Unique Relationship Between MSPs and Business Owners

The ease of acquiring advanced cyber-attack tools on the dark web has enabled criminals to launch devastating attacks on unsuspecting businesses. This has led to the rise of cybercriminals offering hacking-as-a-service, allowing even less skilled individuals to launch complex attacks.

While cost savings may be a driving factor for security stack consolidation, it's important to recognize that this approach offers enhanced protection against multi-vector attacks. By adopting enterprise-level security solutions and consolidating them into a single, comprehensive system, MSPs can provide their clients with the same level of protection enjoyed by larger organizations. However, traditional security tools are often not designed to support the unique relationship between MSPs and small business owners, resulting in inadequate protection and sub-optimal service offerings.

To overcome these challenges and bridge the gap between small businesses needs and traditional security tools' capabilities, MSPs should seek tailored security solutions that cater to the specific requirements of small businesses. These solutions facilitate effective communication between MSPs and their clients, ensuring business owners are well-informed about cybersecurity measures and ongoing efforts to protect their organizations from cyber threats.

By offering customized, multi-layered security solutions that address the unique risks faced by small businesses, MSPs can provide a more comprehensive level of protection against multi-vector attacks and strengthen the relationship with their clients. This collaborative approach enables MSPs to better understand the needs and concerns of small businesses.

Best Practices for Security Stack Consolidation

Implementing a comprehensive security policy

- Adopt an attacker's perspective when examining the digital footprint

- Identifying and addressing vulnerabilities and exposures effectively and on time

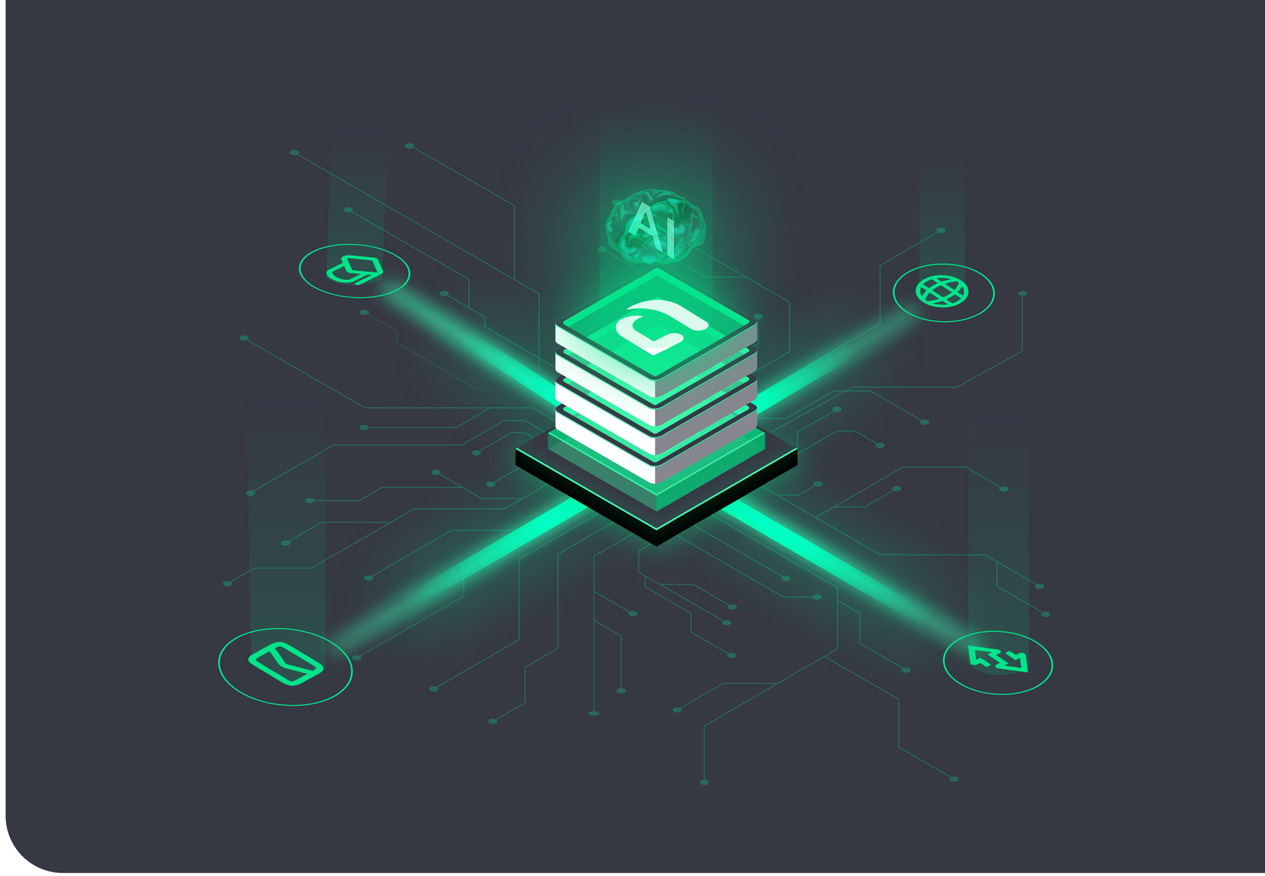
- Actively scan and quarantine emails to prevent phishing attacks - Consistently monitor data stored in the cloud for potential security breaches

- Enforce multi-factor authentication (MFA) for user logins to enhance access security

- Foster a culture of ongoing cybersecurity awareness through continuous education and simulation

- Proactively secure company devices to prevent unauthorized access and Ransomware

- Implement security controls to stop threats before they can cause damage



Unified security platforms can help businesses

lower cybersecurity costs by up to 50%

The Importance of Internal and External Communication in Showing Your MSP Value

Effective communication with clients is crucial for MSPs to showcase their value and maintain successful, long-lasting relationships. By proactively engaging in discussions about cybersecurity, MSPs can help clients understand the importance of robust security measures and the value of the services provided over time.

Practical Tips for Communicating Cybersecurity with Clients

Risk Assessments and Security Audits

MSPs should conduct regular risk assessments and security audits for their clients to identify potential vulnerabilities and areas for improvement. These assessments demonstrate the MSP's proactive approach to cybersecurity and provide an opportunity to discuss the findings with clients, highlighting the value of the services offered.

Security Awareness Culture

Implementing security awareness training and simulation for clients' employees is another valuable service that MSPs can offer. This helps educate the workforce about potential security threats, how to recognize them, and how to react appropriately, ultimately reducing the risk of successful cyberattacks.

Regular Updates and Reports

MSPs should provide clients with regular updates and reports on their cybersecurity status. This informs clients about ongoing efforts to protect their systems and data and demonstrates the MSP's commitment to continuous improvement.

Benefits of Proactive Client Communication

Proactive communication with clients about cybersecurity offers several benefits that can strengthen the relationship between MSPs and their clientsb

Builds Trust and Confidence

Regular communication demonstrates the MSP's commitment to protecting the client's data and systems, fostering trust and confidence in the MSP's expertise and services.

Showcases Value

By discussing risk assessments, security audits, and training progress, MSPs can effectively demonstrate their value to clients regarding enhanced security and risk mitigation.

Encourages Collaboration

Open communication channels facilitate collaborative problem-solving and decision-making, enabling MSPs and clients to address security challenges effectively.

Long-Term Relationships

Engaging clients in cybersecurity discussions can lead to long-term business relationships. Clients are more likely to continue their partnership with an MSP demonstrating commitment and expertise.

Chapter 5

A Data-Driven Approach to Improve Cyber Risk

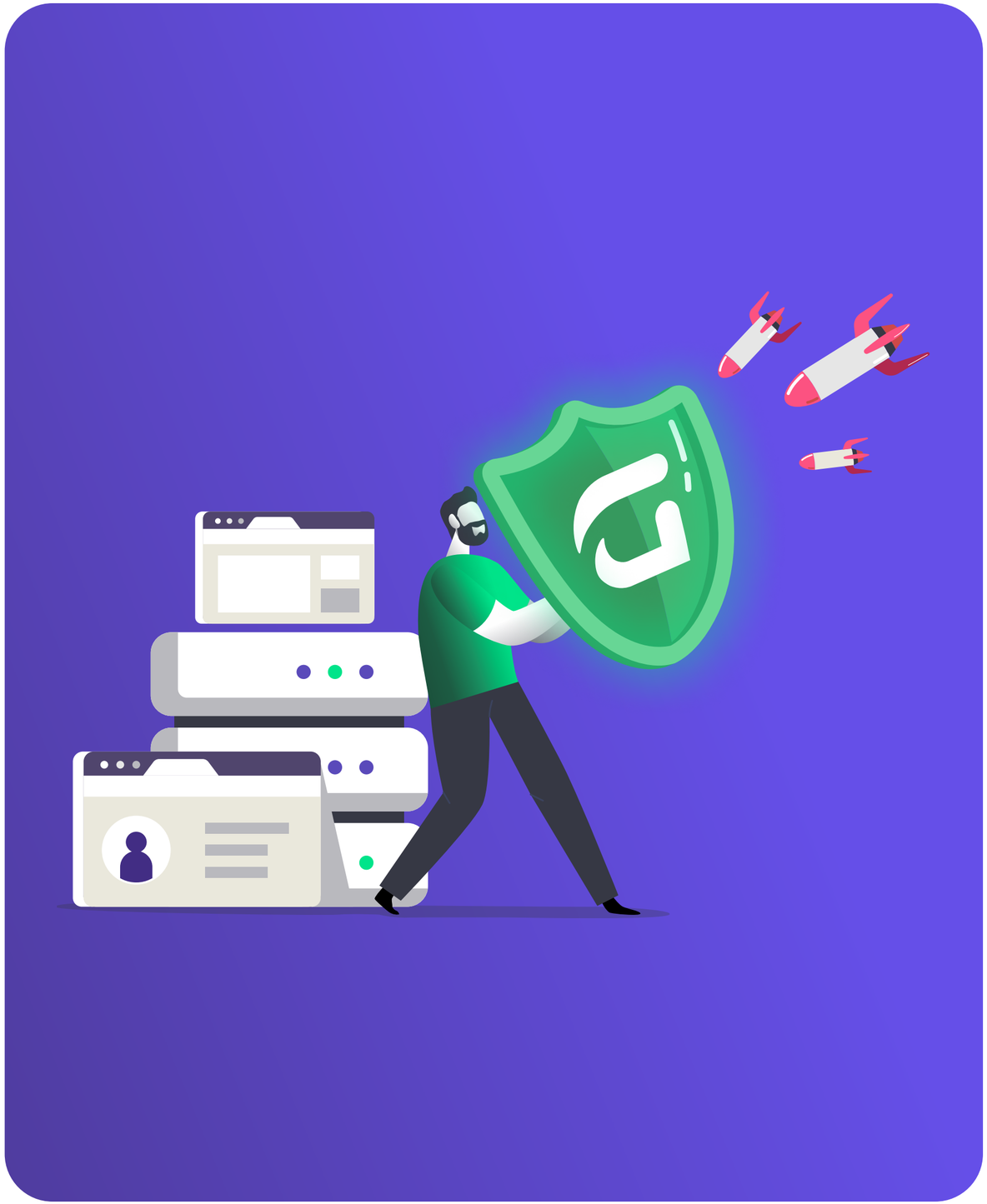
Solid Security and Eligibility for Risk Transfer to Insurance Carriers

The first step in becoming eligible for risk transfer to insurance carriers is establishing a strong, provable security posture.
This provides an additional layer of protection for the MSP and their clients and demonstrates the MSP's commitment to maintaining the highest security standards.

- Implement a comprehensive, consolidated security stack that addresses the unique needs of small businesses.

- Maintain clear documentation and evidence of security practices and incident response plans.

- Communicate the value of their security posture to clients, insurance carriers, and other relevant parties.



The Growing Importance of Cyber Insurance and its Role in Driving Small Business Success

With the increasing reliance on technology and an expanding cyber risk landscape, small businesses are uniquely positioned to be both the beneficiaries of digital transformation and victims of cyberattacks.

The Rising Tide of Cyberattacks

It's no secret that cyberattacks are increasing. According to the 2022 Cyberthreat Defense Report, 81% of organizations experienced at least one successful cyberattack in the past year. Moreover, small businesses are no exception. It is estimated that in 2023, 44% of cyberattacks will target small businesses, and due to limited resources and security infrastructure, they will become an easier target.

The High Cost of a Data Breach

The financial implications of a cyberattack can be devastating for small businesses. According to the Ponemon Institute's 2022 Cost of a Data Breach Report, the average cost of a data breach is set to rise to $4.07 million. This figure could result in insurmountable losses for small businesses and even cause them to shut down.

The Role of Cyber Insurance in Mitigating Risks

Cyber insurance has become essential for small businesses to manage cyber risks more effectively. It provides financial protection in the event of a cybersecurity incident, enabling businesses to recover faster and minimize the long-term impact of a breach.

The Competitive Advantage of Having Cyber Insurance

In today's fast-paced digital economy, businesses with robust cybersecurity strategies attract more customers and drive growth. With a cyber insurance policy, small businesses can showcase their commitment to data protection and privacy, instilling confidence in their customers and becoming trusted partners in the digital era.

The Competitive Advantage of Having Cyber Insurance

In today's fast-paced digital economy, businesses with robust cybersecurity strategies attract more customers and drive growth. With a cyber insurance policy, small businesses can showcase their commitment to data protection and privacy, instilling confidence in their customers and becoming trusted partners in the digital era.

The Path Ahead: Building a Resilient Future

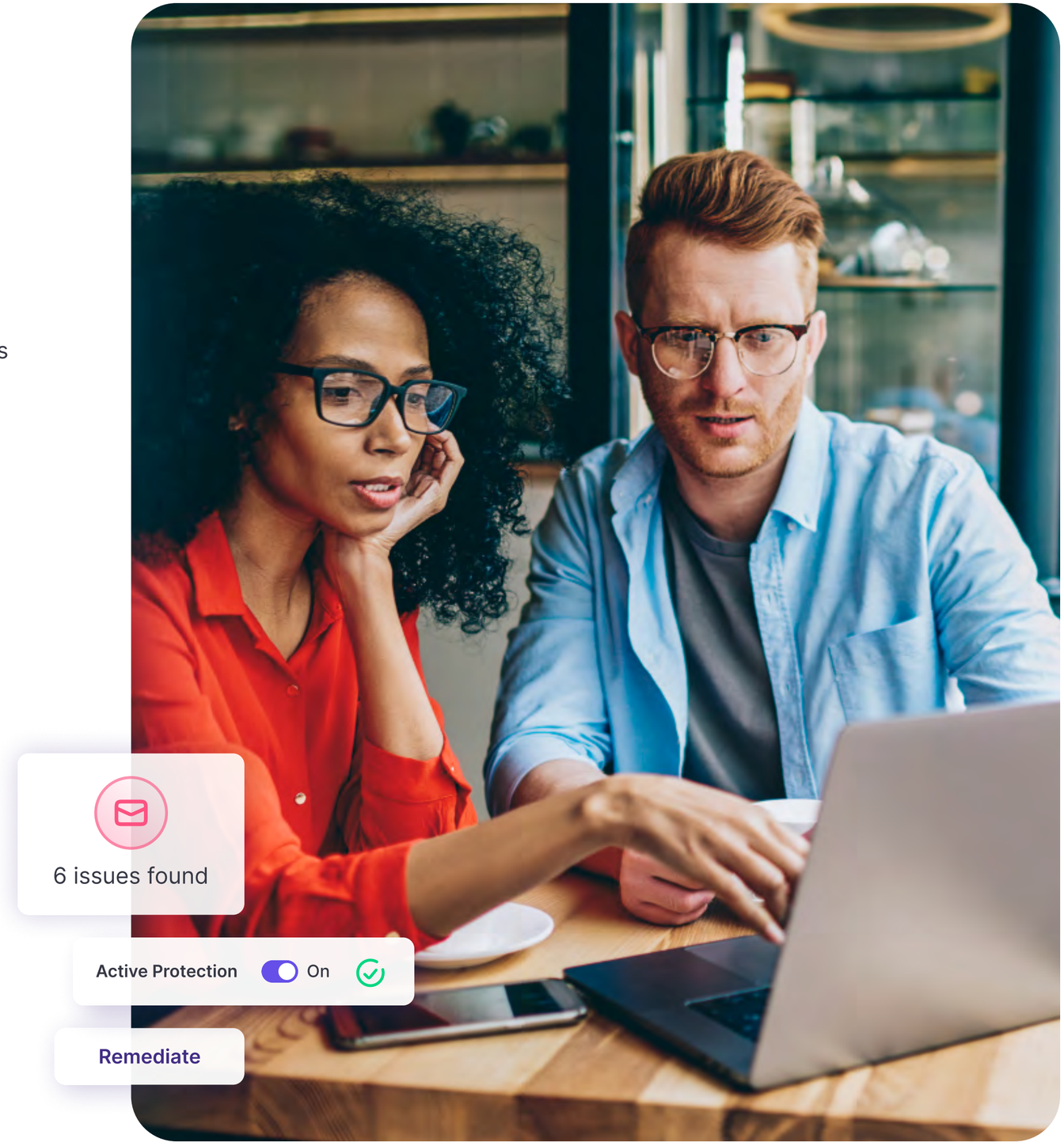
To successfully navigate the evolving cybersecurity landscape, small businesses must view cyber insurance as an essential element of their risk management strategy. By partnering with MSPs offering comprehensive cybersecurity services, small businesses can further bolster their defenses, protect their digital assets, and position themselves for long-term growth in the upcoming years.

Insursec and Why You Should Know Your Risks in Real-Time

In today's digital age, businesses increasingly depend on technology to manage their operations, store sensitive data, and communicate with clients. While this has undoubtedly improved efficiency and productivity, it has exposed organizations to many cyber threats. Insursec, which combines "insurance" and "security," refers to protecting businesses against cyber risks through insurance policies and cybersecurity measures.

The Growing Need for Insursec

With attackers employing new tactics to exploit system vulnerabilities, cyber threats constantly evolve and become more sophisticated. A single cyber-attack can have severe consequences for your business, including financial losses, reputational damage, and legal liabilities. As a result, organizations increasingly recognize the need for a robust Insursec strategy combining insurance coverage and proactive cybersecurity measures.



Here are some reasons why you should know your cyber risks in real-time:

Rapidly Evolving Threat Landscape

Cybercriminals are constantly developing new strategies and tools to infiltrate businesses, making it crucial for organizations to stay informed about the most recent threats and vulnerabilities. Understanding your risks in real-time allows you to quickly identify and respond to potential issues before they escalate into significant incidents.

Regulatory Compliance

Various industries are subject to strict regulations regarding data protection and cybersecurity. Not complying with these regulations can result in significant fines, legal penalties, and reputational damage. Real-time risk monitoring ensures that your organization remains compliant by promptly addressing any issues.

Protect Your Reputation

A cyber incident can damage your organization's reputation, affecting customer trust and confidence. By understanding your risks in real-time and implementing effective Insursec measures, you can minimize the impact of a cyber incident on your reputation and maintain the trust of your clients.

Minimize Financial Losses

Cyberattacks can lead to significant financial losses, directly through theft or extortion and indirectly due to operational disruptions. Real-time risk awareness enables your organization to detect and mitigate threats before they lead to significant financial losses. Additionally, having comprehensive insurance coverage can provide financial support in the event of a cyber incident.

Strengthen Your Security Posture

Real-time risk monitoring identifies vulnerabilities in your security infrastructure. Addressing issues promptly improves your business's security posture, reducing successful cyberattacks chances. This proactive cybersecurity approach safeguards your business, conveying a strong message to stakeholders, clients, and regulators about taking threats seriously.

How Insursec Helps You Manage Your Risks in Real-Time

A comprehensive Insursec strategy involves a combination of insurance coverage and cybersecurity measures designed to work in tandem to protect your organization from cyber risks. Here's how Insursec can help you manage your risks in real-time

Insurance Coverage

Cyber insurance policies provide financial support in the event of a cyber incident, helping your organization recover from the financial losses incurred. These policies typically cover expenses related to data breach notifications, legal fees, public relations efforts, and regulatory penalties. Having adequate insurance coverage can mitigate the financial impact of a cyber incident on your business.

Threat Intelligence

Real-time threat intelligence services inform your organization about the latest cyber threats and vulnerabilities. By leveraging this information, you can proactively implement security measures to counter emerging threats and protect your organization from potential attacks.

Employee Training and Awareness

Human error is often a significant factor in successful cyberattacks. Regular employee awareness training can help prevent incidents by ensuring that your staff understands the importance of cybersecurity and follows best practices to maintain the security of your organization's systems and data.

Continuous Monitoring and Incident Response

Effective Insursec strategies involve constant system and network monitoring for suspicious activity. Organizations can prevent escalation and damage by detecting and addressing potential threats in real-time. A robust incident response plan outlining steps to take in case of a security breach is also essential.

Risk Assessments and Vulnerability Management

Regular risk assessments and vulnerability management are crucial components of an Insursec strategy. By identifying and addressing system vulnerabilities, you can reduce the probability of a successful cyberattack and maintain a strong security posture.amage.

Chapter 6

Leveraging AI to Strengthen Your Cybersecurity Game

Meet Guardz: The Power of One Cybersecurity Platform for MSPs

Guardz, much like a reliable AI sidekick, empowers MSPs with a set of advanced tools and capabilities to enhance their cybersecurity strategies, as well as secure and insure SMEs against evolving threats such as phishing, ransomware attacks, data loss, and user risks by leveraging AI and a multilayered approach.

With a comprehensive suite of features covering the most common attack vectors—including Email, Cloud Apps, External Risk, Devices, Employee Culture, and Web Browsing—the Guardz holistic solution for MSPs to protects their clients in the most cost-effective and user-friendly way.

What Sets Guardz Apart

Holistic

Guardz protects SMBs/SMEs from the most common attack vectors, including emails, cloud apps, browsers, devices, external exposure, and employee negligence, ensuring that your security is shielded from any potential threats that may arise.

Hassle-Free

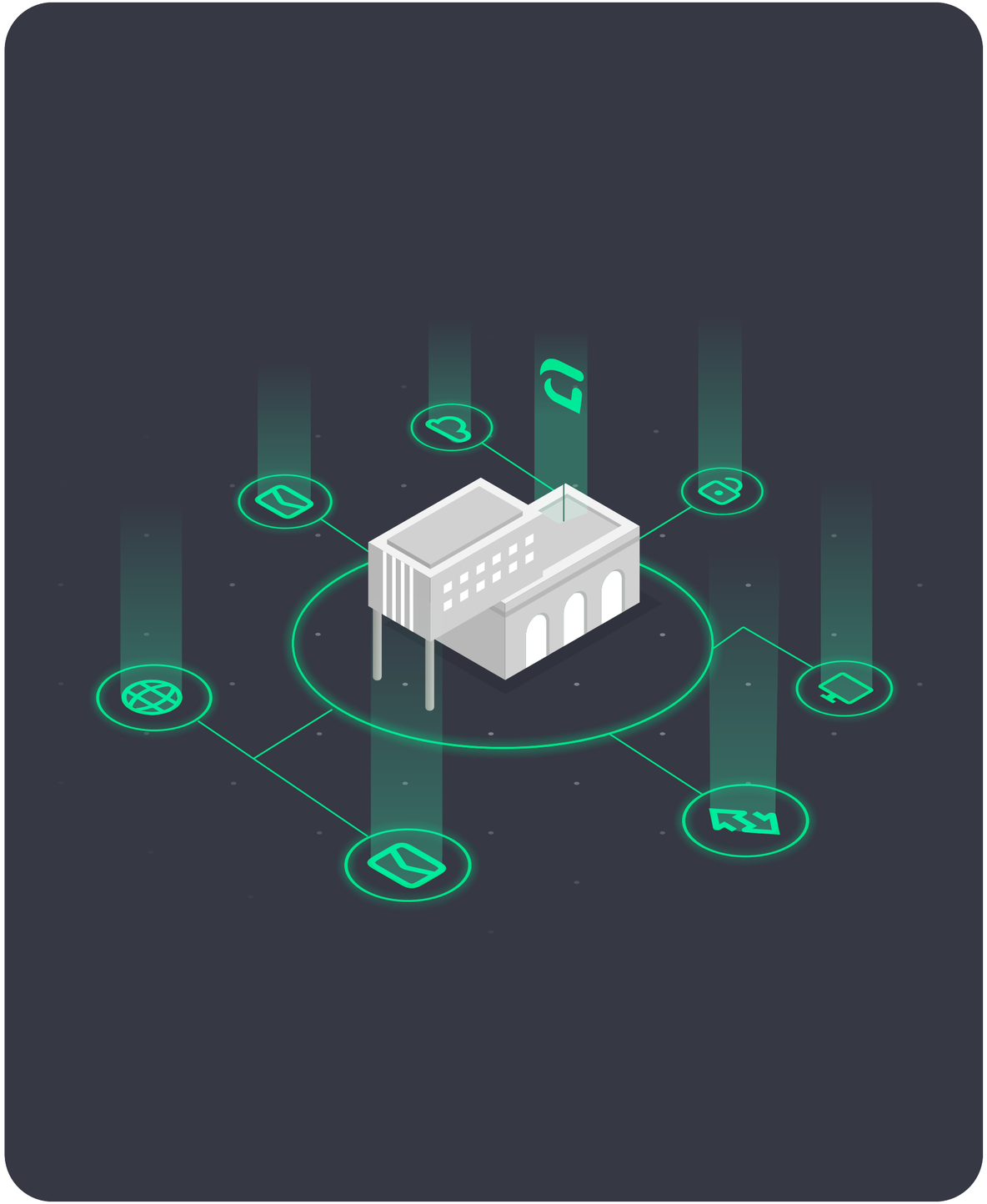
Protecting your business from potential cyber threats should be hassle-free. Guardz offers SMBs/ SMEs a fully managed service so they can rest easy knowing that a dedicated team of professionals works tirelessly to keep the business secure.

Cost-Effective

Guardz provides an holistic security solution that combines vital security tools into a single platform tailored to your specific budget and requirements.

Future-Proof

Guardz facilitates the adoption of cyber insurance to mitigate financial risks from cyber threats like data breaches, ransomware attacks, and phishing by ensuring readiness and access to adequate coverage.



Cybersecurity Co-Pilot for MSPs

Secure Clients Effectively

Guardz offers a holistic solution to safeguard your clients, employees, cloud applications, emails, and devices, all within a multi-tenant platform.

Boost Your Revenue

Attract new clients by demonstrating your reliability through efficient prospecting capabilities, accurate reporting, and complete coverage.

Show Immediate Value

Enhance your security offerings for your clients with just a click of a button to seamlessly demonstrate the value that you bring to the table as an MSP.

What MSPs Are Saying About Guardz

"Guardz offers a thorough service. External, internal, phishing, and compliance/training are all under one umbrella. Reasonably priced for small to medium-sized enterprises. A very well-developed platform."

Alex Martin
MSP, Director of Cyber Services, Trusthogen

★★★★★

Learn more >

"Helps to solve cybersecurity issues by providing additional layers of protection in conjunction with existing malware protection software. This approach ensures that all managed systems are shielded."

Eugene DeVillamil
MSP, Founder YAMA Industrials, Inc

★★★★★

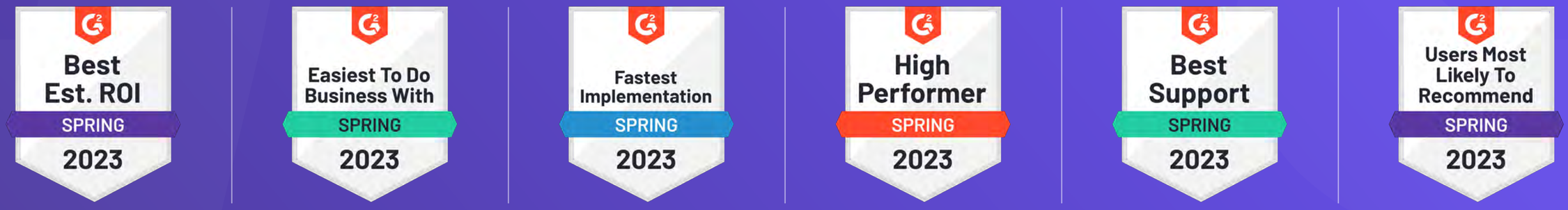
Learn more >

“We added the powerful Guardz platform within our own cloud native environment to make sure our configuration and users stay secure. Guardz is the perfect solution to protect small businesses”

Maikel Roolvink
MSP, Security Officer, Dutch Technology eXperts

★★★★★

Learn more >



Guardz.

Managed Cybersecurity Platform Built for MSPs.

Book a Demo