THRIVE℠

The Mid-Market Company's Guide to Cybersecurity

MID-MARKET EBOOK

Is Your Company Mid-Market?

Mid-market companies are typically defined by key criteria such as revenue, employee count, and growth stage. Mid-market companies typically have annual revenues between $10 million and $1 billion and can have anywhere from 100 to 1,000 employees. Businesses that fall in this category have moved beyond the startup phase, having gained a stable customer base and steady revenue streams. However, they have not quite reached the expansive resources and technical complexity of most large enterprise organizations. As they continue to expand, mid-market businesses face a unique set of challenges that often require tailored solutions distinct from those used by both smaller and larger companies.

Mid-market companies differ from small businesses and large enterprises in terms of their security needs, operational scale, and overall risk tolerance. Small businesses, typically with fewer than 100 employees, often have a simpler IT environment and may not require robust cybersecurity measures or a dedicated IT staff. In contrast, large enterprises usually have extensive in-house IT teams and budgets, enabling them to implement an advanced, multilayered security stack. Mid-market organizations fall somewhere in between, often relying on a leaner IT team to address increasingly complex cybersecurity needs as they grow. This coupling of limited resources and growing needs necessitates a cybersecurity approach that is sophisticated enough to protect against advanced threats but also efficient enough to operate within the organization's resource constraints.

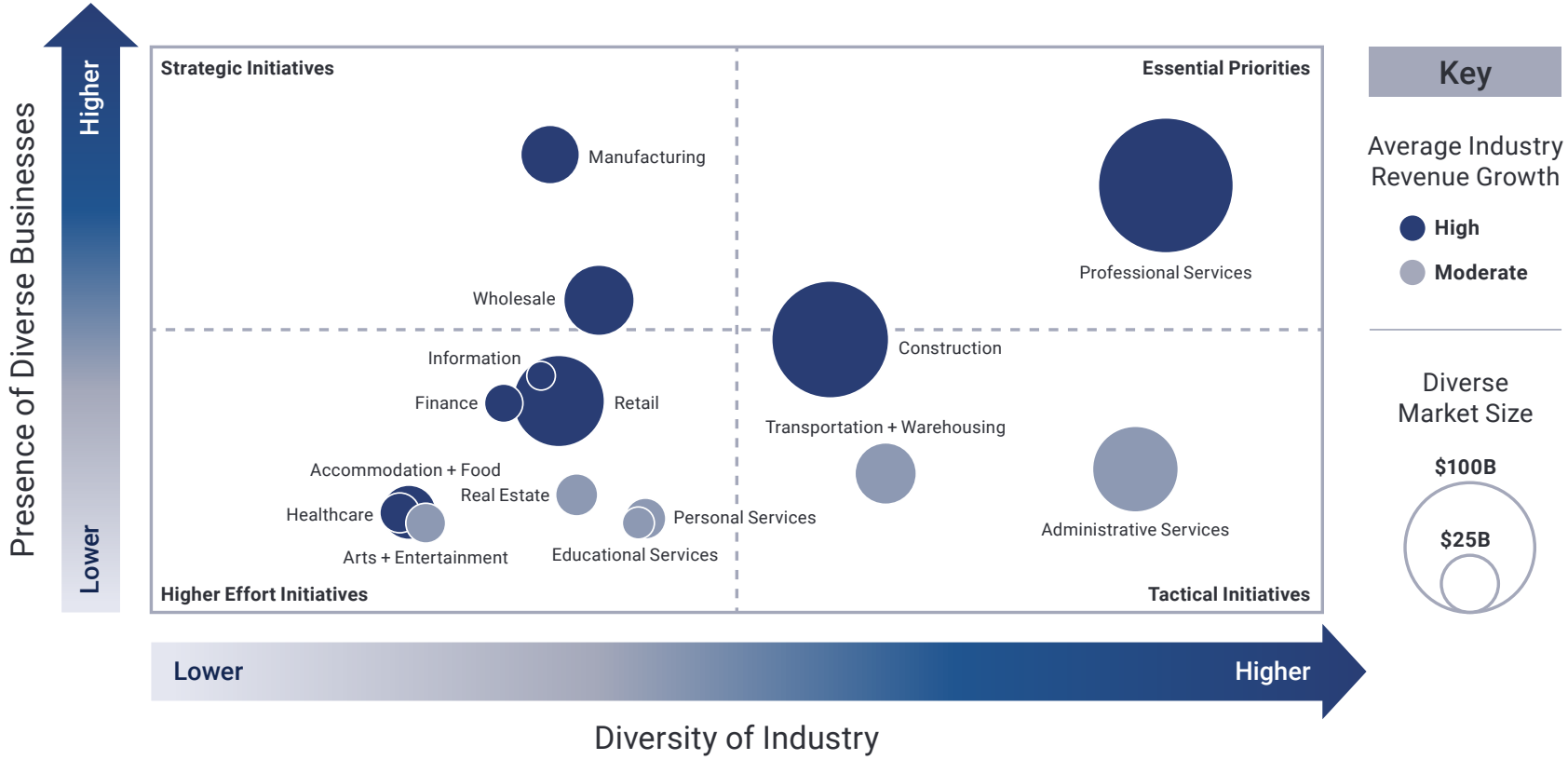
61%

of mid-market businesses do not have dedicated cybersecurity experts in their organization.

Source: huntress.com/resources/the-state-of-cybersecurity-for-mid-sized-businesses-in-2023

For mid-market companies, flexibility and scalability are crucial in their cybersecurity approach. Unlike larger enterprises, which can afford dedicated, large-scale cybersecurity infrastructure, mid-market organizations must adopt solutions that grow and adapt with them. This scalability is especially important as they expand their digital footprint, which can include remote teams, cloud solutions, and adopting interconnected systems that increase the attack surface for cyberattacks. With limited resources compared to large enterprises, mid-market organizations need cybersecurity solutions that are flexible and responsive so they can maintain security while focusing on growth and innovation.

Diverse-owned Midsize Business Presence and Industry Diversity



Source: Next Street Middle Market Survey (2023); U.S. Census Bureau, Annual Business Survey (2020); NAICS; Tagnifi; Next Street analysis of Grata data (accessed September 2023)in-2023

The Unique Security Needs of a Mid-Market Company vs. a Large Enterprise or Small Business

The cybersecurity requirements of mid-market companies are uniquely challenging. They must manage their IT stack with leaner teams and more constrained financial resources, while also being expected to uphold security and compliance standards that can be just as rigorous as those required by larger organizations. This creates a delicate ongoing balancing act for cost-effective, high-impact security measures that can scale in step with growth while staying within budgetary limits.

A key reason mid-market organizations need to invest in their cybersecurity is for compliance with industry regulations. Complying with regulations such as GDPR, HIPAA, GLBA, DORA, and PCI-DSS is often non-negotiable, as failing to meet these requirements could result in costly fines, reputational damage, or even legal action. Unfortunately, traditional enterprise-grade cybersecurity solutions that ensure compliance, are often high-cost, and may not be feasible for mid-market budgets. Because of this, making strategic investments in cybersecurity is essential. Mid-market companies need to prioritize solutions that address both compliance and protection in an efficient, cost-conscious way, such as managed security services, automated compliance tools, and proactive threat detection.

Another complicating factor is the hybrid nature of many mid-market IT environments, which often will combine legacy on-prem systems with cloud-based solutions and remote or hybrid workforces. As mid-market companies evolve, they tend to adopt cloud and SaaS platforms for efficiency and scalability, but may still rely on legacy systems that are deeply integrated into their operations. According to Cybersecurity Insiders 2024 Cloud Security Report, 49% of respondents struggle with integrating cloud services into aging legacy systems, a task complicated by scarce IT resources, which can hinder effective and secure integration. Having a mix of legacy and cloud systems can elevate the risk of security gaps, making it crucial to choose solutions that unify monitoring, threat detection, and response across all environments to prevent breaches.

For mid-market companies, operational efficiency and risk management are especially high-stakes. Cyber incidents can be disproportionately damaging for mid-market businesses, where recovery resources are limited and operational downtime can significantly impact revenues and reputation. Unlike larger organizations that may have backup systems or dedicated disaster recovery teams, mid-market companies often need to avoid disruptions altogether, prioritizing proactive threat mitigation and rapid response in their cybersecurity plans. Solutions that streamline cybersecurity processes—such as centralized security dashboards, automated alerts, and incident response planning—enable these companies to maximize efficiency and mitigate risks effectively, preserving their focus on growth while keeping security and compliance robust.

49%

of cloud and cybersecurity professionals struggle with integrating cloud services into aging legacy systems

Source: Cybersecurity Insiders, 2024 Cloud Security Report

Skills Gap: What Mid-Market Companies May Be Lacking

Mid-market companies often face a significant skills gap in critical areas of cybersecurity and IT, which can leave them vulnerable as they continue to grow and adopt more complex technologies. While large enterprises usually have in-house security professionals, including Chief Information Security Officers (CISOs), security architects, and 24x7 security operations teams, mid-market organizations may not have the budget or bandwidth to maintain this level of dedicated expertise. This lack of specialized security personnel can lead to gaps in threat detection, response, and overall strategic oversight, as general IT staff are stretched thin trying to cover multiple roles. Without a full-time CISO or security architect, many mid-market companies struggle to develop a long-term security roadmap and implement advanced threat defenses. And without sufficient staff, they cannot achieve the round-the-clock monitoring required to defend against pervasive cyber threats.

Another crucial area where mid-market companies often lack expertise is in cloud architecture and engineering. As these organizations scale, they tend to adopt cloud services and hybrid environments to enhance flexibility and support remote workforces. However, without experienced cloud architects and engineers, they may face challenges in securely deploying and managing these cloud environments. Misconfigurations in the cloud are a common cause of data breaches, as the specific security controls for cloud infrastructure can differ significantly from those of traditional on-premises systems. Skilled cloud architects and engineers can help mid-market companies design secure, scalable cloud environments that support growth without exposing the organization to unnecessary risks. According to Gartner, by 2026, 60% of organizations will prioritize the prevention of cloud misconfiguration for their cybersecurity plan.

According to Gartner, by 2026,

60%

of organizations will prioritize the prevention of cloud misconfiguration for their cybersecurity plan.

Compliance and regulatory expertise is another gap for many mid-market companies, especially those that operate in highly regulated industries like finance, healthcare, or retail. As these companies grow, they are subject to more stringent regulatory requirements, yet they often lack the resources for a full-time compliance officer or legal counsel specializing in data protection regulations. Compliance experts can guide organizations in implementing controls to meet standards like GDPR, HIPAA, DORA, GLBA, or PCI-DSS, reducing the risk of penalties and ensuring customer trust. Without this in-house expertise, mid-market companies are more likely to struggle with meeting compliance demands, increasing the risk of costly fines or damage to their reputation.

Mid-market organizations may also lack IT strategists who understand the unique challenges and opportunities of companies in a growth phase. Unlike IT managers in large enterprises or small startups, IT teams in mid-market companies need to focus on both innovation and scalability, balancing the growth ambitions of the company with the practical limitations of their current budgets and resources. These professionals are essential for setting a realistic technology roadmap, identifying strategic investments that will provide long-term value, and ensuring the organization's cybersecurity infrastructure scales effectively with growth. Without these skills, mid-market companies are at risk of under-investing in essential security and infrastructure areas or, conversely, over-investing in solutions that do not align with their current or future needs.

Signs That You Need to Move On from Small-Scale MSPs

Most mid-market organizations that have turned to IT outsourcing start off small with a local IT support firm or even a smaller MSP. But often they realize that the growing complexity of their IT stack and heightened regulatory compliance requirements requires a Managed Security Services Provider (MSSP). While MSPs can help with a broad range of IT and help desk services, MSSPs are cybersecurity-focused, with dedicated Security Operations Center (SOC) specialists, and a deeper scope of services to protect your business.

Below are signs it's time to level up to an MSSP:

- **Outgrowing Service Capabilities:** As mid-market companies grow, they often experience delays in response times and notice unresolved service tickets piling up—signs that their current MSP may lack the capacity to support their expanding needs. Additionally, growing IT environments are usually more complex, requiring comprehensive infrastructure support and specialized expertise to manage new technologies and applications. Many small MSPs struggle to provide this level of service, especially as clients' requirements shift from basic IT maintenance to more sophisticated security and infrastructure needs.
- **Gaps in Proactive Support and Strategic Guidance:** Many small-scale MSPs operate in a reactive mode, addressing issues as they arise. This approach can leave mid-market companies vulnerable and at risk, as they need proactive monitoring, regular security assessments, and an IT partner who can foresee and mitigate potential issues.
- **Inability to Meet Compliance and Security Requirements:** As mid-market companies expand, they face increasingly strict compliance regulations, often requiring specialized expertise and attention to detail. Many small-scale MSPs lack the resources to help clients meet these standards effectively, which can result in compliance gaps that expose the organization to legal fines, an inability to get cyber insurance, and reputational damage.
- **Lack of Focus on Scalability and Business Growth:** For mid-market organizations, scalability is crucial to maintain momentum, from IT infrastructure that grows with the business to adaptable security services. Smaller MSPs often provide a "one-size-fits-all" solution that doesn't support unique growth requirements, limiting a company's ability to scale and adapt. Transitioning to an MSSP with experience serving mid-market clients can provide the flexibility and focus necessary to ensure sustainable growth, enabling companies to expand their operations securely and strategically.

Enterprise Cybersecurity Trends That Can Leave Mid-Market Companies Vulnerable

As the cybersecurity landscape evolves, many mid-market companies find themselves inadvertently exposed to cyber attacks and breaches by attempting to adopt trending niche technologies without having the necessary foundations in place. One major shift affecting companies of all sizes is the movement away from relying solely on perimeter security. In a modern work environment where users are no longer operating strictly within a traditional network perimeter, it is irresponsible to depend entirely on firewalls and network-based security. Mid-market organizations, especially those with hybrid or remote workforces accessing the company's systems from across the world, need to move toward a more holistic approach to security, integrating solutions like endpoint protection and identity management.

Another challenge is that, unlike larger organizations, many mid-market companies lack comprehensive protection for SaaS applications, cloud-based platforms, and employees' mobile devices that have access to the company's systems. As businesses increasingly leverage cloud-based tools and enable mobile workflows, each of these elements becomes a potential entry point for threats if not properly secured. This gap leaves them exposed to threats that can bypass traditional security measures and affect sensitive data or disrupt business operations, which can be costly.

The fast-paced nature of the cybersecurity industry can also create confusion around where mid-market companies should invest their limited budgets. With so many different tools and technologies on the market, it's easy for organizations to become overwhelmed, unsure of which solutions are essential versus which are optional. This confusion can lead to inefficient spending on security products that may not address the company's primary vulnerabilities, leaving gaps that sophisticated threat actors can exploit.

Lastly, the desire to invest in the latest "hot" technology without securing the right cybersecurity basics is a common pitfall. Mid-market companies may be tempted by high-tech solutions like AI-driven threat detection or advanced threat intelligence platforms, however, these tools are often ineffective without solid foundational protections, such as strong access controls, endpoint security, and employee awareness training. Focusing on the fundamentals first ensures that companies have a resilient cybersecurity base to build on, making them less susceptible to attacks, even as they incorporate more advanced technologies.

Mid-market organizations, **especially those with hybrid or remote workforces** accessing the company's systems from across the world, need to move toward a more holistic approach to security, integrating solutions like endpoint protection and identity management.

How Thrive is Different

Thrive is the ideal partner for mid-market businesses, offering solutions that are carefully tailored to meet the distinct challenges of this growth phase. Unlike many MSP providers that deliver one-size-fits-all services, Thrive focuses on designing IT strategies that align with each client's specific needs and business goals. Thrive's team of industry experts takes the time to understand the nuances of each organization's operations, ensuring that they have access to the right mix of technologies and support, optimizing performance, and security as they scale. Thrive's deep expertise in managing cloud environments allows clients to seamlessly integrate and manage both on-premises and cloud resources, ensuring that every component of the IT stack functions harmoniously.

Thrive, as both a Managed Services Provider (MSP) and Managed Security Services Provider (MSSP), not only provides a comprehensive suite of cyber security services but also provides the ability to directly mitigate and remediate security incidents identified by our Security Operations Center by engaging our managed services team that is supporting their IT environment. All pure-play MSSPs can only provide security alerting and instructions for mitigating or remediating security incidents which fall on the client to perform the required actions. This responsibility can result in critical delays that may have additional negative impacts from the security incident.

Security, compliance, and scalability are at the forefront of Thrive's service model, making it an ideal partner for mid-market companies navigating complex regulatory requirements and growth demands. Thrive emphasizes robust security frameworks to protect against ever-evolving cyber threats, as well as compliance solutions that align with industry standards. Additionally, Thrive's flexible approach allows businesses to scale their IT services based on shifting needs, providing a cost-effective solution that adjusts with organizational growth or change. This combination of flexibility, expertise, and security focus enables mid-market businesses to confidently pursue their goals with an agile, resilient IT foundation.

The Thrive Approach

Thrive delivers a comprehensive range of IT services tailored to the unique needs of mid-market companies, covering everything from cloud infrastructure to advanced security management. With a consultative approach, Thrive collaborates closely with each client to understand their specific business objectives and align IT strategies accordingly, ensuring that every solution supports both current needs and future growth. This strategic alignment allows mid-market organizations to maximize their IT investments and adapt seamlessly as they scale, benefiting from enterprise-grade capabilities without the complexity.

In addition to offering end-to-end support—from planning and implementation to ongoing management—Thrive's proactive model includes continuous monitoring to address issues before they become problems. Thrive's 24x7x365 oversight strengthens security, reduces downtime, and enhances operational efficiency, allowing internal teams to focus on core business activities and goals. Thrive's proactive and tailored approach means clients are equipped with a resilient, secure IT infrastructure that supports growth, efficiency, and peace of mind.

Contact the Thrive Team

To Learn More, Contact Us Today, or Give Us a Call At:
thrivenextgen.com | info@thrivenetworks.com | 1-866-205-2810

About Thrive

Thrive delivers global technology outsourcing for cybersecurity, Cloud, networking, and other complex IT requirements. Thrive's NextGen platform enables customers to increase business efficiencies through standardization, scalability, and automation, delivering oversized technology returns on investment (ROI).

They accomplish this with advisory services, vCISO, vCIO, consulting, project implementation, solution architects, and a best-in-class subscription-based technology platform. Thrive delivers exceptional high-touch service through its POD approach of subject matter experts and global 24x7x365 SOC, NOC, and centralized services teams. Learn more at www.thrivenextgen.com or follow us on LinkedIn.