KATALYST

DIGITAL OPERATIONS PARTNER

2026 EDITION

2026 Katalyst Cybersecurity Executive Report

Operating with Intention in an Era of Rising Risk

Most mid-market organizations are running on a technology foundation that nobody fully owns. Built incrementally, managed reactively, held together by vendors with no single point of accountability.

In 2026, that model is no longer acceptable operationally, competitively, or from a risk perspective.

For mid-market executive and technology leaders.

$4.88M
avg breach cost
mid-market (IBM 2024)

60%+
of breaches via
compromised credentials

168
days avg to detect
a breach (IBM 2024)

40+
vendor integrations
avg mid-market org

EXECUTIVE LETTER

A Message From Our CEO

Something has shifted in the conversations I have with executive leaders. They are no longer asking whether cybersecurity matters. They are asking why it feels so hard to get it under control and what it will take to get ahead of it.

- **Security is an operational resilience issue**
- **Boards are asking different questions**
- **Compliance intensity is accelerating**
- **Growth and security are colliding**
- **Vendor sprawl is compounding exposure**
- **Internal bandwidth has reached its limit**

The organizations that solve this in 2026 carry a durable advantage forward. The ones that don't keep paying in downtime, compliance findings, staff burnout, and the deals they lose because they cannot demonstrate they are trustworthy stewards of the data entrusted to them.

Luke Johnson
CEO, Katalyst
Digital Operations Partner

The conversation in every boardroom has changed. Technology risk is no longer a footnote in the annual report. It is a standing agenda item in risk committee meetings across every industry and organizational size.

> *"The Digital Backbone must be intentional. It cannot be inherited, assembled by accident, or managed by whoever has time."*

What does that mean in practice? It means the infrastructure your organization depends on, the network, security controls, cloud environment, and the Microsoft 365 platform your people work in every day, needs to be owned, operated, and improved with the same discipline you apply to your core business.

Security is a discipline, not a purchase.
Winning organizations are not those with the most tools. They have the clearest accountability and the most consistent execution.

Compliance is a floor, not a ceiling.
Regulators, insurers, and clients are raising expectations faster than most organizations are raising their posture.

The co-managed model is how this gets solved.
Mid-market organizations cannot hire their way to security maturity. Embedded partnership with shared accountability is the answer.

Six Forces Reshaping Technology Leadership

The mid-market is experiencing a convergence of pressure that no single tool, vendor, or hire can absorb. These are six converging forces reshaping technology leadership in 2026.

01

Security Leadership Has Changed

68% of CISOs now report directly to the CEO or board, up from 47% three years ago. Technology risk is an executive accountability, not an IT function.

02

Third-Party Risk Expectations Are Increasing

Customers, partners, insurers, and vendors increasingly require organizations to demonstrate their security posture through questionnaires, security reviews, and documented controls. Trust is becoming a business requirement—not just a technical one.

03

Vendor Sprawl Is Getting Worse

The average mid-market organization manages 40+ vendor integrations. Each one is a potential attack surface, a compliance gap, and a budget line nobody fully owns.

04

Technology Teams Are Being Asked to Do More

Technology teams are balancing security, infrastructure modernization, AI adoption, compliance requirements, and day-to-day operations—all with limited time and resources. Strategic priorities increasingly compete with operational demands.

05

Security Is Becoming a Business Requirement

Customers, insurers, lenders, and business partners increasingly evaluate cybersecurity as part of purchasing, contracting, and risk management decisions. Demonstrating a mature security program is becoming a competitive advantage.

06

Growth and Security Are Colliding

New locations, acquisitions, remote workforce, and cloud migration all expand the attack surface. Organizations that grow without security architecture build risk into their foundation.

Connect. Protect. Operate.

One operating model. Three responsibilities. Complete accountability for everything your organization depends on.

01 CONNECT

Infrastructure and connectivity wherever your environment lives.

The mid-market is no longer on-premises only. Your organization may run workloads on-premises, in Azure, in AWS, in a colocation facility or all of the above. That hybrid reality is your Digital Backbone. It must be designed, managed, and optimized as one environment.

We help organizations decide what stays on-premises, what moves to the cloud, and what belongs in a hybrid model then build and operate the connectivity that ties it all together.

- **SD-WAN & Networking**
  Standardized. Monitored. Redundant.
- **Cloud Connectivity**
  Azure, AWS, hybrid environments
- **Branch & Remote Access**
  Secure access for every location
- **Managed Infrastructure**
  Continuously operated and improved

02 PROTECT

Security as an operating discipline not a product you buy once.

Threats don't stop at the firewall. They follow your data into cloud workloads, SaaS platforms, remote workforce, and hybrid infrastructure. We take accountability for your security posture across the full environment: enforced identity controls, behavioral threat detection, monitored endpoints, and continuous improvement.

The result is a security posture you can demonstrate to your board, auditors, clients, and regulators not just a list of tools you have purchased.

- **Identity & MFA**
  Enforced, not just enabled
- **EDR & Endpoint**
  Monitored, not just deployed
- **Email Security**
  Continuously tuned
- **MDR / vCISO**
  24/7 detection and advisory

03 OPERATE

Ongoing accountability for outcomes not just availability.

Showing up when something breaks is not the same as owning the outcome. Operate means continuous management of your full environment: helpdesk, infrastructure, cloud platforms, backup validation, and the Microsoft 365 environment your people work in every day.

A dedicated advisor drives your roadmap, keeps everyone aligned, and delivers quarterly reviews that show actual progress not just uptime reports and ticket counts.

- **Help Desk & Support**
  Responsive and accountable
- **Backup & DR**
  Tested, not just configured
- **Microsoft 365**
  Managed, optimized, secured
- **Advisory & QBRs**
  Roadmap, not just reporting

Connect. Protect. Operate. One model. Complete accountability.

The Numbers That Define This Moment

$4.88M

Average cost of a data breach for mid-market organizations

Mid-market organizations bear the same threat load as enterprises with a fraction of the resources to detect and respond.

60%+
of all breaches involve compromised credentials

168 days
avg time to detect a breach before containment

94%
of ransomware incidents now include data exfiltration

74%
of IT leaders spend majority of time on reactive work

30–50%
cyber insurance premium increase over three years

68%
of CISOs now report to CEO or board up from 47%

70%
of ransomware incidents now involve double-extortion tactics

52%
of organizations say cybersecurity staffing shortages increase operational risk

80%
of organizations experienced at least one identity-related security incident in the past year

The mid-market faces enterprise-level threats with SMB-level resources. That gap is structural and it requires a structural answer.

Not More IT. A Better Model.

The answer to mid-market security complexity is not hiring more people. It is building a smarter operating model.

The Co-Managed Model

What it looks like when it works.

Co-Managed Partnership

Your internal team owns strategy and priorities. Katalyst provides depth, bandwidth, and 24/7 coverage no mid-market team can sustain alone. Shared accountability. Owned outcome.

Embedded Engineering

Engineers embedded in your environment, familiar with your architecture, vendors, and roadmap. Execution without the overhead of hiring or training dedicated staff.

Strategic Advisory

A dedicated advisor who drives your roadmap, attends planning conversations, and brings outside perspective to inside problems. The guide, not just the technician.

Continuous Security Reporting

Monthly reporting with actionable insights. Quarterly business reviews showing actual posture movement. Leadership receives metrics, not just tickets.

Fewer Vendors, Deeper Relationships

One accountable partner replacing 3 to 5 fragmented vendors creates visibility, reduces cost, and eliminates gaps that form between disconnected providers.

The Positioning Shift

How high-performing organizations are reframing the question.

FROM	TO
Hire more IT staff IT talent is scarce, expensive, and leaves with institutional knowledge.	**Embedded co-managed partner** Shared accountability, continuous coverage, and operational ownership without the overhead of building a large internal security team.
Buy more tools Aging infrastructure, disconnected platforms, and overlapping tools create operational complexity, inconsistent patching, and growing security gaps.	**Strategic modernization** A modernized Digital Backbone creates standardized infrastructure, centralized visibility, supported systems, and stronger operational resilience across the organization.
React to incidents By the time you know about it, damage is already done. Reactive is expensive.	**Proactive monitoring** Standardized platforms, centralized visibility, and fully managed tools create a stronger and more measurable security posture.
Compliance as a project Audit prep is not a posture. It is a recurring scramble with diminishing returns.	**Compliance as a posture** High-performing organizations build operational discipline into the environment continuously instead of preparing for audits reactively.

You are the hero of your organization's story. Katalyst is your guide reducing risk, removing friction, and bringing clarity.

Operational Discipline Over Tool Accumulation.

The organizations pulling ahead are not spending more. They are operating better.

01
Consolidate Vendors

Fewer, deeper relationships replace sprawling vendor stacks. One accountable partner is more valuable than five vendors with overlapping scope and no shared accountability.

02
Standardize Platforms

Consistent security stack across every location. Standardization is the prerequisite for monitoring, response, and audit readiness, not just operational efficiency.

03
Move from Reactive to Proactive

24/7 monitoring means threats are detected before they disrupt operations. The question shifts from what happened to what did we catch and contain.

04
Embed 24/7 Oversight

Attackers do not work business hours. High-performing organizations ensure continuous coverage, not just coverage when the internal team happens to be in the office.

05
Measure Security Maturity

Security posture is measured, tracked, and reported to leadership. Quarterly reviews show actual movement, not just a list of tools purchased or tickets closed.

06
Harden Identity First

MFA is enforced, not just enabled. Access rights are reviewed quarterly. Privileged accounts are governed. Identity is treated as the perimeter it has become in 2026.

The difference between organizations that recover quickly and those that don't is not the size of the incident. It is the depth of the preparation.

Complexity Is Not Free.

Fragmentation is not a technology problem. It is a business problem with real financial, operational, and reputational costs.

> *"We were reacting to issues instead of preventing them. The cost was not just financial it was every strategic initiative that never got started."*
> Healthcare IT Leader

Compliance Fines & Findings

Undocumented controls, inconsistent MFA, and missed audit requirements create findings ranging from remediation mandates to formal fines. Average HIPAA fine: $1.2M. Average FTC Safeguards violation: $50K+

Downtime Cost

Average IT downtime cost for mid-market organizations: $8,600 per hour. For ransomware events with 20+ day recovery timelines, that arithmetic is devastating, with lost production, missed commitments, and delayed billing cycles.

Talent Drain & Burnout

Reactive environments burn through IT talent. When teams spend 74% of their time firefighting, they stop developing and eventually leave. Replacement cost for an experienced IT engineer: $30K-60K in recruiting alone.

Vendor Misalignment

40+ vendor relationships with no single owner. Each renewal, each incident, each integration question requires coordination that consumes time and introduces risk nobody is tracking.

Shadow IT Exposure

When IT cannot serve the business fast enough, the business self-serves. Unauthorized SaaS, personal cloud storage, and shadow infrastructure create exposure nobody monitors or owns.

The fix: every vendor in scope. Every access path documented. One accountable partner who owns the full picture not just their piece of it.

AI Is Accelerating Operational Risk

AI-Generated Phishing

AI-enhanced phishing campaigns are becoming more convincing, personalized, and difficult to detect.

Attackers use AI to craft messages that mimic trusted vendors, internal conversations, and executive communications at a scale that traditional awareness methods struggle to keep up with. Technical controls remain essential, but ongoing security awareness training is becoming equally important.

Deepfake Impersonation

AI-generated voice and video are making executive impersonation easier than ever.

Organizations are reporting fraudulent wire transfers, unauthorized system access, and credential theft resulting from increasingly realistic AI-generated voice and video impersonation. Verification procedures and identity controls are becoming critical safeguards.

AI-Powered Vulnerability Discovery

AI is dramatically reducing the time between finding vulnerabilities and exploiting them.

New AI-powered vulnerability discovery tools can identify weaknesses and generate exploit paths in hours instead of weeks. Organizations relying on periodic scans or inconsistent patching cycles are increasingly at risk of falling behind.

AI isn't just creating new attacks—it's dramatically accelerating how quickly attackers can find and exploit existing weaknesses.

Recent demonstrations from AI-powered vulnerability discovery platforms such as Mythos show that vulnerability discovery and exploit development can now happen in hours instead of weeks. Organizations need an ongoing vulnerability management program to continuously identify, prioritize, and remediate risk before attackers can take advantage.

The Risk Is Operational, Financial, and Immediate

AI is increasing the speed, scale, and sophistication of cyber threats across every industry. Organizations are seeing more AI-generated phishing, executive impersonation, credential theft, ransomware, and AI-powered vulnerability discovery. At the same time, employees are increasingly using public AI tools without understanding the security implications, creating new avenues for data exposure. Organizations that combine security awareness training, secure access controls, centralized visibility, behavioral monitoring, and a mature vulnerability management program are significantly better positioned to detect and reduce risk before attacks become business-level incidents.

Security Awareness Training

Build a security-aware culture through ongoing phishing simulations, end-user education, and reporting workflows that help employees recognize evolving AI-powered attacks.

Secure Access (SASE)

Protect sensitive information by applying consistent access policies, web filtering, and data controls across users, devices, and cloud applications—reducing risk from Shadow AI and data exposure.

Managed Security Services

Behavioral monitoring, anomaly detection, and centralized visibility across identity, email, endpoints, and infrastructure enable faster detection and response before incidents escalate.

Vulnerability Management

Continuously identify, prioritize, and remediate vulnerabilities across your environment to reduce the growing window of exposure created by AI-powered discovery tools.

VOICE OF THE CUSTOMER

In Their Own Words.

Across financial services, healthcare, manufacturing, and government the same challenges surface before the relationship. These are the conversations that started it.

"I would get emails at 2 or 3 in the morning with things Rob is fixing. When I see them the next day I think: I am glad somebody did not sleep last night, because I slept great. They are one of the top five vendors I have worked with in my 28-year career."

Steve Yates
CIO, MB Haynes

"Our first experience with Katalyst was when we called them for help when our phone system crashed. Our previous vendor was not responding. Katalyst said they could get someone to help us right away, and they delivered."

Rich Rumney
Network Engineer, Spero Financial

"Katalyst has been very collaborative, inquisitive, and willing to lean in. They asked the right questions and worked with our existing processes."

Damon Sipe
CTO, Engage FI

"I have been impressed with the partnership Katalyst has provided since day one. When our network outage hit, their team jumped in with experience and keen troubleshooting skills, proving they are a resource I can count on."

SVP of IT Operations
$2B+ Mid-Atlantic Credit Union

"Katalyst is there when you need them and things get handled. The team knows the environment like the back of their hand. When you find a company that has the expertise and the ability to provide seamless, continuum of service you keep that."

Nancy Warren
IT Director, HVO

"Katalyst enables my team to focus on direct business activities with our internal partners, knowing that security is being handled, monitored, and managed."

Scott Anzilotti
Senior IT Director, Magellan Aviation Group

VOICE OF THE CUSTOMER

The Outcomes.

Same partner. Different industries. Consistent results.

36%	40%	<4 hr	9 yr	24/7
cost reduction	fewer helpdesk tickets	recovery certainty	active partnership	operational coverage
Spero Financial	6-office SD-WAN rollout	Regional Credit Union	Graystone Eye	AZEK, 24+ sites

"What I appreciate most is trust. I know Katalyst is invested in our journey, and that makes them more than a vendor they are a partner I can count on."

Michelle Kasson
VP & CIO, The AZEK Company

"The implementation process was well-organized, starting with a full assessment of our existing infrastructure. Katalyst helped us design a standardized firewall policy and migrate to new hardware with minimal downtime."

Tim Jeffries
Lead System Engineer, Magellan Aviation

"From start to finish, Katalyst goes the extra mile to make sure you are taken care of."

Jimmy Dickson
VP of Information Security, All South FCU

"Katalyst has been flexible, even addressing things outside of contract terms. Their engineers also take the time to learn and master new technologies when needed."

Matt Bosch
Senior Network Engineer, Live Oak Bank

"It has made a huge difference. It allowed us to do our normal jobs instead of worrying about security on a moment to moment basis."

Craig Barnes
CIO, Dick Smith Automotive

"There was no sales team looking for opportunities to take advantage of our vulnerable situation just a partner willing to support us."

Ted Bayack
Director of IT, Graystone Eye

A Practical Roadmap for 2026

1 Immediate

- **Review Identity and Access Management (IAM)**

  Assess how identities are managed across users, devices, applications, and remote access. Verify MFA is consistently enforced, review privileged access, and identify outdated accounts or excessive permissions that increase risk.

- **Validate backup testing documentation**

  Pull the last restore test record. Confirm it covers all critical systems. If it is more than 90 days old, or you can't find it, that is the first thing to fix.

- **Assess third-party and vendor risk management program**

  Map which vendors have active access to your systems and data. Identify which relationships lack a formal security review or access policy.

2 Mid-Term

- **Implement a Vulnerability Management Program**

  Establish a centralized process to continuously identify, prioritize, and remediate vulnerabilities across servers, endpoints, network devices, and cloud environments. Focus on risk-based remediation rather than one-time scanning.

- **Implement centralized monitoring**

  Establish centralized visibility across the full environment from a single platform. Every alert should have an owner, an escalation path, and a documented response.

- **Formalize incident response coordination**

  Document who does what, in what order, when an incident occurs across IT, leadership, legal, and operational stakeholders. Practice it before you need it.

3 Long-Term

- **Establish Digital Backbone ownership and governance**

  Define clear ownership for Connect, Protect, and Operate across your organization. Document accountability, performance metrics, and the escalation path to leadership.

- **Continuously align security investments with operational and business priorities**

  Establish an ongoing process to evaluate security investments against business goals, operational risk, compliance requirements, and long-term initiatives. Regular reviews help ensure priorities evolve alongside the organization rather than remaining static.

- **Introduce structured executive reporting and accountability**

  Leadership cannot improve what they cannot clearly measure. Quarterly posture reports that show movement, not just activity, give decision-makers what they need.

Ready to strengthen your digital backbone? Schedule a conversation with Katalyst.

KATALYST

DIGITAL OPERATIONS PARTNER

In 2026, cybersecurity is not about more tools. It is about operating your Digital Backbone with intention.

The organizations that figure this out in 2026 carry a durable advantage forward. The ones that don't keep paying in downtime, in compliance findings, in staff burnout, and in the opportunities they miss because they cannot demonstrate they are trustworthy stewards of the data entrusted to them.

Assess.
Benchmark your full environment across Connect, Protect, and Operate.

Transform.
Build and execute a prioritized roadmap. Plans don't sit on a shelf.

Manage.
Ongoing ownership, visibility, and continuous improvement 24/7/365.

katalystng.com
704-790-4440
Charlotte, NC | Spartanburg, SC | Wilmington, NC

SOURCES & REFERENCES

1 IBM Cost of a Data Breach Report, 2024
2 Sophos State of Ransomware Report, 2025
3 Verizon Data Breach Investigations Report, 2025
4 Gartner CISO Reporting Structure Analysis, 2025
5 Forrester State of IT Operations, 2025
6 Cyber Insurance Market Research, 2025
7 AI Phishing & Threat Analysis, 2025
8 Katalyst Digital Backbone Readiness Benchmark, 2025
9 HHS Office for Civil Rights Breach Portal, 2025

Digital Backbone Assessment
Benchmark your environment across Connect, Protect, and Operate. Understand your gaps in terms your leadership team can act on.