Report

jumpcloud™

## Stronger Together:

# Why IT-Security Collaboration Drives Greater Security and Efficiency

For years, the go-to cybersecurity strategy has been a simple one: throw more money at more tools. But here's the problem—more tools doesn't equal more security. In fact, the opposite is often true. Fragmented systems, misconfigurations, and siloed teams create vulnerabilities that attackers exploit. It's a vicious cycle that drains budgets, burns out teams, and leaves organizations exposed.

So, what's the real solution? A fundamental rethinking of how we approach security—shifting from tool obsession to team unification.

This report, which surveyed 100 security leaders from the United States and the United Kingdom, reveals why IT and security must join forces to break down silos, simplify complexity, and deliver results that no single tool ever could.

# Why IT-Security Collaboration Is the Missing Weapon in Cyber Defense

When it comes to cybersecurity, fragmented tools and siloed teams are leaving organizations vulnerable. Here are five critical insights from security professionals that underscore why IT-security collaboration is no longer optional—it's essential.

### Security without IT is a losing battle

1

**91%**

of security professionals say collaboration with IT is critical to their strategy.

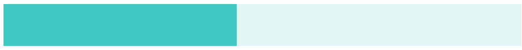
The takeaway?
Security can't succeed without IT—it's time to break down the silos.

### Fragmentation is killing your security

2

**Nearly half**

(45%) of respondents say fragmented tools create blind spots and inefficiencies.



Complex systems aren't just hard to manage—they're a liability.

## Unified systems aren't a luxury–they're a necessity

3

**2 in 3**

security leaders believe unified IT-security tools significantly improve visibility, control, and overall posture.

Simplification isn't just operational—it's strategic.

## Unifying device and identity management tools increases productivity by 25% or more

4

**100%**

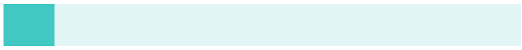
believed unification would improve productivity by at least 25%, among those who saw productivity as a key benefit of unifying tools.

## Fragmented tools are failing SMBs

5

**<10%**

of respondents believe current IT and security tools meet their needs.



Complexity, high costs, and tool fragmentation are leaving SMBs and midmarket companies exposed, overwhelmed, and underserved in a market designed for enterprises.

# Security Is Broken Without IT

In a world where the threat landscape is constantly evolving, the tools and strategies used to mitigate risks are only as effective as the teams behind them—and security professionals understand this. Survey results show that **91% of security professionals** recognize IT as an important partner in achieving their goals. The belief that IT-security collaboration is critical is even more strongly held in the UK, where security professionals are **1.6 times more likely to say it's critical** than their US counterparts.

**91%** **of security professionals consider collaboration with IT to be critical or important to their security strategy.**

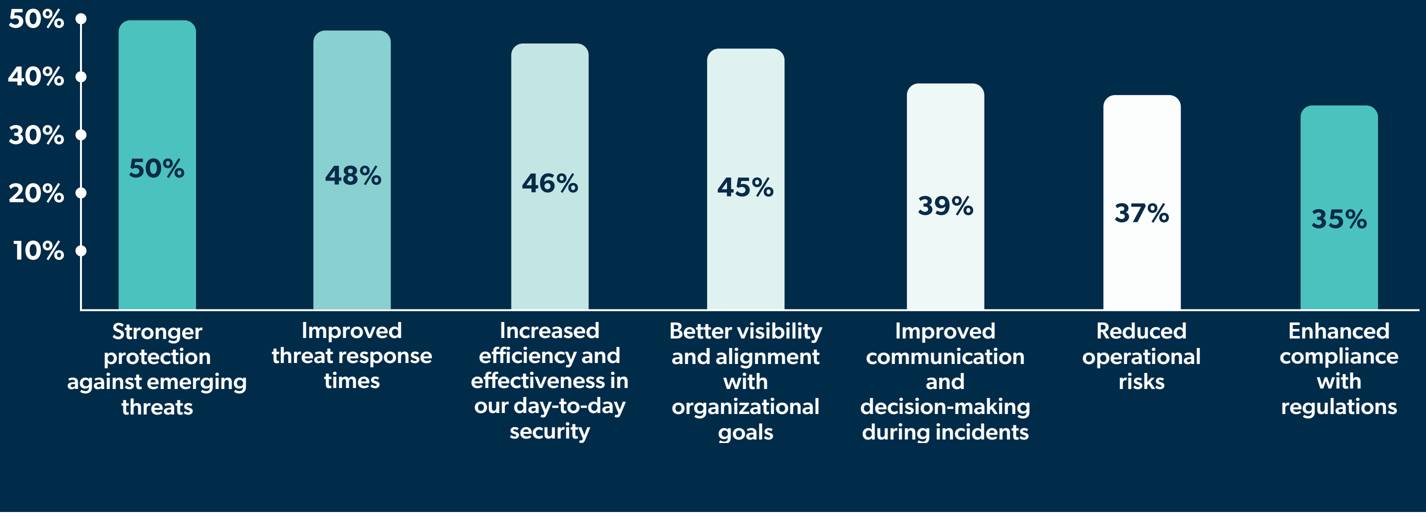
## Strong IT-security collaboration drives real security gains

Over one-third of all respondents reported that IT-security collaboration offered benefits in every area we asked them about. This collaboration goes beyond aligning teams—it enhances an organization's ability to detect, respond to, and mitigate threats effectively.

The top three benefits were:

1. Stronger protection against emerging threats
2. Faster threat response times
3. Increased efficiency and effectiveness in day-to-day security operations

### What benefits do you believe stronger collaboration between IT and security teams could provide to your organization?

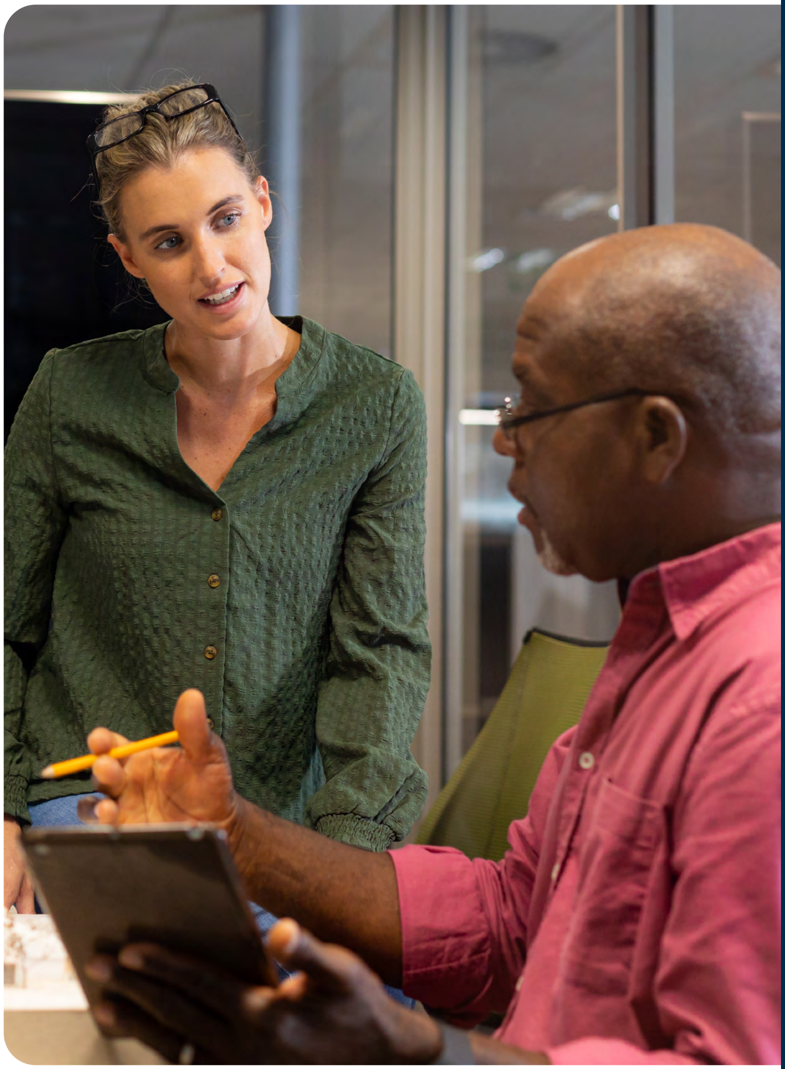


## Why Collaboration Works

IT teams are more than just technical support—they're a critical force multiplier for security functions.  Their expertise in managing devices, controlling access, and maintaining infrastructure makes them indispensable allies for security teams. When IT and security work together, they:

- **Break down silos,** fostering open communication and shared goals
- **Reduce operational risks** by ensuring that security measures are integrated into IT systems from the start
- **Align their efforts** to meet compliance requirements more effectively

While tools and technology are essential components of any security strategy, our research shows that the collaboration between IT and security teams is just as important, if not more so. Unified teams can adapt faster to emerging threats, streamline daily operations, and respond to incidents with greater speed and precision. By combining forces, IT and security don't just protect organizations—they create resilience and efficiency that no standalone team can achieve.



# Unification: The Key to Simplified and Stronger Security

When it comes to security, complexity is the enemy of effectiveness. As organizations grow and threats evolve, fragmented tools and siloed systems create inefficiencies, slow response times, and introduce vulnerabilities. Security professionals increasingly view the simplification and unification of IT and security tools as more than operational improvements—they are strategic imperatives.

# The Hidden Costs of Fragmentation

Fragmented IT and security tools pose significant challenges for organizations:

**45%**

of respondents say fragmented tools make it difficult to integrate data for a holistic security view.

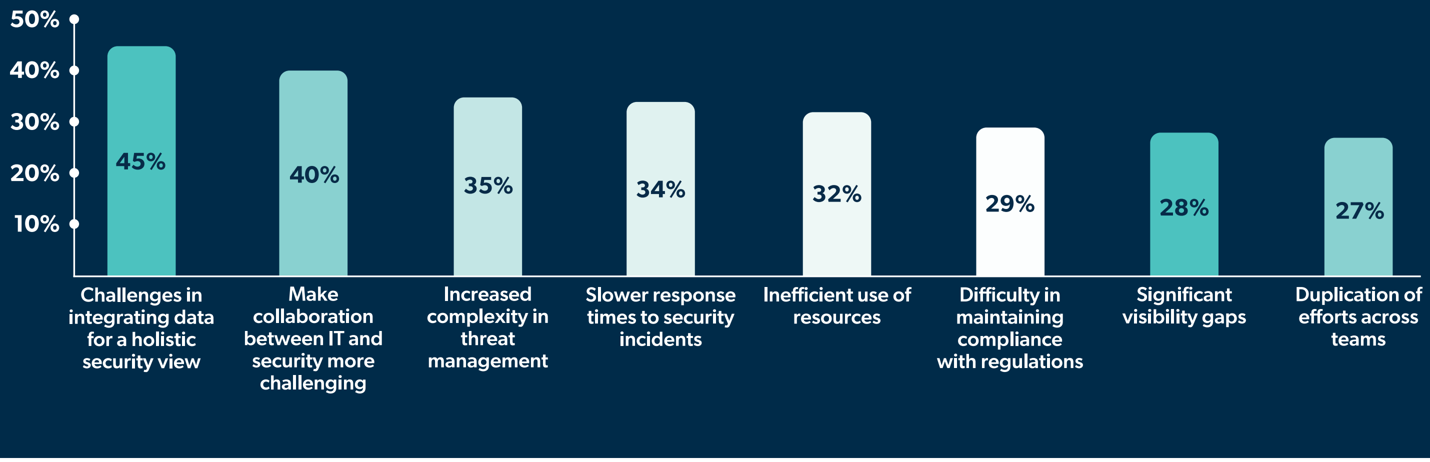
**40%**

report that these tools hinder collaboration between IT and security teams.

**35%**

of respondents reported increasing complexity in threat management.

## What challenges do you believe are caused by having fragmented IT tools in your organization?

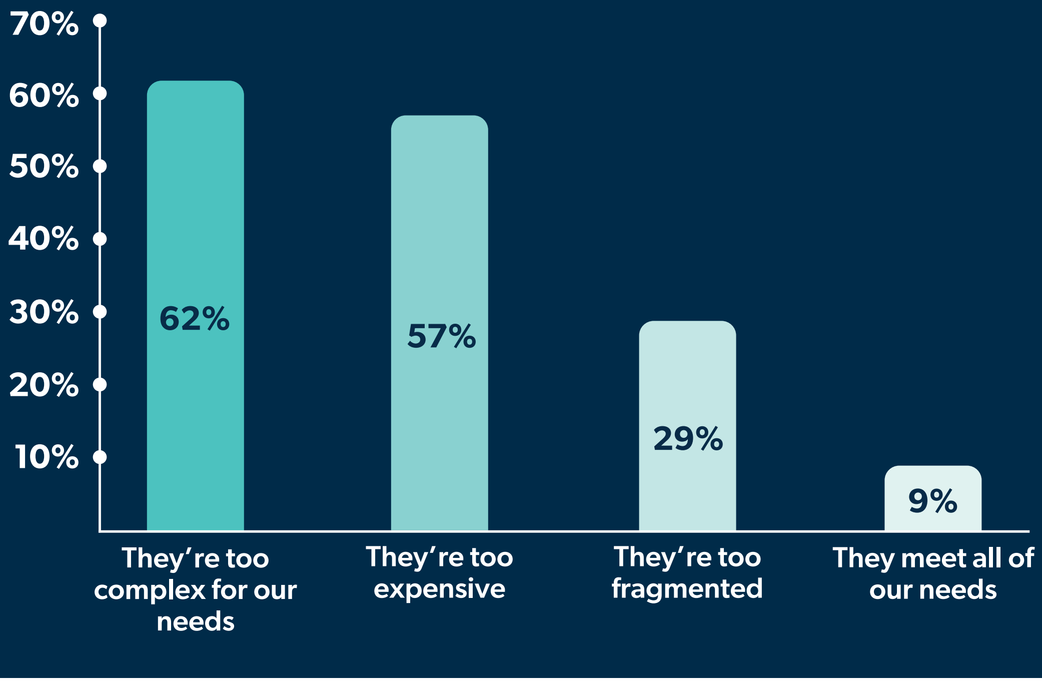


In addition, most SMBs find that tools designed to enhance security often fail to meet their needs—with tool fragmentation an issue for nearly one-third of respondents.

**<10%**

**of SMB and midmarket security professionals believe current IT and security tools meet their needs**

## Which of the following do you find to be true of current IT and security tools on the market in meeting your organization's needs?



The data also underscores the potential of unified IT and security tools to transform organizations:

**49%**

of respondents believe unifying tools provides better visibility and control over users, devices, and access.

**2 in 3**

say unified management of IT systems would be somewhat or very effective in improving their organization's security posture.

# Unification Unlocks Greater Productivity

Unification benefits go beyond security—it also boosts efficiency, freeing up resources for strategic initiatives. Among those who saw productivity as a benefit:

**100%**

believed unified tools would improve productivity by at least 25%

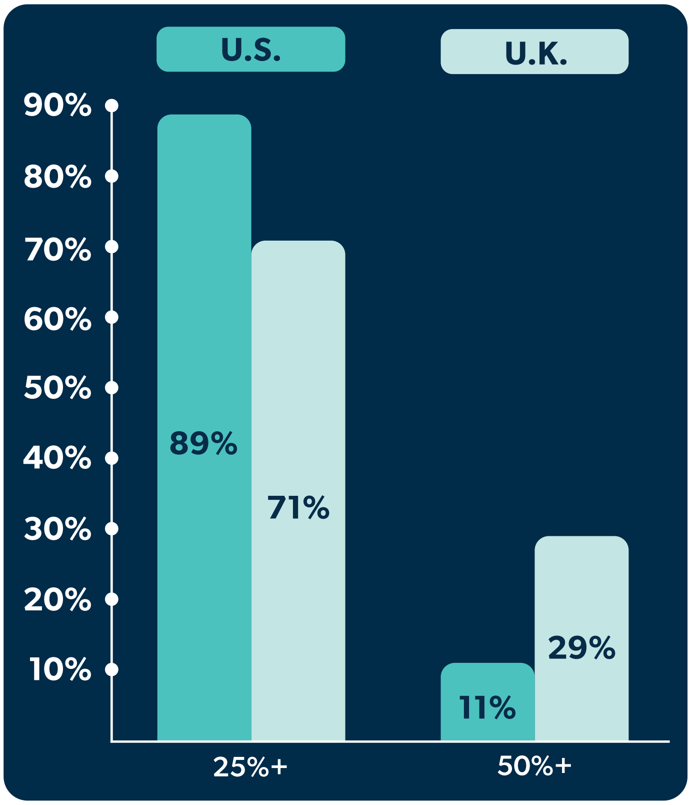
**1 in 5**

(19%) expected gains of 50% or more

**1 in 3**

(29%) in the UK expected gains of 50% or more

## By how much do you believe consolidating point solutions could improve productivity?



For small and mid-sized businesses, where resources are limited, unifying IT and security tools is particularly impactful. Unified tools:

**Streamline management:** Reduce costs and complexity of managing multiple systems.

**Enable growth:** Scalability allows companies to expand without costly overhauls to their security infrastructure.

**Strengthen alignment:** Unified tools foster collaboration between IT and security, creating more seamless and efficient workflows.

Simplification is not just about reducing the number of tools – it's about consolidating point solutions to drive measurable improvements. By unifying IT and security tools, organizations can lay the groundwork for stronger collaboration, resilience, and efficiency.

# Building Security by Default

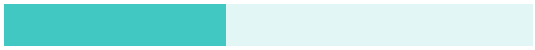
When it comes to securing an organization, the adage “an ounce of prevention is worth a pound of cure” holds true. Security professionals agree (81%) that embedding security principles and controls into IT infrastructure from the start is the most effective approach. This proactive method shifts security from being an afterthought to becoming a core element of operations.

## Stop Reacting, Start Preventing

Survey respondents were clear: proactive strategies are significantly more effective than reactive ones. Among the findings:

42%

of respondents rate “building security into IT infrastructure from the start” as very effective for ensuring a strong security posture.



**In contrast, reactively addressing risks or incidents as they arise was less effective, with many respondents ranking it only as somewhat effective or not effective.**

This preference for proactive security reflects a broader industry shift toward prevention and preparedness rather than waiting for incidents to occur.

## IT’s Role in Proactive Security

IT teams are uniquely positioned to lead proactive security efforts and implement critical security control policies because of their management of the organization’s infrastructure. Their responsibilities directly impact key areas of security, including:

- **Device management:** Ensuring that all devices are secure, updated, and compliant with organizational policies.
- **Identity management:** Managing user identities to ensure that employees only access the resources they need, reducing insider threats and accidental exposures.
- **Access control:** Implementing robust measures like multi-factor authentication (MFA) and Zero Trust principles to safeguard sensitive systems.

By integrating security into these foundational IT processes, organizations can create a seamless, scalable and resilient defense approach that strengthens their overall posture.

# Unifying IT and Security Tools for Greater Impact

Unified tools don’t just simplify operations, they redefine how organizations approach security. By embedding security measures directly into IT systems, unification turns security from a reactive patchwork into a seamless, proactive function integrated into the organization’s core processes.

**77%**

of respondents who believe unified management is very effective also agree it enhances productivity and strengthens security.

**49%**

of respondents said unifying tools improves visibility and control over users, devices, and access.

**2 in 3**

respondents believe unified tools would be somewhat or very effective in strengthening their security posture.

For SMBs and midmarket organizations, unifying tools offers a range of benefits:

**Cost efficiency:** Consolidating tools reduces licensing fees and maintenance costs, freeing up resources for other priorities.

**Simplicity:** Unified systems are easier to manage, requiring less time and fewer personnel to maintain.

**Scalability:** Integrated solutions can grow with the organization, eliminating the need for costly overhauls as SMBs expand.

**Improved collaboration:** Unified tools foster better communication and alignment between IT and Security teams, streamlining operations and reducing silos.

# Better Security Starts with Better Collaboration

Collaboration between IT and security teams is the cornerstone of a resilient and adaptable security strategy. By working together and adopting unified tools and processes, IT and security teams can simplify operations, enhance visibility, and strengthen overall security efforts.

When systems are integrated and goals are shared, organizations achieve tangible benefits:

### Improve visibility across systems

**45%**

of respondents emphasized the importance of enhanced visibility for identifying risks and responding effectively. Integrated dashboards and analytics reduce blind spots, enabling teams to spot and address threats faster.

### Strengthen access controls

**42%**

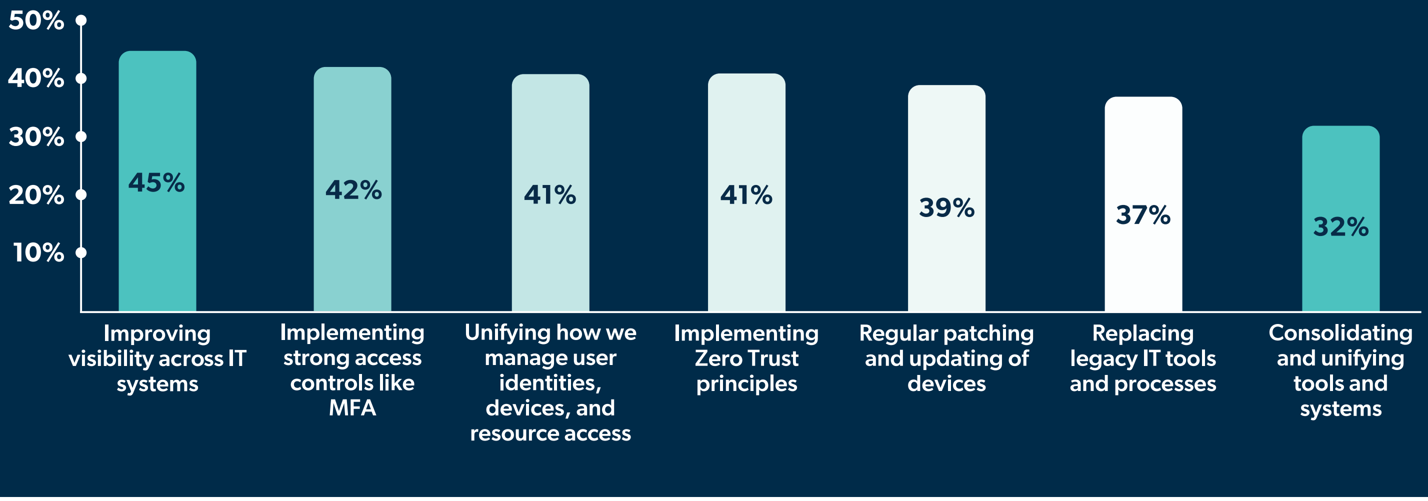
highlighted the critical role of measures like multi-factor authentication (MFA) and Zero Trust principles in safeguarding sensitive resources. IT teams are pivotal in implementing and maintaining these controls across the organization.

### Centralize management of identities, devices, and resources

**41%**

of security professionals cited the need for unified management to streamline processes and enhance security. A centralized approach ensures consistent application of protocols and reduces gaps in security.

## Which IT actions have the greatest impact on improving your organization's security posture?



# Recommendations for Building a Unified IT-Security Strategy

Unifying IT and security functions is the key to building a resilient, efficient, and scalable security posture. By adopting a unified IT-security framework, businesses can address inefficiencies, enhance collaboration, and better protect against emerging threats.

Here are six recommendations to enable greater unification of both IT-security teams and tools:

## 1. Stop guessing: Map your weak spots before they exploit you

Before implementing changes, organizations need a clear understanding of their current environment. Key steps include:

- **Assess tools and systems:** Identify redundancies, inefficiencies, and gaps in existing IT and security tools.

- **Evaluate collaboration:** Analyze the effectiveness of IT-security communication and workflows.

- **Map blindspots, gaps, and inefficiencies:** Assess where fragmented systems or outdated tools hinder visibility, disrupt workflows, or create potential security risks, and prioritize these areas for improvement.

## 2. Ditch the clutter: Why fragmented tools are your biggest liability

Investing in tools and platforms that unify IT and security functions is essential for simplifying operations and reducing risks. Organizations should:

- **Choose platforms that integrate identity, access, and device management** into a single solution.

- **Opt for tools that provide centralized visibility and control**, reducing the need for manual data reconciliation.

- **Eliminate outdated or redundant tools** that add complexity without delivering value.

## 3. Collaboration or chaos: The culture shift security demands

Unified tools alone won't deliver results without a culture of collaboration between IT and Security teams. To build this culture:

- **Encourage joint planning:** Include IT and security in strategic decision-making and incident response planning.

- **Establish shared metrics:** Use KPIs that reflect the shared goals of both teams, such as response times and risk mitigation success rates.

- **Promote regular communication:** Schedule cross-functional meetings to review progress, address challenges, and align priorities.

## 4. High-impact, high-stakes: IT and security must lead the security revolution

Focusing on high-impact security measures ensures that resources are allocated effectively and that the organization builds a strong foundation for resilience. IT's involvement is crucial in identifying and implementing these priorities. To achieve this:

**Collaborate with IT to proactively add security into existing and new infrastructure,** ensuring systems are secure by design.

**Prioritize critical controls** like multi-factor authentication and Zero Trust principles to protect key assets.

**Automate workflows that help eliminate vulnerabilities.** Automating patching, SaaS application discovery, employee lifecycle management, and other workflows that increase close vulnerabilities, increase visibility, and reduce misconfigurations will greatly improve security resilience across the organization.

## 5. Think ahead: Multiyear planning to outpace threats

Creating a strategic, long-term plan ensures that your business can scale securely while staying ahead of emerging threats. This means building flexibility and resilience into every step of the process.
To achieve this:

**Choose scalable, adaptable tools** that reduce complexity and align with both current and future needs.

**Collaboratively reassess the organization's security framework** on an ongoing basis to address growth, new technologies, and evolving threats.

**Adopt a proactive, iterative approach:** Focus on measuring outcomes consistently to identify gaps, refine strategies, and adapt as your organization grows. Explore new frameworks and industry best practices incrementally, ensuring readiness before implementing changes to avoid overwhelming teams.

## 6. A never-ending process: The hard truth about security evolution

Building a unified IT-security framework isn't a one-time effort—it's an ongoing process. Organizations should:

**Monitor key metrics,** such as threat detection rates, response times, and system uptime, to gauge effectiveness.

**Solicit feedback** from IT and security teams to identify areas for improvement.

**Adjust tools, workflows, and strategies** as needed to stay aligned with organizational goals and industry best practices.

# Cyber Resilience Starts with Unification: Security Threats Won’t Wait

The era of throwing money at fragmented solutions is over—and good riddance. Complexity isn’t just inconvenient; it’s dangerous. Security leaders must face a simple truth: patchwork fixes won’t cut it anymore. It’s time to stop reacting to problems and start building a stronger foundation.

A unified IT-security strategy doesn’t just fix today’s problems; it rewrites the rules for the future. Integrate, simplify, and collaborate—or stay stuck in the endless loop of inefficiency and vulnerability. The choice is clear: evolve now, or risk everything.

## Methodology

This report is based on a survey conducted by Redpoint, exclusively for JumpCloud, gathering insights from 101 security professionals, specifically from organizations with 250–1,000 employees across a variety of industries during November 2024.

### Key Demographics

**Geography:**

United States: 64%
United Kingdom: 36%

**Roles and Responsibilities:**

C-Suite/Executive: 27%
Director/Manager: 67%
Individual Contributor: 33%

**Company Size:**

250–500 employees: 55%
501–1,000 employees: 45%

**Primary Responsibilities:**

Security only: 63%
Combined IT and Security roles: 37%

**Industries:**

Financial Services: 33%
Technology: 27%
Retail/E-commerce: 27%
Manufacturing: 15%
Education: 12%
Healthcare/Life Sciences: 11%
Media & Entertainment: 8%
Professional Services: 5%