Publication date:
June 2025
Author:
Maxine Holt

Trust: The Strategic Differentiator in Modern Cybersecurity

Commissioned by:

OMDIA

SAFEBASE by DRATA

Contents

Summary

Organizational trust is imperative in today's cybersecurity landscape

Resilience sits at the center of modern digital trust, enabling organizations to operate, adapt, and grow confidently in the face of constant risk and complexity. As threats grow more frequent, regulations tighten, and customer expectations rise, organizations must prove not only that they can prevent incidents but that they can endure, respond, and build trust through any disruption.

To achieve this, today's security leaders must architect resilience across multiple dimensions: digital, cyber, and organizational, each reinforcing the other to create durable, enterprise-wide trust. Omdia defines digital and cyber resilience as follows:

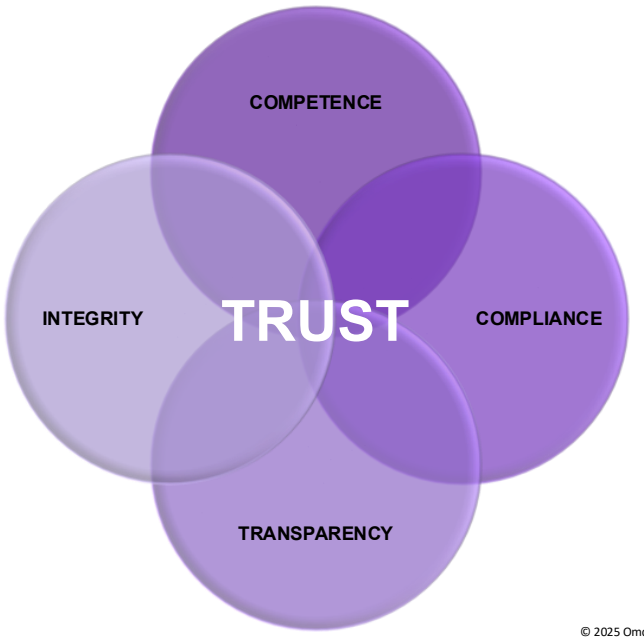
Digital resilience is the ability to continuously operate and quickly leverage digital opportunities.

Cyber resilience is a core component of digital resilience. It ensures that the organization continuously operates **despite** security challenges.

Overall, organizational resilience is the ability of a company to withstand, adapt to, and recover from cyberattacks, breaches, and disruptions, all while preserving operational continuity, customer trust, and business value.

Resilience leads to organizational trust. This trust is built on the foundation of competence, compliance, transparency, and integrity (see **Figure 1**).

Figure 1: Components of organizational trust



Source: Omdia

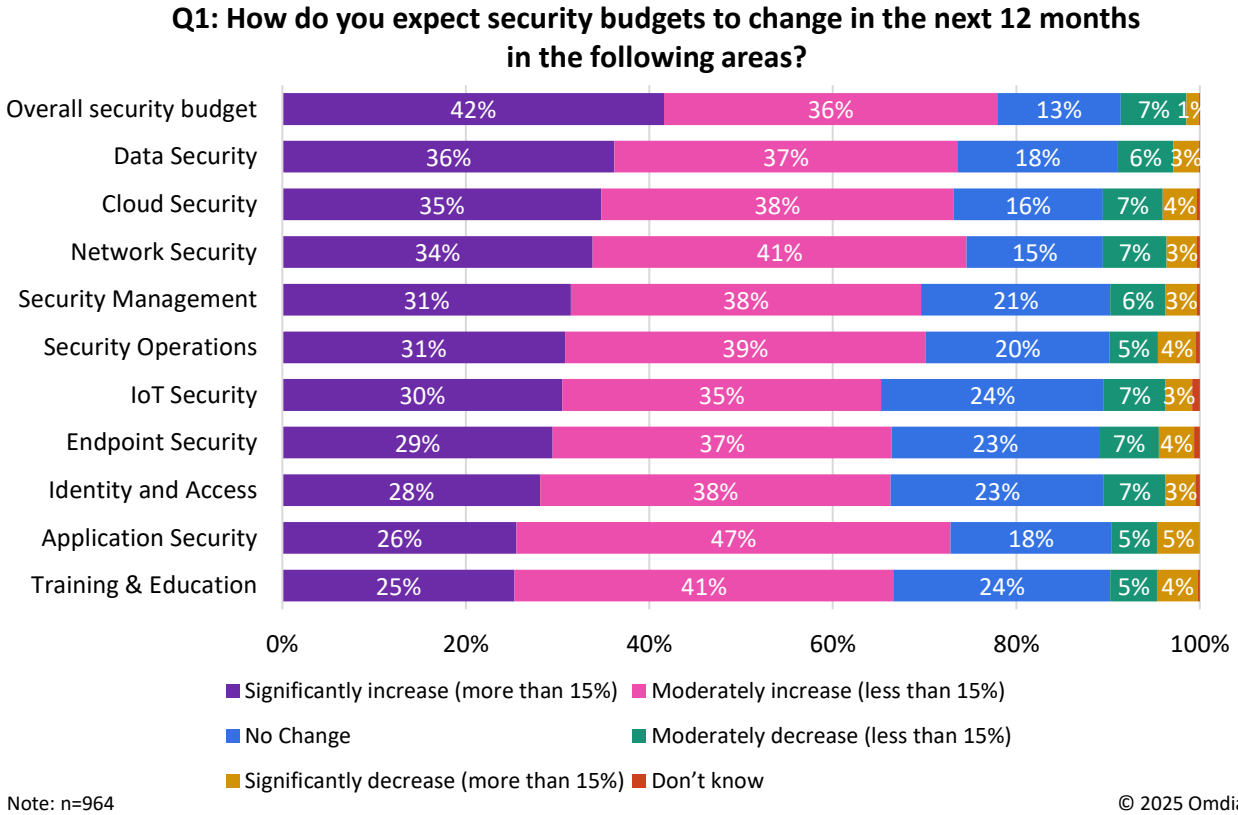
Digging into the components of trust from a cybersecurity perspective:

- **Competence:** Ability to continuously operate and innovate despite security challenges, a key component of cyber resilience.
- **Compliance:** Complying with appropriate cybersecurity regulations and legislation across jurisdictions supports resilience. Customers expect compliance.
- **Transparency**: You know the security posture of your suppliers, and your customers know your security posture.
- **Integrity**: Security is complex and challenging; an organization must take its security responsibilities seriously and act with integrity.

Today's security landscape: Omdia survey results

Omdia's latest cybersecurity decision-maker survey highlights that security budgets are growing across security domains, from cloud to endpoint to training and education. Over three-quarters of respondents noted a moderate (<15%) or significant (15%+) increase in in security budgets in 2024 (see Figure 2).

Figure 2: Change in security budgets



Note: n=964

Source: Omdia

The survey also noted that 62% of organizations surveyed believe that the severity of security issues has worsened over the past 2 years, with over half of survey respondents suffering from multiple severe security incidents in the preceding 12-month period. Over 60% of organizations with 1,000 employees or more suffered breaches costing over $0.5m to recover and remediate. Over one-third of organizations with fewer than 1,000 employees also suffered breach events at this level of cost.

Defending against threats is critical but organizational resilience isn't built on defense alone. Security leaders must pair protection with proactive trust-building, creating transparency and confidence that strengthen customer relationships and fuel business growth.

Resilience and trust work best together

Security control frameworks provide essential structure for organizations, but true resilience requires going beyond compliance checkboxes to establish genuine trust, such as actively sharing real-time security posture, maintaining continuous visibility into risks, openly communicating during incidents, automating security review processes for faster transparency and assurance, and aligning security outcomes to business objectives that customers care about. This human and strategic layer transforms security from a technical function into a business enabler that strengthens stakeholder relationships.

Yet the security talent shortage presents a persistent challenge, with nearly half (46%) of organizations from Omdia's cybersecurity decision-maker survey reporting staffing and skills deficiencies. However, this gap need not compromise security effectiveness or stakeholder trust. Strategic deployment of security tools can:

- Automate routine monitoring and detection processes.
- Streamline incident response workflows.
- Optimize resource allocation based on risk prioritization.
- Enable security teams to shift from reactive firefighting to proactive trust-building programs that strengthen transparency, resilience, and customer confidence.

By leveraging these capabilities, organizations can maintain robust security, reduce friction, and boost transparency, ultimately building customer trust through reliable protection rather than cumbersome controls.

The power of AI

In today's complex threat landscape, AI has emerged as a critical enabler for security operations and the wider security function. In the security operations center (SOC), for example, AI technologies can:

- Analyze vast datasets to identify anomalous patterns that human analysts might miss.
- Automate routine security tasks, freeing people for strategic initiatives.
- Provide real-time threat intelligence and response recommendations.

Use of AI in cybersecurity can create the foundation for trustworthy, responsive security interactions that protect without impeding business operations.

Risks of external security providers

Many organizations turn to external security providers to address capability gaps, but this approach introduces its own set of risks that require careful oversight. While third-party expertise can strengthen certain aspects of a security program, it also introduces new dependencies and potential vulnerabilities if not properly governed. For example:

- **Expanded privilege and identity risk**: Third-party providers frequently require administrative-level access to critical systems to perform monitoring, detection, or remediation functions. These elevated privileges create additional identity sprawl, increasing the attack surface. A compromised vendor account, whether through credential theft, social engineering, or supply chain compromise, can serve as a privileged entry point into core environments.

- **Supply chain and software dependencies**: Security providers often deploy proprietary agents, connectors, or APIs within the customer's environment. Each of these integrations represents an extension of the organization's supply chain. Vulnerabilities or misconfigurations in these tools, whether in endpoint agents, SIEM (security information and event management) connectors, or response orchestration platforms, can be exploited to bypass controls, exfiltrate data, or disable defenses.

- **Operational and response dependency**: Incident response timelines can be directly impacted by reliance on third-party providers. During critical events, response coordination, SLA limitations, or lack of immediate operational control may delay containment efforts. Over-reliance on external providers for key incident response functions can hinder an organization's ability to execute rapid, autonomous decisions during time-sensitive breaches.

Outsourcing critical security functions without appropriate oversight can result in the erosion of trust rather than strengthening it.

As such, transparency serves as arguably the most valuable asset in building trust. Organizations that communicate clearly about their security posture—sharing appropriate details about controls, incidents, and remediation efforts—signal accountability and operational rigor. Increasingly, security leaders are adopting structured approaches to make this information accessible and actionable for stakeholders. Examples of these practices include:

- **Centralizing security disclosures and artifacts**: By consolidating documentation such as certifications, policies, audit reports, and security architecture summaries, organizations can streamline how stakeholders access assurance materials, reducing the administrative overhead of ad hoc information requests.

- **Providing visibility into risk and remediation processes**: Sharing structured information on vulnerability management programs, incident response frameworks, and policy governance helps external stakeholders understand how risks are actively managed and addressed over time.

- **Enabling consistent communication across stakeholder groups**: A centralized approach to security transparency ensures that internal teams, customers, partners, and regulators are all accessing aligned, current information, which in turn can minimize inconsistencies and potential miscommunication across assurance conversations.

Build durable trust for your organization

Organizations must make trust integral to their ongoing strategy, instead of an afterthought or byproduct. There are various ways of evolving an organization's approach to trust, including:

- Address the evolving threat landscape with integrity.
- Establish robust compliance and transparency frameworks.
- Build organizational trust through security competence.

These three points are now reviewed in more detail.

Address the evolving threat landscape with integrity

The threat landscape continues to evolve rapidly, even as organizations increasingly leverage emerging technologies such as AI to drive digital transformation. Investments in cybersecurity controls remain foundational, not only to ensure operational continuity and regulatory compliance, but also to enable innovation that keeps organizations relevant and competitive in the eyes of their customers.
However, in today's environment, protecting the business is only part of the equation. Security leaders are also recognizing the opportunity to use transparency as a strategic lever for earning, growing, and retaining customer trust. Proactively communicating the organization's security posture—through clear, accessible disclosures around controls, certifications, incident readiness, and ongoing risk management—demonstrates operational integrity while directly supporting customer assurance and confidence.

This approach reframes cybersecurity as not just a cost center, but a growth enabler. When customers feel confident in an organization's ability to manage risk responsibly, they are more likely to expand partnerships, entrust sensitive data, and view security as a differentiator. For both B2B and B2C organizations, this ongoing demonstration of trust can support revenue expansion, customer loyalty, and longer-term business resilience (see Figure 3: The Cybersecurity Balancing Act).

Figure 3: The cybersecurity balancing act

Source: Omdia

In this regard, it remains critical for boards and C-suites to stay engaged on the increasing business impact of security. As digital adoption proliferates, maintaining an appropriate balance between agility and assurance requires ongoing investment in both technical controls and trust-building practices that span security, compliance, and privacy across the entire ecosystem.

Establish robust compliance and transparency frameworks

Compliance and transparency are essential components of building durable trust in both B2B and B2C relationships. While regulatory compliance provides the baseline, ensuring organizations meet legal and industry standards across jurisdictions, it is transparency that increasingly differentiates organizations as trusted partners.

Beyond simply maintaining compliant policies and controls, leading organizations are investing in mechanisms to proactively communicate their security posture to external stakeholders. This includes publishing evidence of certifications, audit results, policies, and security practices in a structured, accessible, and secure format. By enabling customers, partners, and auditors to easily review relevant assurance artifacts, organizations can reduce friction in the due diligence process and demonstrate an ongoing commitment to responsible risk management. Furthermore, internal stakeholders can also gain transparency and access a single source for answers around the company's security and trust posture.

Governance structures also play a critical role, embedding accountability across the organization while extending visibility into third-party suppliers. Conducting thorough security assessments of vendors, documenting risk management practices, and enabling secure, real-time sharing of these materials with customers helps create a more open and resilient security ecosystem.

In this way, transparency becomes a reinforcing layer on top of compliance, not only signalling adherence to standards, but actively inviting external trust through clear, verifiable, and consistently updated information.

Build organizational trust through security competence

Knowing that your organization is focused on managing the threat landscape whilst enabling innovation, and that there are robust and transparent frameworks in place around security, supports resilience, which in turn supports and builds trust.

Competent security from all components of an ecosystem enables availability and reliability, which can also support innovation and growth. Organizations frequently have dozens of standalone security products (31-50 being the most common) and are keen to reduce the volume of suppliers to make their security estate more manageable. However, few are achieving a reduction (just 3% of survey respondents between 2023-24), indicating that not only is it complex to reduce supplier volume but also the effectiveness is paramount. Increased utilization of AI tools and technology is seen to support the security function, enabling increased focus on strategic initiatives.

Security competence drives trust

Trust is not incidental, it is the outcome of deliberate, transparent, and consistently executed security practices that can scale with the business. For today's CISOs, this means moving beyond reactive controls and static compliance checklists toward an operating model where security directly supports business growth, customer confidence, and long-term resilience.

Invest in capabilities that allow your organization to continuously demonstrate its security posture, communicate openly with customers and partners, and provide assurance in real time. Establish governance structures that embed accountability across both internal operations and third-party relationships. And most importantly, recognize that trust is not a one-time achievement, but an

ongoing discipline, one that will increasingly distinguish market leaders as digital ecosystems continue to expand.

For security leaders, now is the time to elevate transparency as a core pillar of the security strategy, not simply as a defensive measure but as a proactive driver of business value.

Appendix

Author

Maxine Holt
Vice President, Enterprise & Channel
maxine.holt@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together “Informa TechTarget”) or its third party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.