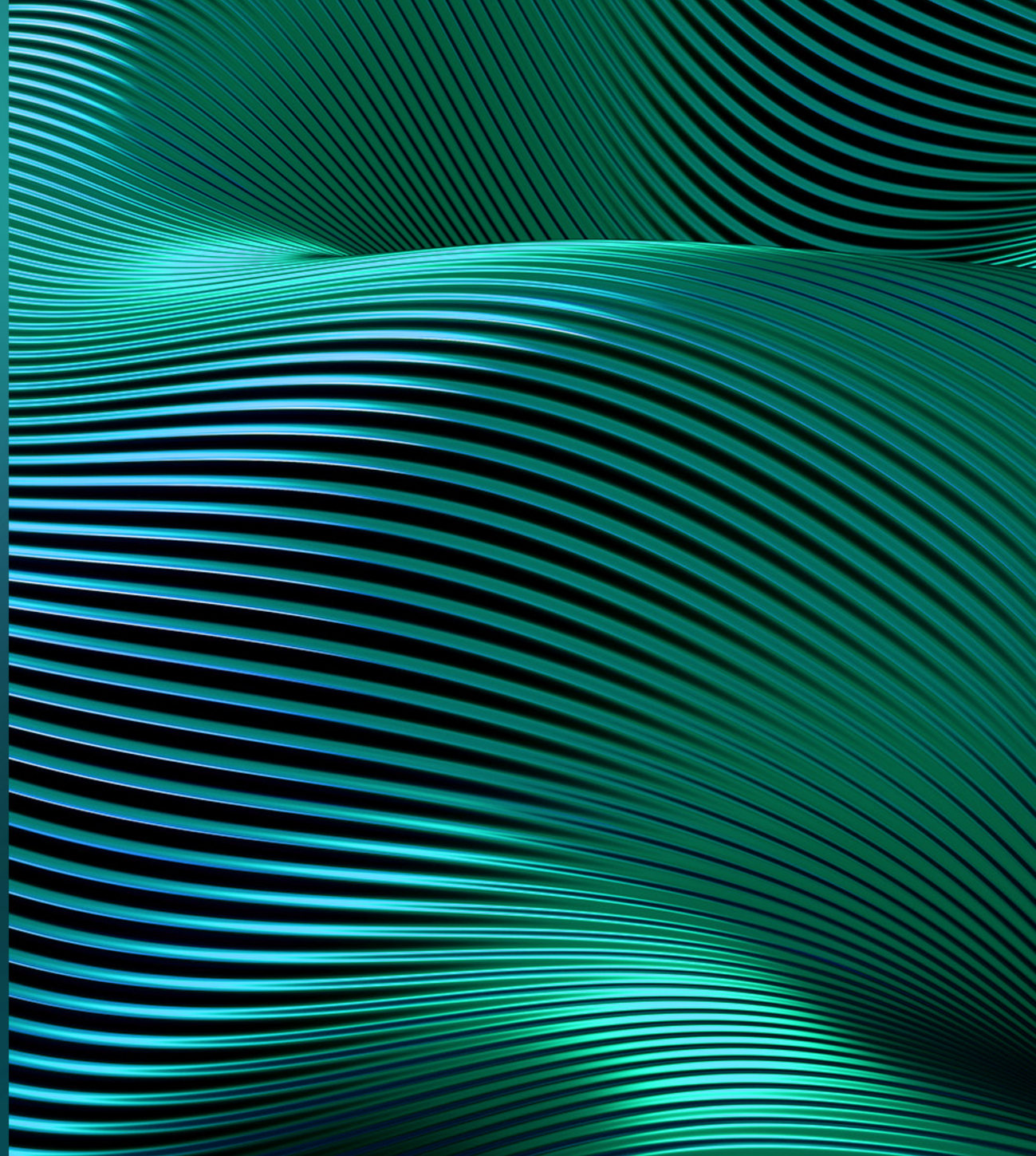
MAKING THE CASE TO THE BOARD:

Why cyber readiness can't wait

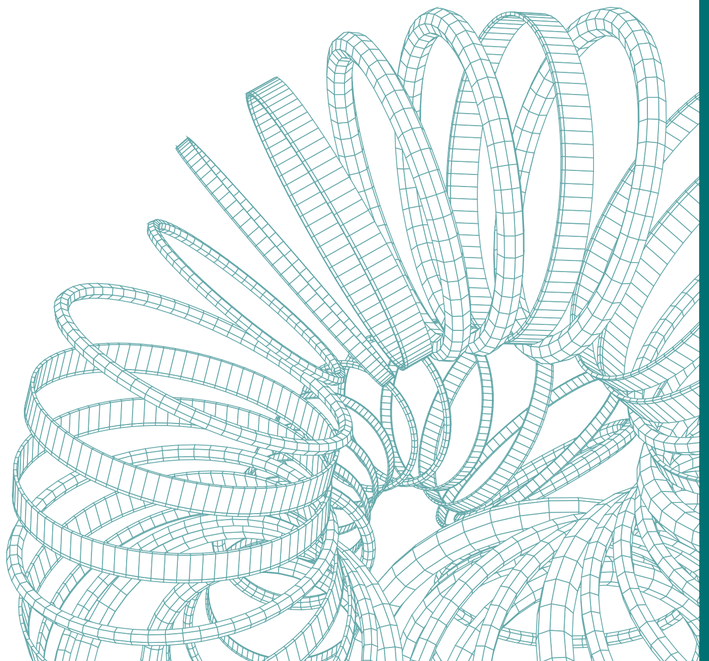
Equipping IT and security leaders to secure executive buy-in for cyber resilience and risk readiness

unisys



Executive summary

Investment in cybersecurity continues to rise, yet most organizations remain reactive, responding to threats after impact rather than preventing them. Security leaders can either secure board approval for strategic resilience programs or accept the competitive disadvantage that comes from extended breach detection times, mounting costs and operational disruption.



YOUR MESSAGE TO THE BOARD

The gap

Most organizations respond to threats after impact, extending breach detection times and multiplying costs.

The root cause

Fragmented, tool-heavy security initiatives fail to deliver proactive protection. Legacy perimeter defenses leave gaps that modern distributed environments expose.

The opportunity

Organizations that adopt an integrated, intelligence-driven approach to resilience, grounded in Secure by Design principles, position themselves for business continuity and a competitive advantage.

The numbers tell the story: Data we'll explore in this guide

85% **of organizations operate with reactive cybersecurity postures,** revealing widespread vulnerability and delayed threat response. ↗

Organizations will be measured by how quickly they recover, making equal investment in rapid recovery and business continuity a defining competitive advantage. ↗

14% **of organizations are prepared for post-quantum cryptography threats,** leaving the majority exposed to emerging encryption-breaking technologies. ↗

What this guide provides

Cyber resilience looks different for every organization. Your industry, risk appetite, regulatory environment and security maturity all shape the right approach. The practices described here are examples drawn from actual security transformations — use them as a starting point, not a prescription. This guide will equip IT and security leaders with the information they need to secure executive buy-in for cyber resilience and risk readiness.

Use the home button located at top right of each page to return to the table of contents.

01

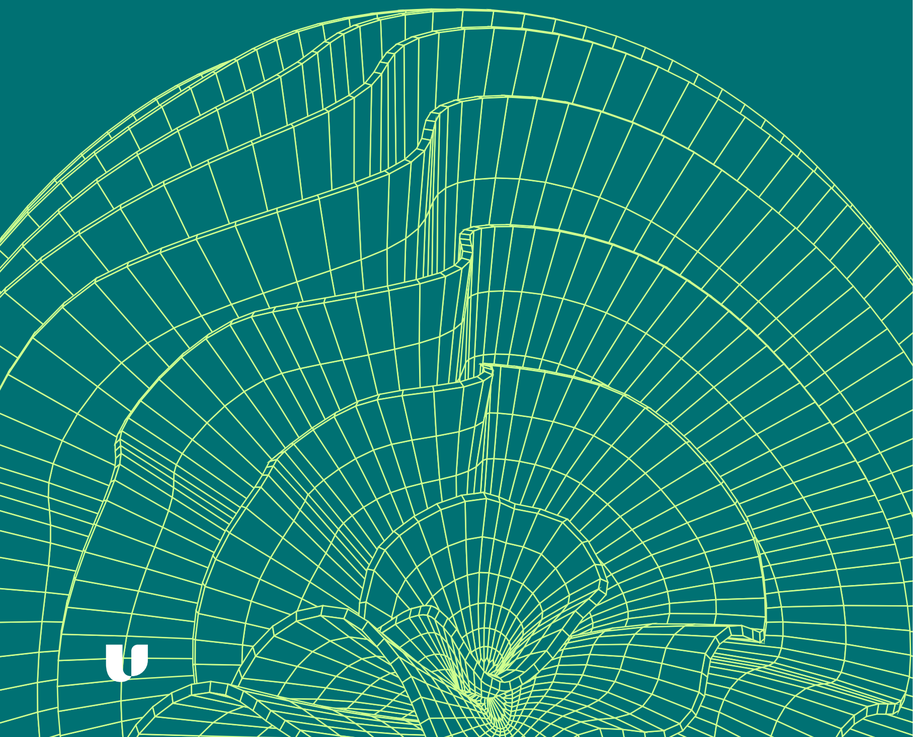
THE QUESTIONS

Three questions your board is asking

Boards are asking tougher questions about cybersecurity investments. They want to understand not just what you're spending but whether your approach keeps pace with evolving threats and enables business objectives. Here are three questions that matter along with data-backed answers that will resonate.

QUESTION 1

Is our cybersecurity approach too reactive? Should it be more proactive?



The numbers reveal the most common answer to that question.

85% of organizations describe their cybersecurity posture as reactive. ↗

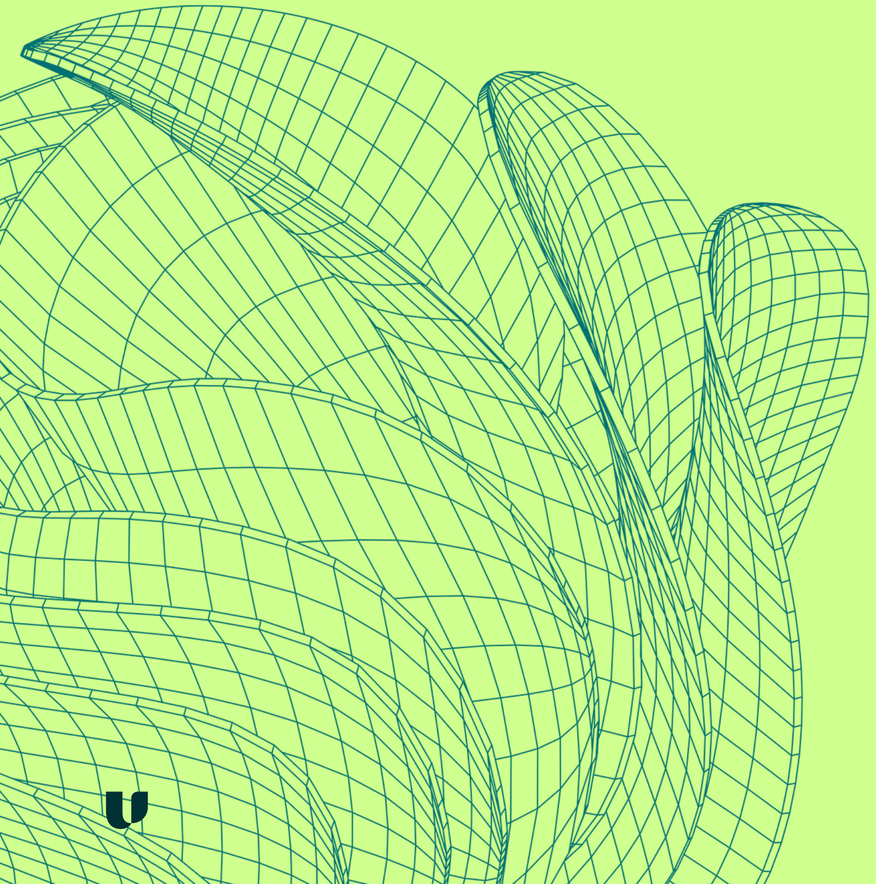
Organizations remain reactive because legacy security architectures were built for perimeter defense, not modern distributed environments. Fragmented tools that don't share intelligence create information gaps. Manual processes slow response times. As a result, threats are often detected days or weeks after the initial compromise, extending the breach's impact and multiplying costs.

What's at stake

- Financial impact: Up to $500,000 per hour in breach downtime costs ↗
- Operational disruption: Critical business processes halted during incidents
- Reputational damage: Customer trust eroded by breaches and slow response
- Regulatory exposure: Non-compliance penalties for inadequate security postures

QUESTION 2

Are we adequately prepared for emerging threats?



The preparedness gap is evident in three key statistics.

14% Only 14% of organizations are prepared for post-quantum cryptography threats. ↗

62% 62% are adopting or planning to adopt Zero Trust models.

43% Only 43% have implemented AI-based cybersecurity measures. ↗

The gap between intent and implementation leaves organizations exposed.

Organizations face converging threats: quantum computing that could break current encryption, AI-powered attacks that evolve faster than human response and sophisticated adversaries exploiting the gap between security planning and actual implementation.

When security infrastructure *is* modernized and proactive:

Continuous threat exposure management identifies vulnerabilities before exploitation.

AI-based detection can begin to respond to threats automatically.

Post-quantum cryptography protections are implemented before quantum threats materialize.

QUESTION 3

How do we shift security from a cost center to a business enabler?

Organizations often default to viewing security as a cost center because there is no unified, end-to-end security vision integrated across the digital enterprise. Without a clear strategy, consistent execution and defined approach to measuring return on security investment, security efforts appear fragmented and the value they generate remains invisible.

What's blocking value

- Fragmented security tools that don't integrate or share intelligence
- Manual processes that slow incident response and drain resources
- Lack of visibility into the whole attack surface and exposure risks
- Security architectures built for perimeter defense in a cloud-first world

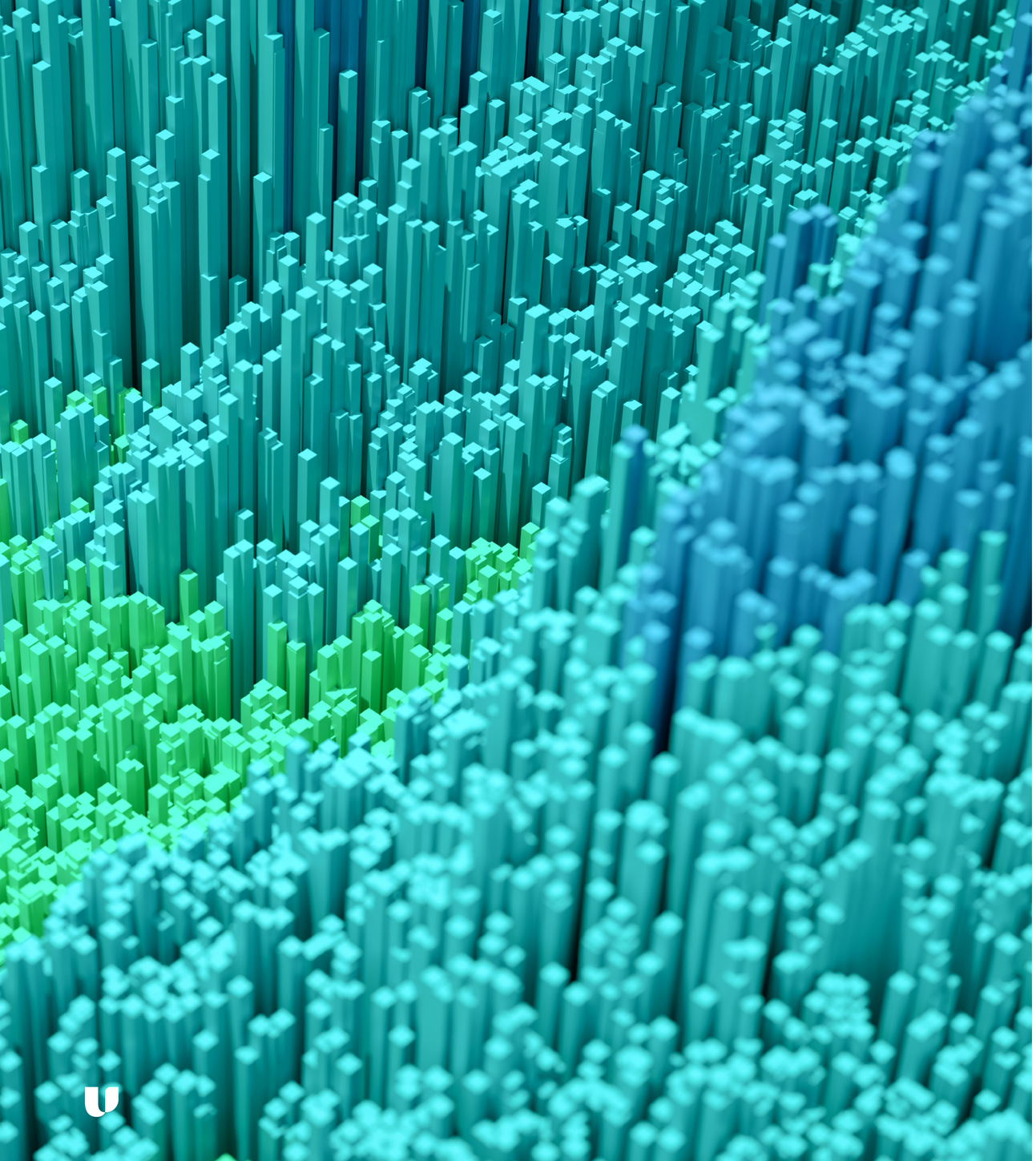
A Secure by Design foundation, combined with integrated security, enables business agility, accelerates digital transformation and protects revenue-generating operations. Organizations that invest strategically can operate confidently in digital markets and maintain continuity that competitors cannot.

02

THE FRAMEWORK

Show boards what they care about most

With their questions answered, you can now translate cybersecurity solutions into the business outcomes your board prioritizes. This framework helps you speak their language by connecting initiatives to financial protection, risk management, business continuity and competitive positioning.



Boards prioritize business outcomes over technical specifications. Frame cybersecurity around what matters most to them:

Financial discipline

Measurable ROI through proactive defense, cost control and regulatory confidence

Risk and resilience

Secure, compliant operations that sustain uptime and limit exposure

Growth enablement

Cyber-ready foundation supporting digital innovation and business agility

Competitive positioning

Trusted, resilient brand reputation built on proven security leadership

Translating security into board language

The three questions your board is asking map directly to the actions, outcomes and capabilities that close the gap between security investment and business value. The table below shows what each priority looks like in practice — and how Unisys can help deliver it.

Board priority	Security action	Business impact	How a partner like Unisys can help
Cost-efficiency	Shift from reactive to proactive security posture	Reduce breach downtime from $500K/hour to minimal disruption	**Managed detection and response, continuous threat exposure management**
Resilience and compliance	Implement cyber recovery and business continuity strategies	Accelerate recovery from days to hours, maintain operations	**Cyber recovery, security managed services**
Growth/Innovation enablement	Advance Zero Trust principles continuously guided by risk priorities and business needs	Enable secure cloud adoption, protect distributed operations	**Digital identity and access management**
Competitive positioning	Prepare for emerging threats (quantum, AI-powered attacks)	Future-proof security, demonstrate leadership, build customer confidence	**Post-quantum cryptography, security transformation**

Real results: What value are organizations realizing with cybersecurity readiness and resilience?

The following examples show how Unisys has helped organizations across industries turn security modernization into measurable business value.

Organization	What we did	What they gained
Benjamin Moore	Modernized cloud infrastructure with managed detection and response, unified threat monitoring and 24/7 protection	Secured operations and IP while reducing breach exposure
Ensuring global food supplies	Deployed Continuous Threat Exposure Management, 24/7 monitoring and SASE protection across 40+ countries	Continuous threat management across a complex global operation
Queensland Transport and Main Roads	Secured driver's licenses using smart biometrics and cloud solutions	Protected citizen data across 5 million records and strengthened digital resilience
Fortifying financial data security	Modernized data protection with Cyber Recovery and Zero Trust backup	Faster recovery, reduced costs and minimized downtime
U.S. Public School System	Implemented Cyber Recovery with AI monitoring to detect ransomware and protect backups	Safeguarded student data and enabled rapid, secure recovery
Global Biotech Leader	Strengthened cyber resilience with cloud, AI and Zero Trust solutions across global sites	Enhanced data security and compliance at scale

03

THE PATHWAYS

Cybersecurity pathways and solutions

Discussing board priorities was the first step. Now you can show the board how specific security capabilities deliver those outcomes.

Security Managed Services

What it addresses

Organizations under pressure to protect infrastructure, applications and data while managing increasingly complex security environments and ensuring regulatory compliance

Key features

- 24/7 security operations with continuous threat monitoring, detection and rapid incident response
- AI-driven analytics and automation workflows integrated with leading tools like Microsoft Sentinel, Defender and CrowdStrike
- Vendor-neutral approach with industry-specific overlays for financial services, higher education, public sector and manufacturing
- Integrated security delivery across four pillars: Detect (AI-enhanced monitoring), Protect (layered defense), Respond (rapid protocols) and Govern (compliance and advisory)

Continuous Threat Exposure Management

What it addresses

The challenge of proactively and continuously identifying, assessing, prioritizing and mitigating cyber threats across an organization's entire attack surface

Key features

- Attack surface discovery with an actual adversary perspective
- Unified vulnerability management and mitigation
- Threat intelligence to identify and address emerging threats
- Continuous penetration testing for real-time defense assessment

Managed Detection and Response

What it addresses

The need for 24/7 monitoring, rapid threat detection and immediate response to minimize breach impact and reduce the $500K/hour downtime cost

Key features

- Security monitoring by expert analysts
- Threat detection, event enrichment and alerting
- Immediate incident response that contains threats before they spread
- Integration with existing security tools for comprehensive visibility

Secure Network Access

What it addresses

The need for robust protection to the enterprise network that powers critical operations and safeguards valuable data residing in the cloud or on-premises

Key features

- Microsegmentation to fortify your network with close-range defense
- Identity-centric access controls that verify every user, device and application
- Managed services for Secure Access Service Edge (SASE)
- Zero Trust network access for network, application and data access security
- Managed SD-WAN tailored to your business needs

Digital Identity and Access Management

What it addresses

Managing user identities, access privileges and authentication across complex, distributed environments

Key features

- Maturity assessment of the current state of your identity and access management (IAM) controls and a roadmap for the future
- Passwordless and single sign-on for a modern user experience
- Centralized identity governance across all systems
- Holistic approach encompassing design, architecture and implementation services

Cyber Recovery

What it addresses

Restoring critical operations quickly after cyber attacks to maintain business continuity

Key features

- Isolated, immutable backups
- Rapid recovery protocols that restore systems in hours
- Regular testing and validation of recovery procedures
- Integration with business continuity planning

Post-Quantum Cryptography

What it addresses

The emerging threat of quantum computing that could break current encryption methods

Key features

- Assessment of current cryptographic implementations
- Migration planning for post-quantum standards
- Hybrid approaches that maintain current security while adding quantum resistance
- Crypto agility for rapid algorithm updates

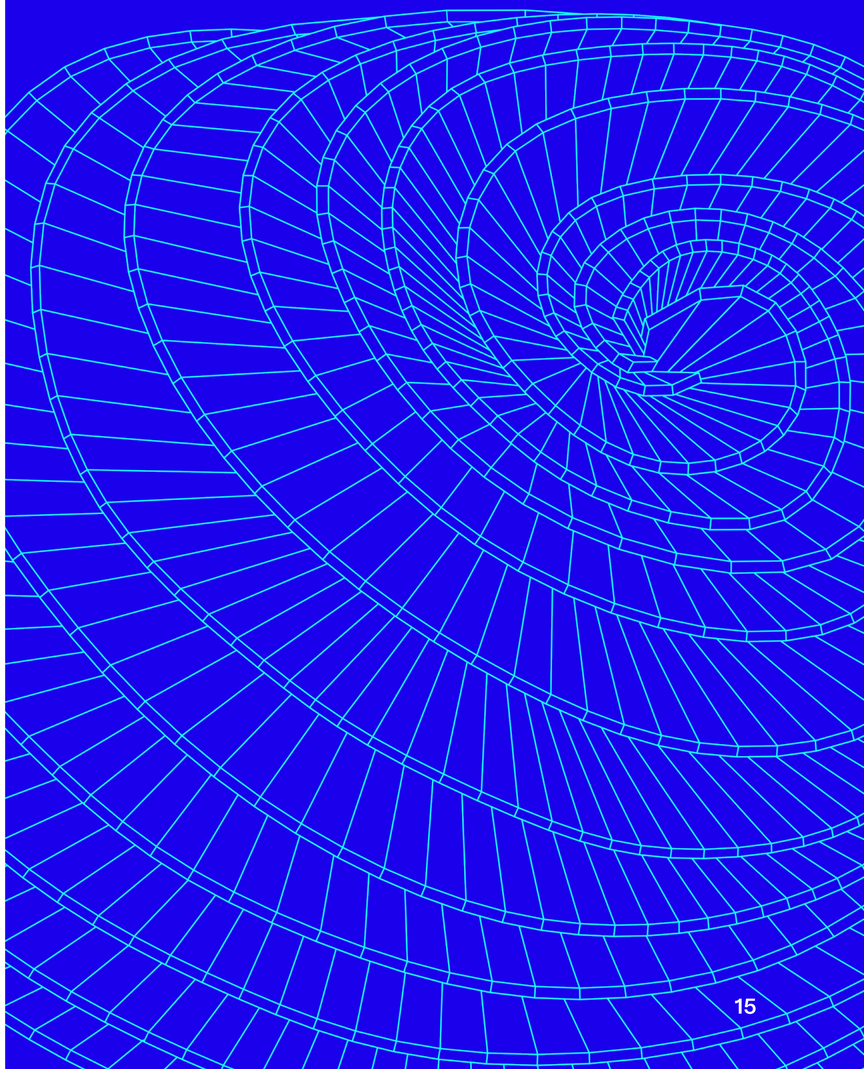
Security governance and management

What it addresses

Helping govern, maintain and protect critical assets, keeping them secure, up to date and compliant

Key features

- Serves as an extension of the CISO (Chief information security officer) team
- Comprehensive assessment of current security capabilities and gaps
- Strategic roadmap development aligned to business objectives
- Capability building and team enablement

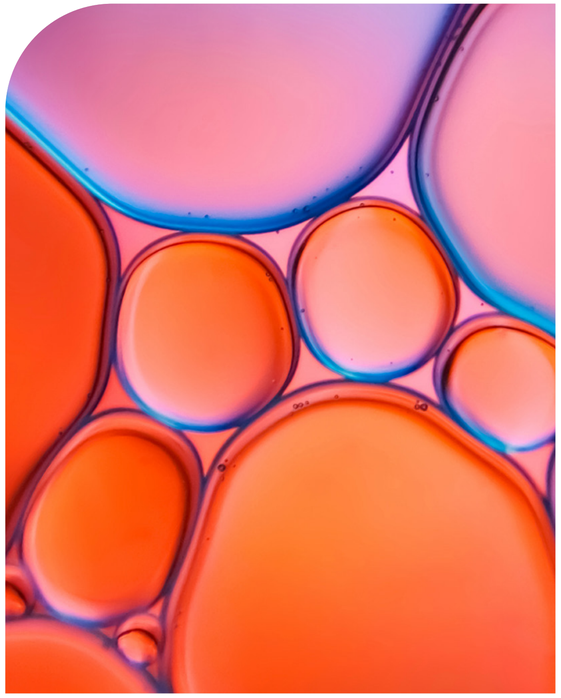


04

THE ASK

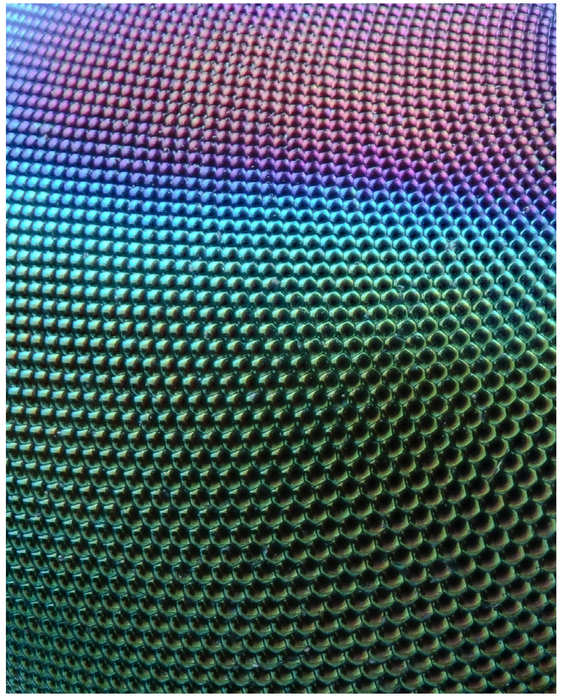
What IT and security leaders need from the board

You've demonstrated the problem, quantified the opportunity and outlined the solution pathways. Now it's time to be clear about what you need from the board to move forward.



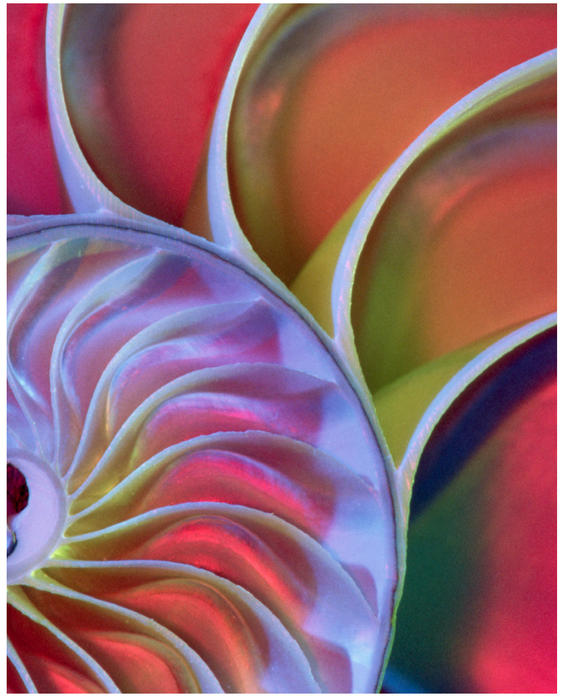
Budget approval for cybersecurity resilience

Funding for prioritized security initiatives with measurable ROI, from managed detection and response to Zero Trust implementation



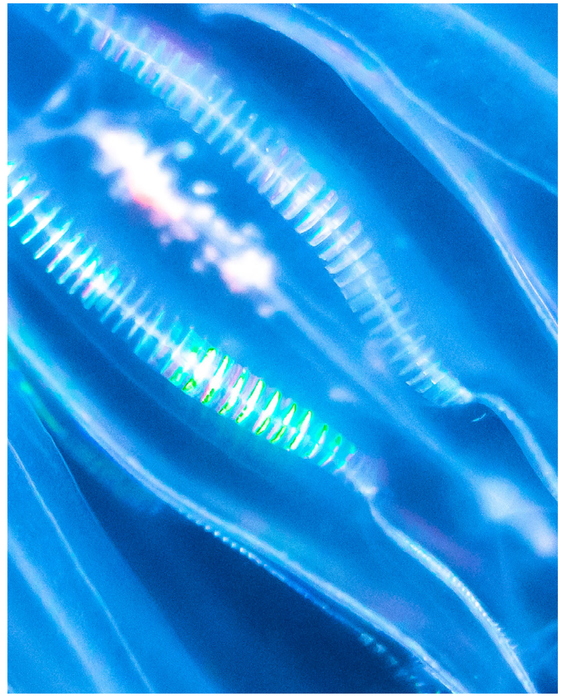
Endorsement for proactive security operations

Support to transition from reactive defenses to continuous threat exposure management and AI-driven monitoring



Strategic alignment beyond IT execution

Executive sponsorship to embed Secure by Design principles into enterprise strategy, governance and risk management



Investment in emerging threat readiness

Commitment to prepare for quantum and AI-powered threats, bridging the gap between today's 14% of organizations that are quantum-ready ↗ and the 62% still planning Zero Trust adoption ↗

05

THE PAYOFF

What business outcomes boards can expect

Here’s what the board can expect in return for its investment. These outcomes demonstrate how cybersecurity modernization delivers measurable value, protecting revenue, strengthening resilience and positioning the organization as a trusted market leader.

Operational resilience and financial protection

Accelerated detection and response reduce the impact of breaches and downtime. Equally important: When a breach occurs, how fast you recover determines how much it costs you.

- Faster mean time to detect (MTTD): from days to hours
- Faster mean time to respond (MTTR): from hours to minutes
- 24/7 monitoring and response without expanding internal teams
- Recovery from cyber incidents in hours instead of days
- Immutable offline backups and clean-room rebuild capabilities that restore operations without paying extortion demands
- Cross-functional playbooks covering IT, security, legal, communications and operations that reduce chaos and reputational damage when incidents occur

Board-level value

Reduces the $500K-per-hour downtime risk through faster response, continuous monitoring and rehearsed recovery capabilities. Customers and regulators increasingly ask how quickly and transparently you recovered, not whether you were breached. Organizations that demonstrate recovery readiness gain measurable advantages in customer trust, insurance rates and regulatory relationships. It helps drive strategic security transformation for agility and growth.

Proactive defense and business agility

Organizations can shift from reactive to proactive protection through integrated architecture and automation. But protection alone is no longer enough. Boards must budget equally for recovery as they do for prevention.

- Unified security fabric replacing fragmented tools and manual processes
- Improved team productivity and efficiency through AI-driven workflows
- Balanced resilience portfolios that fund both prevention and rapid recovery equally
- Network segmentation and access controls that limit how far a breach can spread
- Enhanced compliance through continuous governance and audit readiness, with recovery SLAs as board-level metrics alongside prevention metrics
- Secure enablement of digital transformation and cloud initiatives

Board-level value

Moves the organization from the 85% reactive majority to proactive security leadership. An "assume breach" posture backed by rehearsed recovery, immutable backups and pre-negotiated crisis capabilities means the organization is prepared for the inevitable, not just the possible. It enables secure business agility, regulatory confidence and measurable resilience in the face of emerging threats.

06

THE ROADMAP

Next steps for engaging with cyber resilience partners and building your roadmap

Achieving these outcomes requires the right partner — one with proven expertise, global scale and a history of protecting mission-critical operations.

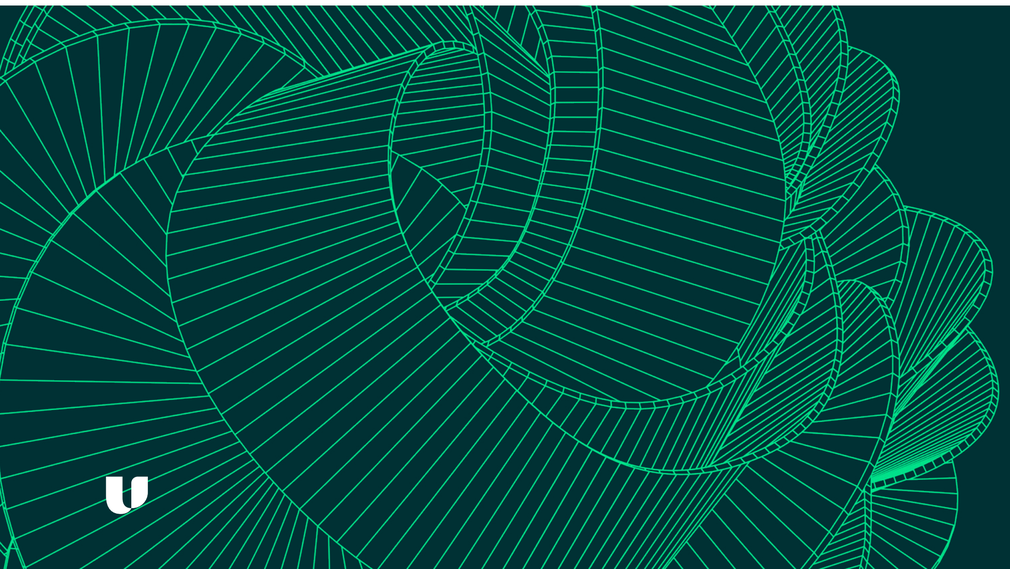
Unisys helps organizations worldwide strengthen security, reduce risk and sustain business continuity. With decades of experience across highly regulated industries and 24/7 security operations centers, we guide enterprises through every stage of their cybersecurity transformation with:

Unbiased guidance: Recommendations that integrate seamlessly with your existing technology investments. Our experts align strategy to business outcomes, not to specific tools.

Proven methodologies: Structured, repeatable frameworks that unify prevention, detection, response and recovery. Our approach ensures measurable resilience while maintaining compliance at every step.

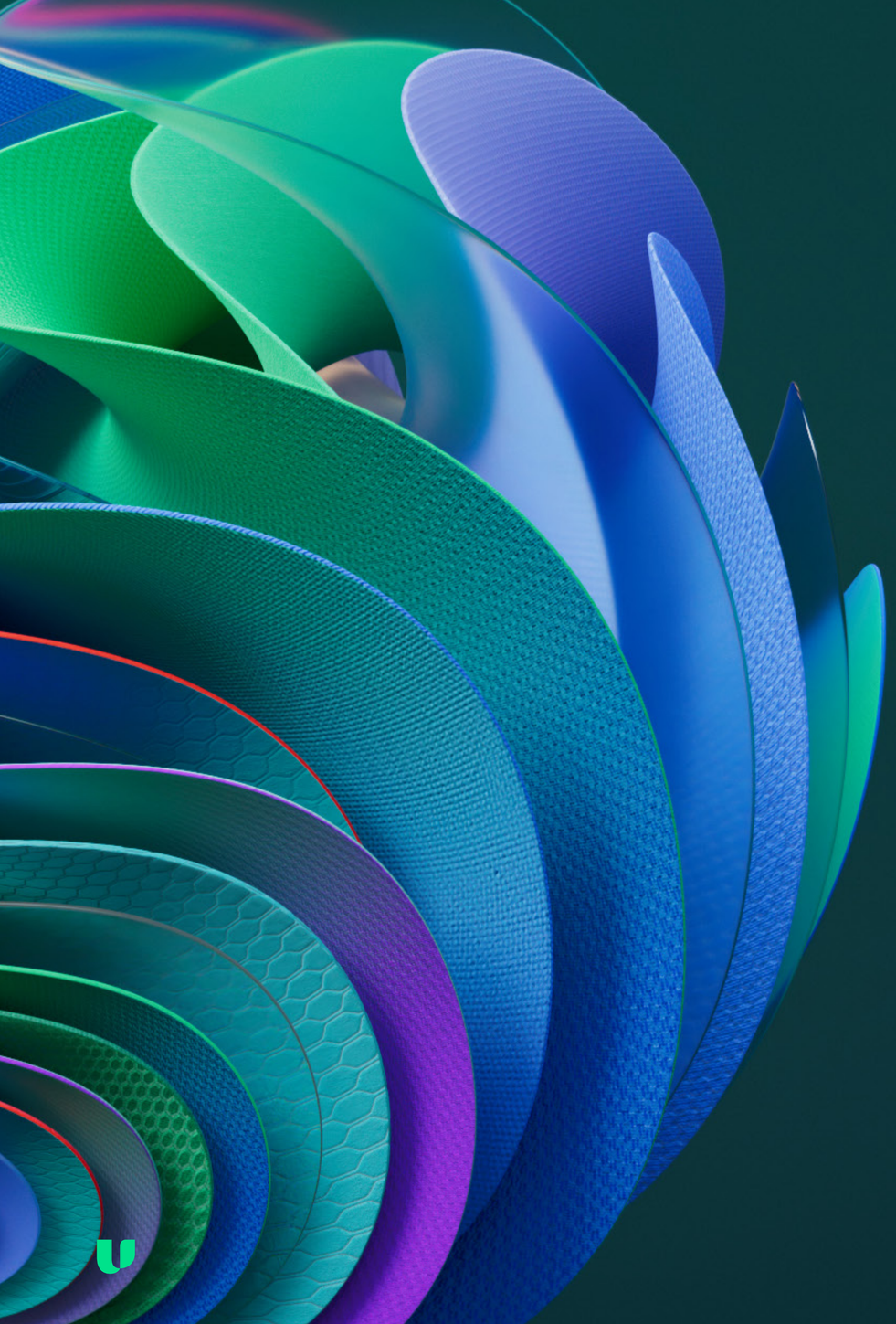
Security embedded at every layer: From infrastructure to identity, we design solutions that integrate security into every platform, process and service delivery model.

Solutions tailored to your board's priorities: Whether you need comprehensive security transformation, managed services or targeted programs like Zero Trust or cyber recovery, Unisys delivers outcomes aligned with your organization's risk tolerance, budget and growth strategy.



TAKE ACTION NOW

Cyber threats are evolving faster than most organizations can adapt. Those who act decisively — modernizing defenses, embedding security into business strategy and preparing for next-generation threats — will protect more than data; they'll protect trust, reputation and growth.



Ready to make your case?

Visit Unisys.com/cyber to learn more or schedule a cyber readiness assessment.

We'll help you:

- → Identify your highest-priority security risks and opportunities
- → Build a business case that resonates with your board
- → Develop a roadmap that delivers measurable resilience and confidence at every phase

Appendix

- Unisys Cloud Insights 2025: From Complexity to Clarity: Modernizing Cloud and IT for What Comes Next
- Unisys IT Insights Report 2026
- Enterprise Cyber Resilience Strategies guide
- **Solution briefs:** Managed Detection and Response, Continuous Threat Exposure Management, Zero Trust explained, Digital Identity and Access Management, Cyber Recovery, Post-Quantum Cryptography, Security Transformation
- Unisys Cybersecurity Resource Center