Omdia
by informa techtarget

Digital resilience: A security imperative

Today's workforce operates in multiple environments, demanding frictionless security to support resilience

Author: Maxine Holt

November 2025

In partnership with:

ZOHO

Contents

Digital resilience in the age of mobile work: A security imperative

Digital resilience is the foundation of modern business continuity

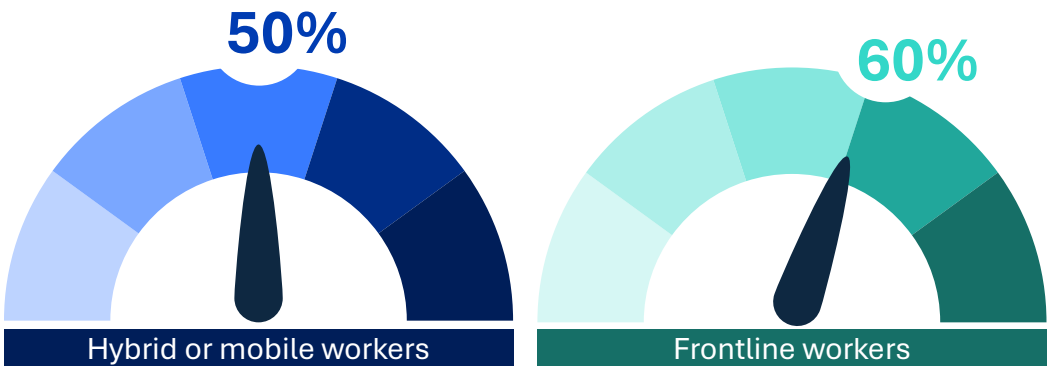
As defined by Omdia, digital resilience represents an organization's ability to continuously operate and quickly leverage digital opportunities, even when facing disruption from security, operational, or market challenges.

At its core, this concept encompasses cyber resilience, ensuring an organization functions despite constant security threats and attempted cyberattacks.

Over the past decade, workplace reality has fundamentally shifted. Omdia research shows that 50% of the typical workforce now operates in hybrid or mobile environments, despite many organizations deploying “return to office” mandates for most of the working week.

Furthermore, approximately 60% of workers are frontline employees who rely primarily on mobile devices, from retail staff to field service technicians (see Figure 1).

Figure 1: Today's workforce



Source: Omdia

This is more than a trend: it is a permanent restructuring of how organizations operate, irrespective of size.

This evolution presents a challenge to organizations, not least because the cyberthreat landscape continues to evolve at pace. Almost nine out of 10 security decision-makers in 2025 reported to Omdia that security issues have either worsened or remained critically challenging over the past two years.

This is reinforced by Omdia's security breaches tracker, which in 2024 tracked 7.6 billion breached records—almost one record per human on the planet. Data for the first half of 2025 suggests that number will be exceeded this year.

Security teams protect and serve to support digital resilience

Security teams face a dual mandate to "protect and serve," safeguarding the organization while enabling daily business operations. Too often, an organization's security function is referred to as the "Department of No," perceived as creating barriers that frustrate employees and slow business processes. However, the most effective security functions position themselves as business enablers, finding ways to say "yes, and here's how we can do it securely."

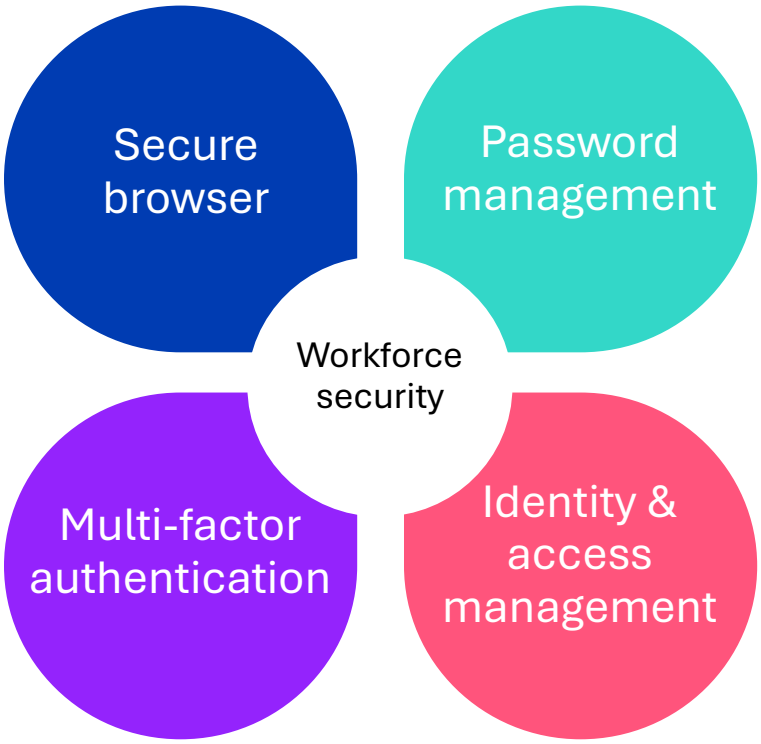
Likewise, business decision-makers recognize the value of security, with the management of security, identity, and privacy ranked as one of the top three concerns for 41% of organizations globally—the leading issue in Omdia's *IT Enterprise Insights 2025* survey. Furthermore, Omdia's research also shows digital transformation projects, including the many AI initiatives organizations are undertaking, present ongoing challenges for over half of security functions worldwide.

Many organizations, irrespective of size, face limited budgets, inadequately resourced security teams, and skills shortages, making it difficult to keep pace with evolving threats while supporting business growth and digital transformation initiatives.

Utilizing four pillars of security for a digitally resilient workforce

Protecting today's workforce requires a comprehensive approach that includes four pillars of modern security: browser protection (as part of endpoint security), credential management, multi-factor authentication (MFA), and identity governance (see Figure 2).

Figure 2: Four pillars of workforce security



Source: Omdia

These capabilities work together to deliver a robust security framework that supports the focus of security teams on protecting and serving the organization. Considering each capability in turn:

Secure browser

Secure enterprise browser capabilities, as part of endpoint security, provide granular control over web interactions without sacrificing user experience. Since web browsers serve as the "eyes" of the organization as a major interface with the digital world, they

require specialized protection. Organizations should focus on browser security that operates at the application level, targeting the browsing layer where many sensitive interactions occur.

Password management

Passwords are known as a considerable weakness for organizational security. This can be mitigated to a significant extent through organization-driven workforce password management, with centralized and secure authentication credentials. This directly tackles common vulnerabilities such as written-down passwords, credential reuse, and password sharing, and reduces security friction for employees in their day-to-day work.

Multi-factor authentication (MFA)

Multi-factor authentication provides an additional layer of security that is known to deliver major reductions in account takeovers and identity attacks. Modern MFA solutions minimize friction while maximizing protection, using technology such as biometric authentication, card readers, and more. Even if credentials are compromised through phishing or data breaches, attackers face additional barriers before gaining system access.

Identity governance

Identity governance can provide an overarching framework for authorization decisions, enabling consistent policies that align with business requirements and security principles. Identity governance frameworks typically focus on three questions:

- Who can access the organization's resources?
- What exactly can they access?
- Under what conditions can access occur?

Identity governance and lifecycle management that grants, adjusts, and revokes access at precisely the right times can prevent the accumulation of unnecessary permissions that create security risks.

In support of these pillars, organizations typically develop an implementation strategy that starts with a comprehensive assessment of the mobile workforce's security posture. Technological controls are generally selected in support of both protection and business enablement.

“Comprehensive security controls require people and processes to be implemented alongside the technology, and effective security should be as frictionless as possible for the employee, whilst simultaneously providing protection for the organization.”

Source: Maxine Holt, Vice President, Enterprise & Channel

The goal? Achieving the delicate balance between security, innovation enablement, and operational efficiency: the foundation of true digital and cyber resilience in today's mobile-centric business environment.

Appendix

Methodology

Omdia research includes data from a range of mobile workforce studies, *cybersecurity decision-maker survey*, *IT Enterprise Insights survey*, plus extensive expertise in cybersecurity and workforce transformation.

Author

Maxine Holt, Vice President, Enterprise & Channel Research
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.

Get in touch

www.omdia.com
askananalyst@omdia.com