SPOTLIGHT

Zero Trust Enabled By Microsoft Security

COMMISSIONED BY MICROSOFT, MAY 2026

FORRESTER®



Microsoft commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying the Microsoft Security portfolio, which includes Entra, Defender, Intune, Sentinel, Purview, and Security Copilot.[1] This abstract will focus on organizations using Microsoft Security to enable Zero Trust and its value.

Forrester interviewed 11 decision-makers and surveyed 362 customers with experience using Microsoft Security products. Enabling a Zero Trust framework was one of the key decision-making criteria when evaluating an investment or expansion in use of Microsoft's security portfolio. Microsoft Security enables Zero Trust by operationalizing its three core principles — verify explicitly, use least privilege access, and assume breach. It does so across the Zero Trust pillars: identity, devices, applications, data, network, infrastructure, and AI, with unified policy enforcement, rich telemetry, and automation.

64%

Percentage of survey respondents that experienced improved identity protection as an outcome of Zero Trust adoption

59%

Percentage of survey respondents that experienced improved MFA/conditional access coverage as an outcome of Zero Trust adoption

82%

Percentage of survey respondents considered Microsoft's commitment to Zero Trust "Important" or "Very important" when selecting a security provider

> *"Federal agencies that need to adopt and implement a Zero Trust framework would benefit from the Microsoft portfolio and would enhance their overall security data management and operational efficiency as a result of implementing these products."*
>
> **Regional CIO, government**

> *"I'm better able to enforce Zero Trust because of the data [in Defender and Sentinel]. It can correlate and aggregate data from all these various products, and that's what's going to really offer a lot of enhanced value to your enterprise."*
>
> **Regional CIO, government**

Forrester Perspective: Zero Trust

Zero Trust (ZT) is a security model that assumes no implicit trust and demands continuous verification of identities, devices, and context to protect against modern threats. Why is this important? Traditional security solutions are often made up of siloed and overlapping tools, which makes it difficult for organizations to embrace new technology like AI-driven operations. This can exacerbate the challenges of implementing Zero Trust with a fragmented market of point solutions.[2] In Forrester's 2025 Security Survey of 2,665 security decision-makers, 67% of respondents said their organization's sensitive data was potentially breached at least once in the previous 12 months — proof that traditional security models are not working.[3]

Achieving a Zero Trust architecture does not require ripping out current security controls and starting from scratch. As long as their current security estate meets certain conditions, security leaders can utilize existing tools to increase their ZT competence and realize immediate security benefits.[4] First, Forrester advises that "interoperability is nonnegotiable" because an organization can leverage existing investments while reducing complexity, costs and risks.[5] A second key consideration is support for open APIs, standardized protocols, and prebuilt connectors that enable faster deployment and orchestration across diverse ecosystems. This enables organizations to accelerate digital transformation and adopt new technology like AI without sacrificing security.[6] Finally, centralization delivers unified control and ZT platforms with centralized policy management, visibility, and analytics will create a unified experience, reducing overhead and strengthening governance.[7]

Zero Trust has become critically important in the age of agentic AI. Forrester's AEGIS framework for agentic AI security is, to a large extent, based on a Zero Trust architecture and principles. The first principle in the framework is "least agency." Similar to the Zero Trust concept of least privilege, "AEGIS relies on least agency. AI agents within agentic architectures must receive the minimum set of permissions, capabilities, tools, and decision-making to complete specific tasks bound by time and scope of approval."[8]

"How important was Microsoft's commitment to the Zero Trust framework for your organization when selecting a security solutions provider?"



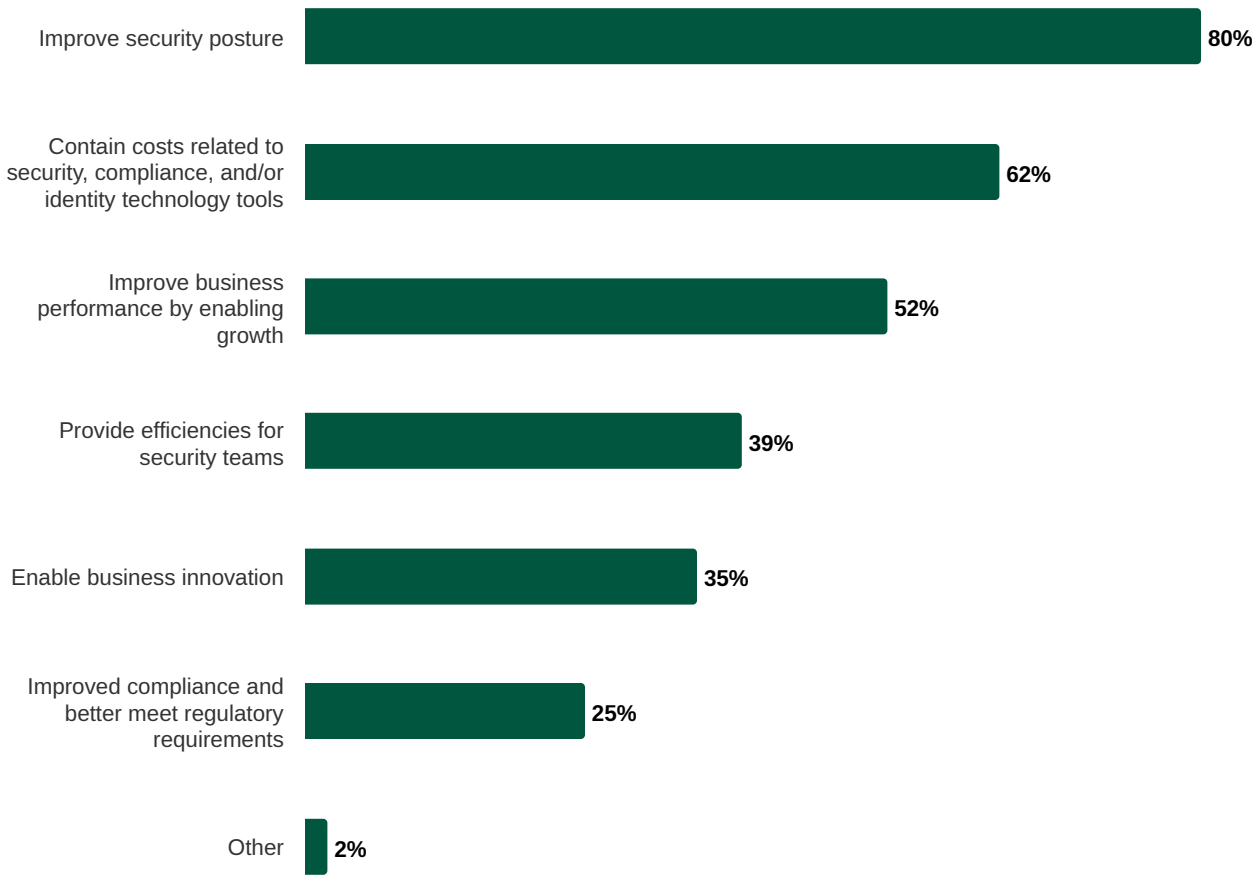
Base: 362 global IT and security decision-makers at large enterprises using Microsoft Security as their end-to-end security solution across security, compliance, and identity
Source: Microsoft Security Solutions Study, a commissioned study conducted by Forrester Consulting

Investment Drivers

The interviewees' organizations adopted Microsoft Security to improve threat protection, better meet compliance policies, and enable a Zero Trust environment. Interviewees faced the following challenges that influenced their Microsoft investment:

- **Lack of adherence to internal compliance policies.** Interviewees highlighted compliance as particularly difficult to enforce without dedicated tools and automation. Before deploying Microsoft solutions, interviewees relied on targeted manual enforcement and/or employee honor systems, which resulted in poor compliance.
- **Lack of resources to holistically achieve Zero Trust.** As interviewees' organizations expanded cloud and AI adoption, Zero Trust was essential to reducing risk by continuously verifying identities, enforcing least-privilege access, and assuming a breach. Interviewees indicated that while Zero Trust was a strategic priority, limited resources made holistic adoption difficult. The director of technology and security for a healthcare firm explained: "We have gone to Zero Trust in certain segments of our environment when it comes to any foreign connectivity inbound or outbound. We go with a Zero Trust geographical rules for our firewalls, for all of our MFA authentications, so any external authentication. So, it's not something that we had the staff on hand or the finances to attack holistically to go 100% Zero Trust in every way that that term can be applied."
- **Federal mandates.** Interviewees noted that Zero Trust is mandated, not optional, for federal agencies in the United States.

"What goals/challenges did your organization hope to address?"



Base: 362 global IT and security decision-makers at large enterprises using Microsoft Security as their end-to-end security solution across security, compliance, and identity

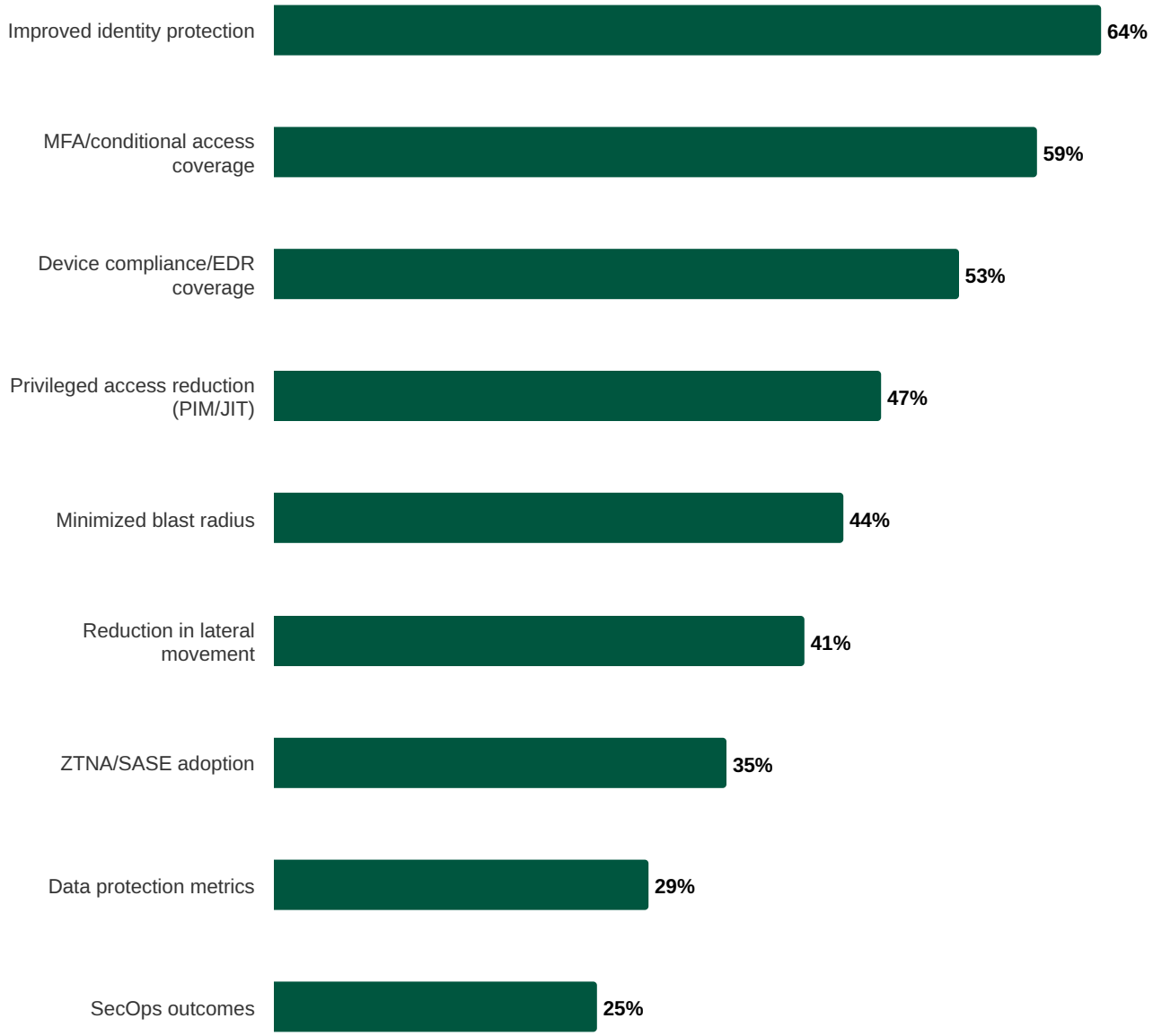
Source: Microsoft Security Solutions Study, a commissioned study conducted by Forrester Consulting

Key Results

The regional CIO at a federal agency in the United States and the senior information security officer and senior IT officer at a global NGO all highlighted the importance of Microsoft on their organizations' Zero Trust journeys:

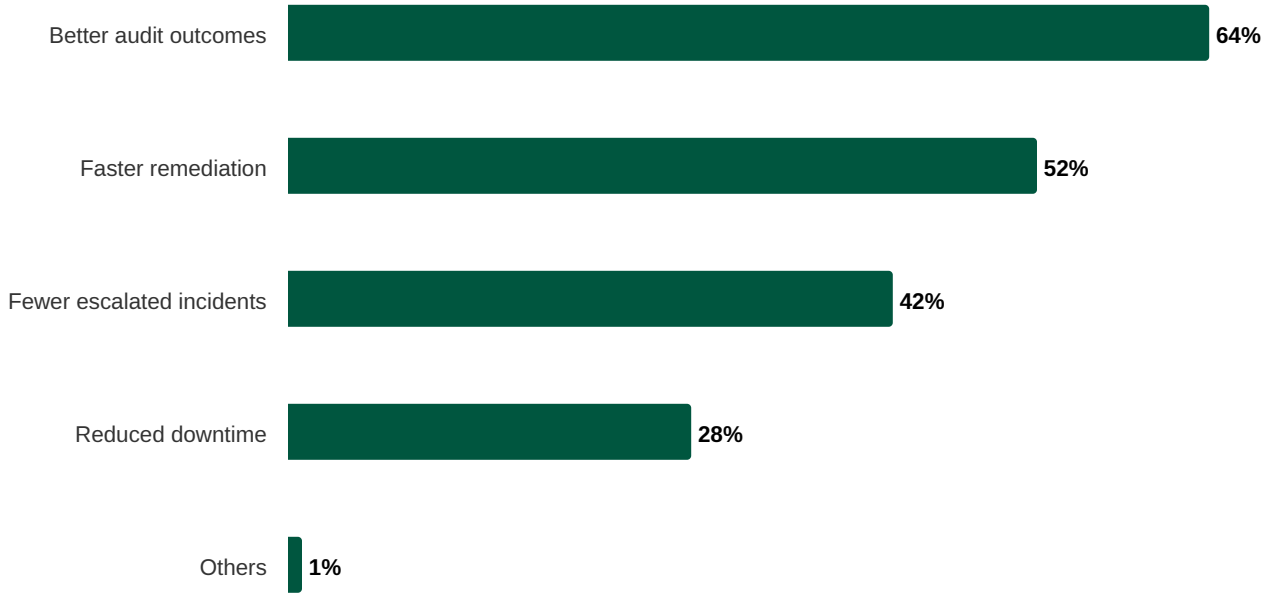
- **Federal agency in United States.** The regional CIO said Microsoft provided an integrated, end-to-end security platform that maps directly to federal Zero Trust mandates, especially OMB Memo M-22-09 and CISA's Zero Trust Maturity Model, to help their organization implement Zero Trust. This interviewee reported clear, quantified improvements at their organization that were tied to Zero Trust outcomes, including the following:
    - A significant reduction in password resets and manual access management due to single sign-on (SSO), MFA, and automated provisioning and a 25% to 35% improvement in mean time to respond (MTTR) due to MFA and conditional access enforcement.
    - Device security configuration and deployment timelines cut roughly in half through Intune and Defender integration.
    - A 25% to 35% improvement in investigation, response, and false-positive reduction through Microsoft Sentinel and Defender automation.
    - A 75% improvement in data governance maturity due to auto-labeling, retention policies and eDiscovery.
- **Global NGO.** The interviewees noted that Microsoft helped their organization operationalize Zero Trust by shifting trust away from the network perimeter and anchoring it in strong identity, device posture, and session risk signals. The foundation of their organization's Zero Trust strategy was Microsoft Entra ID, which the interviewees described as replacing "trust in the network with trust in strong user identity, machine identity, and session strength." The interviewees reported measurable outcomes related to the maturity they achieved on their Zero Trust journey because of Microsoft Security, including the following:
    - Identity maturity significantly improved, confirmed via independent cybersecurity and Zero Trust maturity assessments. They noted a material improvement in endpoint security driven by Defender.
    - Zero Trust-aligned extended detection and responses (XDR) playbooks led to measurable improvements in MTTR. Importantly, Zero Trust maturity enabled their organization to measure response metrics that it could not previously measure.

“You previously indicated that your organization has adopted a Zero Trust approach as a benefit. What metrics or outcomes best demonstrate the impact of Zero Trust adoption at your organization?”



Base: 297 global IT and security decision-makers at large enterprises using Microsoft Security as their end-to-end security solution across security, compliance, and identity
Source: Microsoft Security Solutions Study, a commissioned study conducted by Forrester Consulting

“Which of the following business outcomes have improved at your organization as a result of Zero Trust adoption?”



Base: 297 global IT and security decision-makers at large enterprises using Microsoft Security as their end-to-end security solution across security, compliance, and identity
Source: Microsoft Security Solutions Study, a commissioned study conducted by Forrester Consulting

TOTAL ECONOMIC IMPACT ANALYSIS

For more information, download the full study: “The Total Economic Impact™ Of Microsoft Security,” a commissioned study conducted by Forrester Consulting on behalf of Microsoft, May 2026.

Study Findings

Forrester interviewed 11 total representatives at organizations and surveyed 362 customers with experience using Microsoft Security and combined the results into a three-year financial analysis for a composite organization. Risk-adjusted present value (PV) quantified benefits for the composite organization include:

- Improved security posture that reduces the likelihood of a breach by up to 30%.
- Reduced annual external technology spend by up to 23%.
- Saved business users an average of 50 minutes per week with improved SSO, more efficient onboarding, and better performance.

124%

Return on investment (ROI)

$16.6M

Net present value (NPV)

Appendixes

APPENDIX A

Endnotes

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

[2] Source: Buyer's Guide: Zero Trust Platforms, 2025, Forrester Research, Inc. January 30, 2026.

[3] Source: Guage Your Zero Trust Maturity, Forrester Research, Inc., December 1, 2025; Forrester's Security Survey, 2025

[4] Source: A Practical Guide To Zero Trust Implementation, Forrester Research, Inc. December 17, 2025.

[5] Source: Buyer's Guide: Zero Trust Platforms, 2025, Forrester Research, Inc. January 30, 2026.

[6] Source: Buyer's Guide: Zero Trust Platforms, 2025, Forrester Research, Inc. January 30, 2026.

[7] Source: Buyer's Guide: Zero Trust Platforms, 2025, Forrester Research, Inc. January 30, 2026.

[8] Ibid.

Disclosures

Readers should be aware of the following:

This study is commissioned by Microsoft and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Microsoft.

Microsoft reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Microsoft provided the customer names for the interviews but did not participate in the interviews.