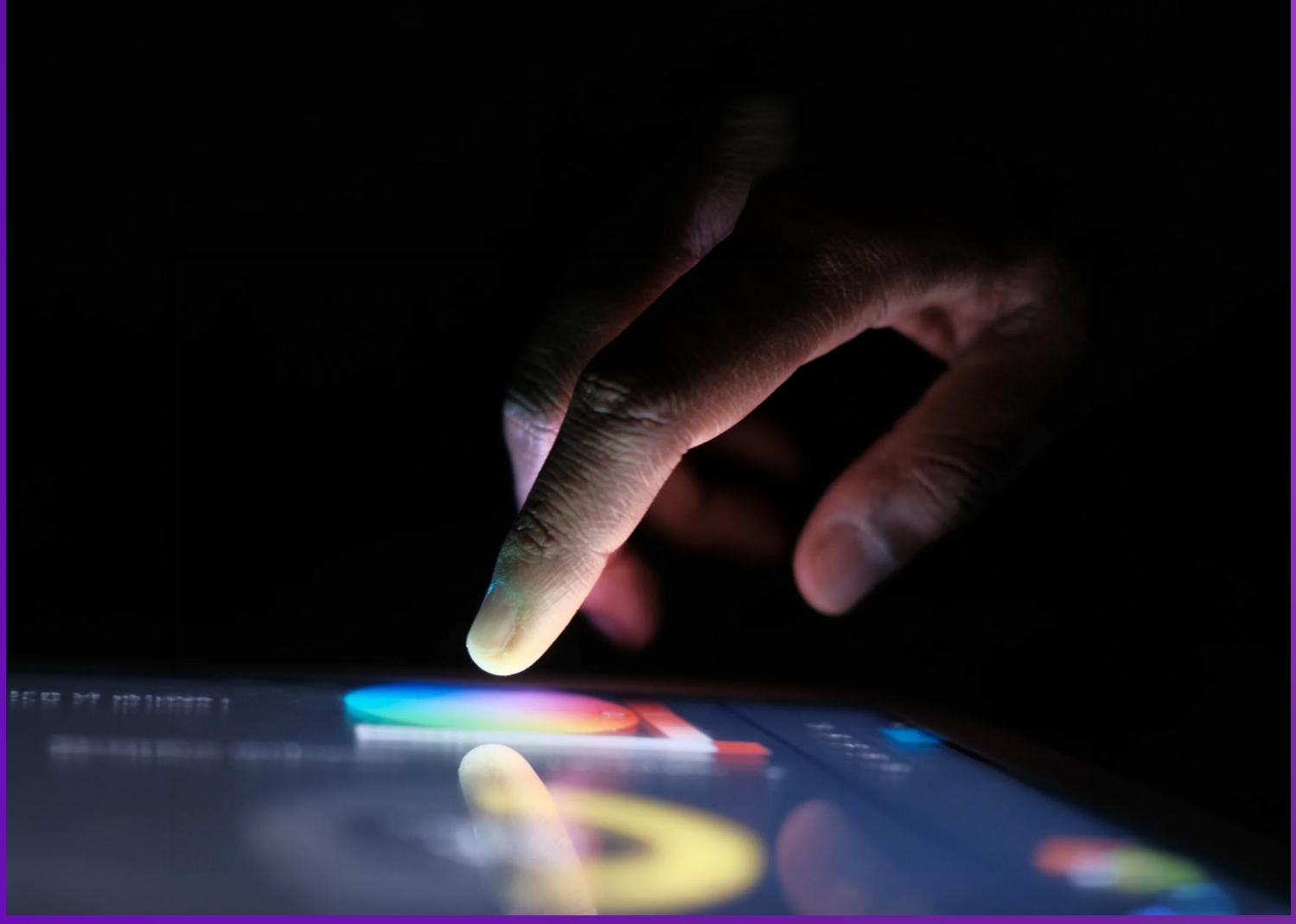
The mid-market security scale trap

How to avoid fragmented defenses that leave mid-market companies exposed to enterprise-level threats



Accenture Cybersecurity

Jason Lewkowicz, Amit Vasudeva, Deepak Mathur and Yusof Seedat

Accenture Edge

Contents

The mid-market is reaching an inflection point

Small and medium companies have never been more capable, or more exposed.

Operating across markets, cloud platforms, AI-driven workflows and a web of third-party dependencies, these mid-market companies have taken on the complexity of large enterprises without the security to match.

In 2025, 88%[1] of ransomware-linked breaches hit small to medium sized businesses, more than double the rate for large enterprises. Three-quarters[2] of small companies believe a single major cyberattack could put them out of business. Yet only 28% embed security into transformation decisions from the start, according to Accenture's State of Cybersecurity study of more than 1,600 mid-market companies across 17 countries.

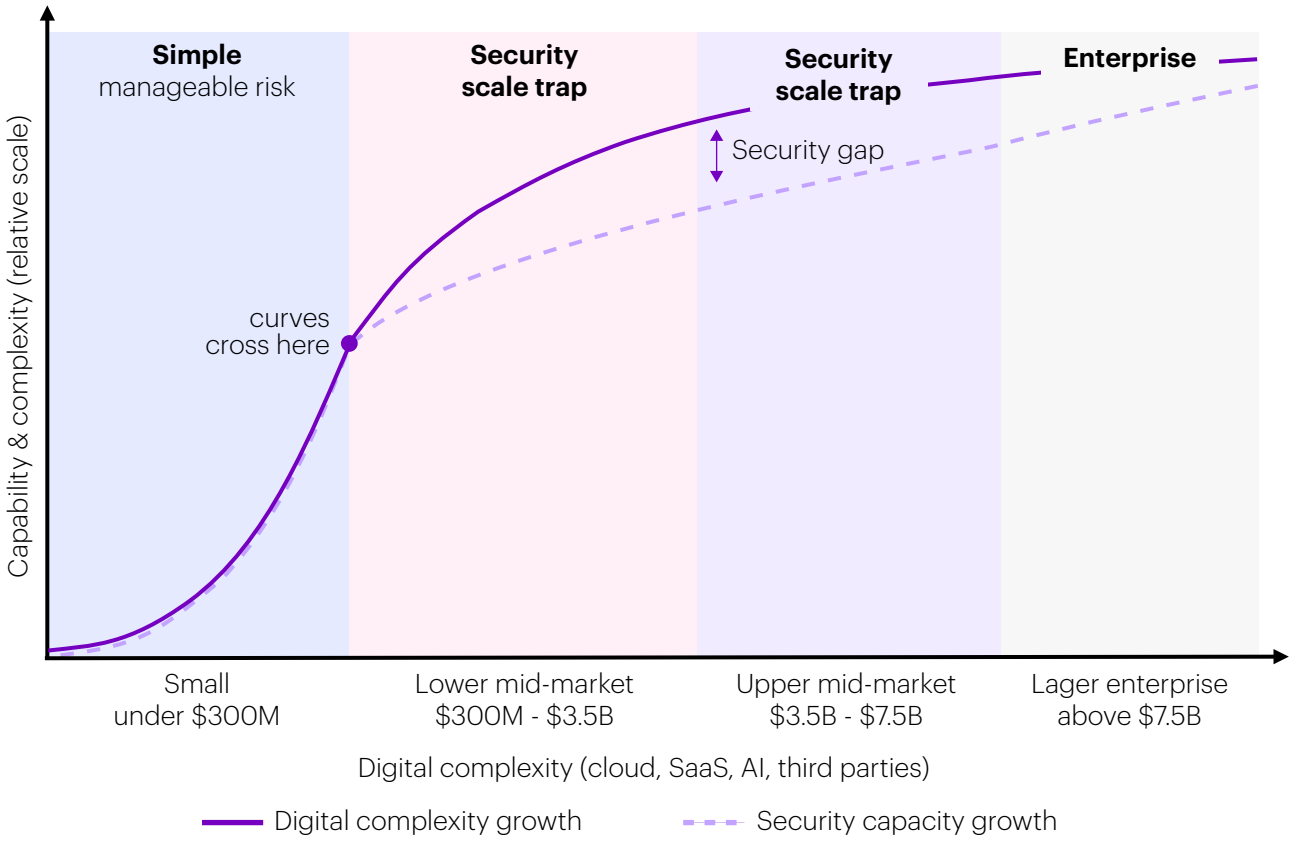
Many recognize the risk but struggle to operationalize security. Eighty-eight percent struggle to apply zero trust principles effectively during transformation, while 84% struggle to translate cyber risk strategies into practices that support growth and reinvention.

Their response is often to invest in more security tools, providers and controls. One new tool per risk. One new vendor per worry. Each may add value alone, but collectively increase cost, complexity and coordination demands.

As capabilities accumulate, the effort required to manage them can grow just as quickly. We call this structural problem the cybersecurity scale trap.

Figure 1: The cybersecurity scale trap

As organizations grow in digital complexity, security capacity struggles to keep pace. The gap is widest in the mid-market, where companies face enterprise-level complexity without enterprise-level resources.



Source: Accenture Research.

Understanding security debt

The trap creates a liability that rarely appears on a balance sheet: security debt. Like financial debt, it can accelerate progress in the short term while creating constraints that become increasingly difficult and expensive to unwind. Two forms can accumulate and reinforce each other: **design debt** and **coordination debt**.

Bolt-on security, a debt you'll pay later

Only **28%** embed cybersecurity into transformation from the outset

Design debt accumulates when security arrives after architecture decisions are made. A company migrates to cloud, integrates suppliers, launches a digital channel or embeds AI into workflows, and only then does the security team begin asking which identities should have access, what sensitive information an AI agent may retrieve or how operations will continue if a critical platform becomes unavailable.

By then, security teams are compensating for architectures they did not design, contracts they did not shape, and business processes that are expensive to change.

Signs include recurring exceptions, compensating controls, access workarounds, and persistent concerns that critical systems are difficult to secure and recover.

A 2024 intrusion at a technology provider illustrates the consequences of security design debt. Attackers gained access through a legacy test account that lacked multifactor authentication and sat outside the environments modern identity controls. The environment had modernised. The account had not. Retrofitting the gap meant reworking identity governance across the architecture, not adding a tool.

More controls, less coordination

84% struggle to translate cyber risk strategy into growth supporting practices

Coordination debt builds when companies keep adding controls without rethinking how they work together. More products generate more alerts. More providers create more handoffs. More specialist teams increase the coordination burden. No single control has to fail for the defensive system to break down.

Coordination debt becomes most visible during an attack, when delays between detection, decision-making and response create openings for attackers.

A recent regulatory penalty over a ransomware breach at a services group reads as a map of coordination failure. Detection fired within minutes; containment took over two days. That was far beyond the company's own internal target, one its security operations centre had been missing for months. A known weakness in administrative account structure, flagged repeatedly and never owned, let the attacker move laterally across the estate. Penetration test findings stayed inside the business units that commissioned them. Millions of records were compromised. Detection was in place. What was missing was a system connecting detection to decision to action.

AI widens the coordination gap

AI makes coordination debt more dangerous. Attackers are using AI to automate reconnaissance, improve social engineering, accelerate vulnerability discovery and scale attacks. At the same time, enterprises are connecting AI systems to valuable data, applications and workflows, creating new machine identities and expanding the attack surface.

The numbers reflect how unprepared most organizations are: 77% of mid-market companies lack the foundational security practices required to protect critical AI assets and cloud infrastructure, yet only 35% of technology leaders acknowledge that AI is outpacing their defenses.

The Five Eyes alliance[3] warned in 2026 that frontier AI is transforming offensive and defensive cyber capabilities on a timeline measured in "months, not years." Frontier models are lowering the cost and skill required to conduct sophisticated cyber operations at scale. Attacks are moving at machine speed. Most defenses are not.

What this means for leaders

For mid-market leaders, the implication is clear: cybersecurity can no longer be viewed as a collection of controls managed independently. As digital complexity grows, security effectiveness increasingly depends on how well technologies, processes and decision-making structures work together. Organizations that continue to scale security through addition alone risk increasing both cost and complexity without materially improving resilience. Those that reduce security debt and simplify coordination will be better positioned to defend against enterprise-scale threats while sustaining growth.

Different security model for the mid-market

Mid-market companies don't have to replicate every specialist team, overlapping control, global intelligence capability and 24-hour security operation used by the largest enterprises.

They also have a structural advantage that many large enterprises envy. Fewer legacy systems, shorter decision-making chains and a more concentrated technology estate mean security architectures can often be reshaped in months rather than years. A global bank may spend years modernizing an identity estate. A $1.5 billion manufacturer can often make the same strategic shift within a single planning cycle. That matters because, while design debt remains costly, mid-market companies are often better positioned to repay it before years of complexity accumulate around it.

Our experience suggests that the organizations escaping the cybersecurity scale trap are not necessarily spending more on security. They are simplifying how security is designed, operated and scaled.

The opportunity is to capitalize on that advantage through a model built around three principles: **own** the judgments only your business can make, **orchestrate** defenses so they act as one system, and **obtain** the scale you cannot afford to build.

Principle 1: Own the decisions only your business can make

No tool or external provider can tell you which operations are critical, how much disruption you can tolerate, or what must be restored first when an attack hits. Those are business judgments with security consequences.

Ownership starts with knowing what you have. Companies must understand their critical assets, data and processes before determining who should have access. As human and non-human identities multiply, the business must define access, privilege and accountability. Passwordless authentication, adaptive access, identity governance and just-in-time privilege can enforce those rules but cannot define them.

The same applies to governance and resilience. External specialists can advise, but leadership must define risk appetite, escalation thresholds and recovery priorities before a crisis.

Cimpress[4], the $3.7 billion mass-customization company, embedded security principles into its transformation decisions rather than adding them afterwards. As the company expanded through acquisitions and digital transformation, it adopted a zero trust architecture built around continuous verification, least privilege access and segmentation. This provided a scalable security foundation that could support growth without extensive redesign later.

Principle 2: Orchestrate your defenses to act as one system

As security capabilities accumulate, so do costs and coordination efforts that make them work together.

Identity, managed detection and response, exposure management, secure access, governance and resilience should form one continuous defensive system.

A risky login or unexpected privilege change should immediately trigger response across endpoints, cloud applications, SaaS platforms and the network edge.

Managed Extended Detection and Response (MxDR) connects signals across identity, endpoint, cloud and network environments so threats can be contained across technology boundaries. Continuous Threat Exposure Management (CTEM) moves exposures from discovery through remediation and verification. Governance feeds the same system, giving executives, boards and regulators a single, current view of risk.

AKD[5], an Australian structural timber producer, offers an example. Tools had accumulated over years, each solving a specific problem but never forming a coherent whole, and a small IT team absorbed the growing workload. Round-the-clock monitoring was essential but impossible to resource internally. After unifying identity, cloud, endpoint and data protection onto one platform, backed by continuous monitoring, AKD reported a 10% rise in its security score within three months and a 15% reduction in vulnerabilities, shifting from reacting to incidents to anticipating them.

Principle 3: Obtain the scale but keep the accountability

Some cyber capabilities depend on scale: 24-hour operations, intelligence across hundreds of threat groups, specialist incident response, cross-platform automation. Few mid-market organizations can afford to build any of that internally.

An integrated managed model gives mid-market firms access to enterprise-grade detection, intelligence and specialist skills without recreating the internal structure of a global security operation. AI-driven analytics correlate signals across technologies. Automated playbooks contain routine threats. Continuous exposure management tracks cloud services, APIs and internet-facing systems as they change.

The AKD[5] example also shows what this looks like in practice. Round-the-clock coverage was essential at its scale but impossible to resource internally, so it drew 24-hour detection and response from a managed provider rather than building a security operation of its own. Capability expanded without the operating structure expanding with it.

Prevention is not enough, recovery is the real test

The real test of security is what happens after a breach: can the company contain the impact, keep critical operations running, and recover with confidence?

Our research found nine in 10 mid-market companies struggle to achieve this. Resilience depends on decisions made long before a crisis: tested recovery runbooks, immutable records, clear escalation authority and a defined sequence for restoring systems. Leaders must know what cannot stop, even when parts of the technology environment are unavailable or untrusted.

Mid-market companies must own the judgments, orchestrate the defenses and obtain the scale while keeping accountability. That is how complexity becomes a control, not a liability.

The leadership imperative

For mid-market organizations, the challenge is no longer deciding whether to invest in cybersecurity. It is deciding how to scale security without scaling complexity. Organizations that continue adding controls, providers and processes without reducing security debt risk creating defenses that become harder to operate and harder to sustain. Those that own critical decisions, orchestrate capabilities as a single system and obtain scale where it matters can turn security into an enabler of growth rather than a constraint on it.

About the authors

Jason Lewkowicz is the Global Cyber Resilience and Defense lead at Accenture.

Amit Vasudeva is the Global Cybersecurity Lead for Scaling Businesses at Accenture.

Deepak Mathur is the Global Cyber Modernisation Lead at Accenture.

Yusof Seedat is the Global Cybersecurity Research lead at Accenture.

The authors would like to thank **Emily Thornton, Arlene Lehman** and **Gargi Chakrabarty** for their support and contributions.

References

This research in this report is based on analysis of the mid-market segment from **Accenture's 2025 State of Cybersecurity survey**, based on analysis of more than 1,600 mid-market organizations across 17 countries.

1. **Verizon Data Breach Investigations Report (DBIR) 2025**

2. **ConnectWise The State of SMB Cybersecurity in 2024**

3. **National Security Agency (NSA), Five Eyes Cyber Security Agencies Statement, June 2026**

4. **ISACA: Case Study: Building a Zero Trust Architecture to Support an Enterprise, 2021**

5. **Microsoft, AKD secures the backbone of an essential industry with Microsoft Defender and Entra, June 2026**

About Accenture

Accenture is a leading solutions and global professional services company that helps the world's leading enterprises reinvent by building their digital core and unleashing the power of AI to create value at speed across the enterprise, bringing together the talent of our approximately 786,000 people, our proprietary assets and platforms and deep ecosystem relationships. Our strategy is to be the reinvention partner of choice for our clients and to be the most AI-enabled, client-focused, great place to work in the world. Through our Reinvention Services we bring together our capabilities across strategy, consulting, technology, operations, Song and Industry X with our deep industry expertise to create and deliver solutions and services for our clients. Our purpose is to deliver on the promise of technology and human ingenuity and we measure our success by the 360° value we create for all our stakeholders. Visit us at accenture.com

About Accenture Research

Accenture Research creates thought leadership about the most pressing business issues organizations face. Combining innovative research techniques, such as data science-led analysis, with a deep understanding of industry and technology, our team of 300 researchers in 20 countries publish hundreds of reports, articles and points of view every year. We use generative AI in our research production process. Our research experts review and validate the generative AI outputs with traditional research methods where possible, applying Accenture's Responsible AI standards. Our thought-provoking research developed with world leading organizations helps our clients embrace change, create value and deliver on the power of technology and human ingenuity.