Microsoft Security

Rapidly Modernize Your Security Posture

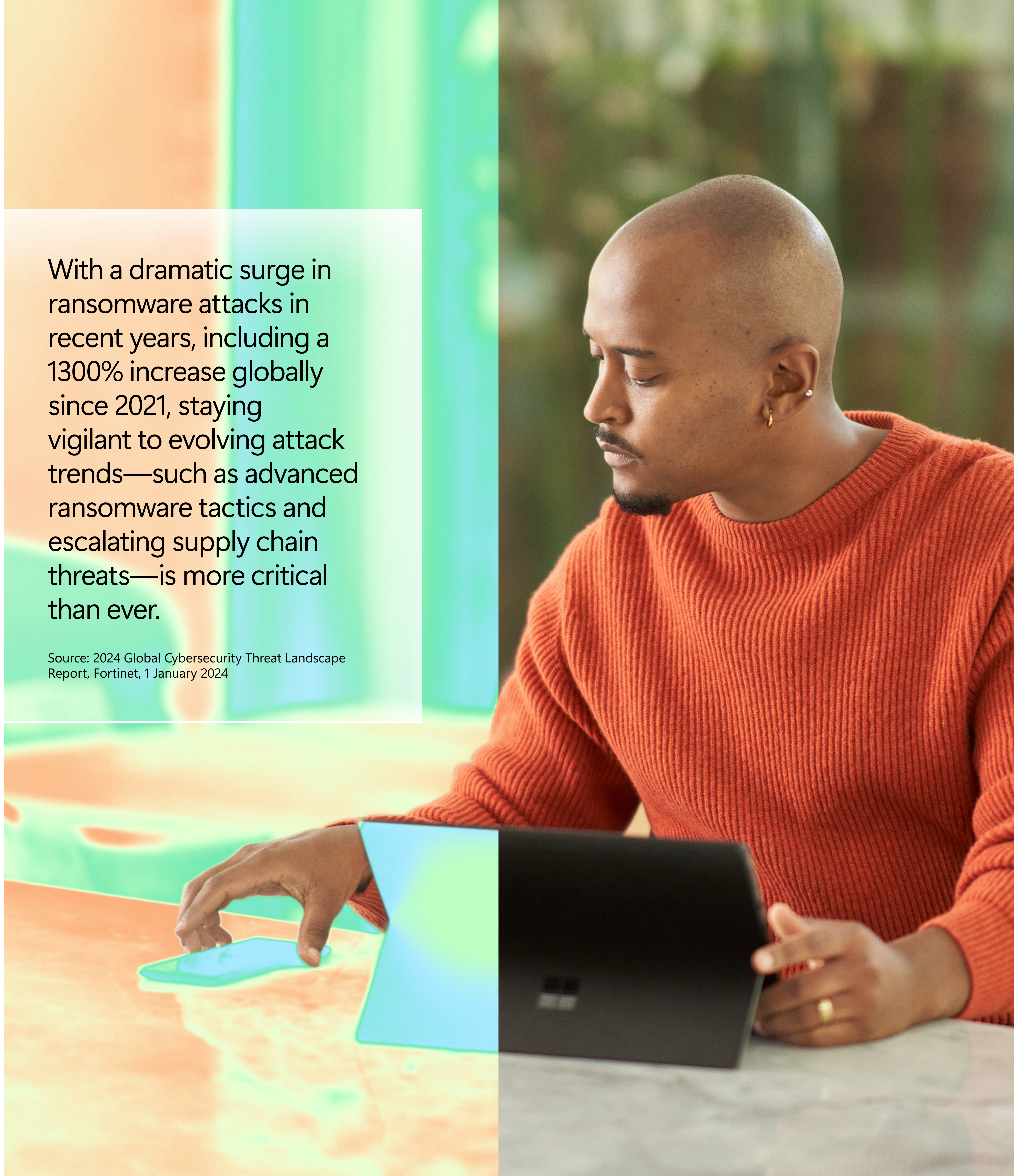
Use a Zero Trust Framework to Build Confidence with Your Employees, Partners, Customers, and Other Stakeholders

Evaluating Your Security Posture is an Ongoing Challenge

The security landscape is rapidly evolving, driven by the widespread shift to hybrid work, a surge in ransomware attacks, and dynamic regulatory requirements. In this environment, security leaders must navigate these challenges while meeting the business demands for collaboration, innovation, and growth. This creates critical questions from employees, partners, customers, and C-suite stakeholders:

- Do we have a comprehensive approach to risk-based vulnerability management?
- Do we have the right security strategy and controls?
- Can we measure breach risk and identify potential attack paths?
- Are our security controls sufficient to manage modern-day cyber risks and vulnerabilities?
- Do we have tools for continuous security assessment and exposure reduction?
- Can we easily meet today's and future compliance and reporting needs?

Confidence in security teams depends on the answers to these questions. These answers are integral to your security posture, which impacts your ability to protect resources and keep your organization out of headlines that damage business reputation, erode customer trust, and affect profitability.
To build confidence and strengthen security posture, you need continuous security assessment and exposure reduction.



With a dramatic surge in ransomware attacks in recent years, including a 1300% increase globally since 2021, staying vigilant to evolving attack trends—such as advanced ransomware tactics and escalating supply chain threats—is more critical than ever.

Source: 2024 Global Cybersecurity Threat Landscape Report, Fortinet, 1 January 2024

Building Confidence and Trust with Zero Trust Principles

Implementing a modern security strategy enhances visibility across endpoints, identifies risks, before they can be exploited, and automates detection and response. A Zero Trust model, combined with continuous exposure management, enables proactive security monitoring, risk-based access controls, and automated remediation to protect critical assets (data) in real-time within a dynamic threat environment. An effective Zero Trust architecture reduces risk across your digital estate by adhering to the following principles:

1. Verify Explicitly

Protect all assets against attacker control by explicitly validating that trust and security decisions use all relevant and available information and telemetry. It is no longer enough to check credentials once; real-time insights are essential for continuously validating trust. Continuous monitoring of real-time security insights helps organizations proactively assess risk exposure across identities, endpoints, and workloads.

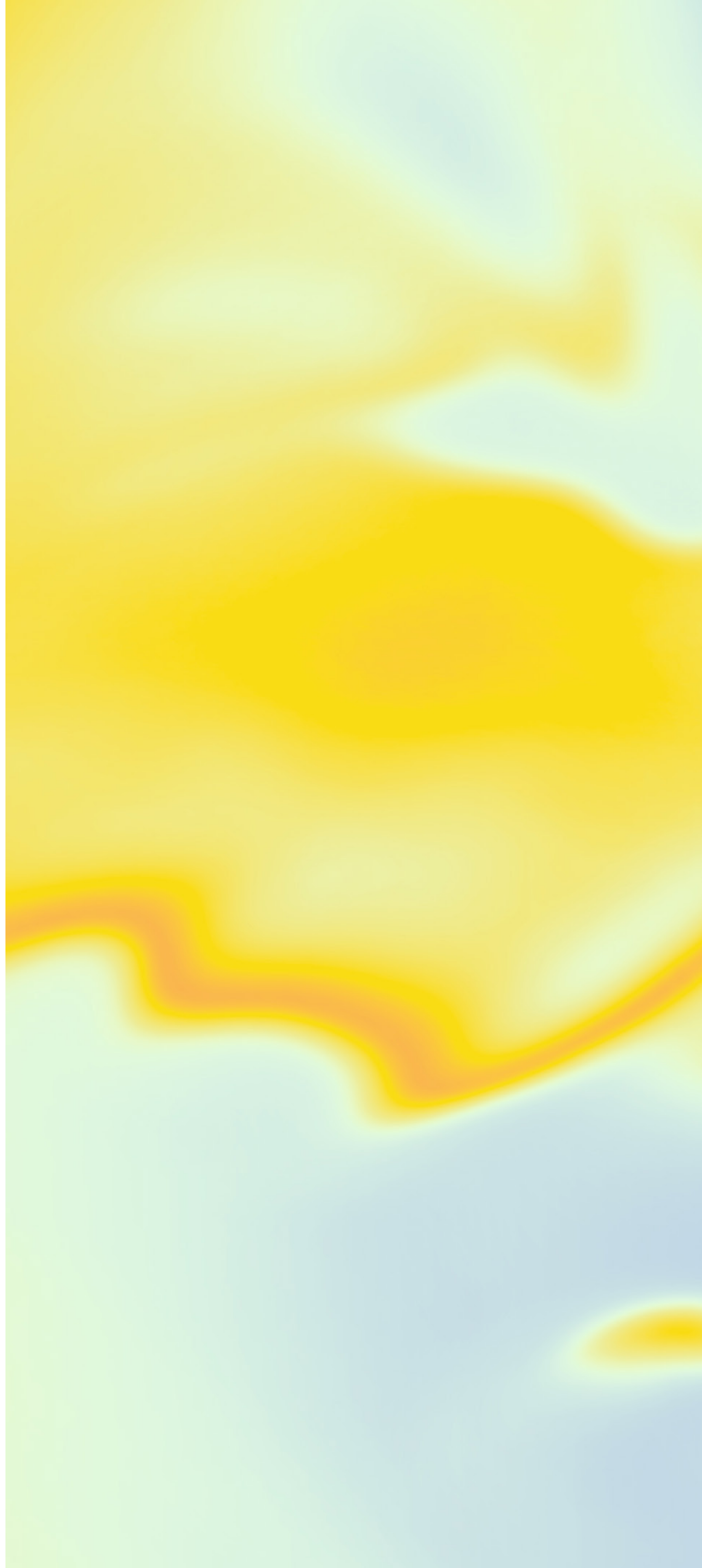
2. Use Least-Privilege Access

Limit access to a potentially compromised asset, typically with just-in-time and just-enough access (JIT/JEA) and risk-based policies like adaptive access control. Minimize access rights to reduce risk and ensure that users and devices only have the permissions they need, and for only as long as they need them. Organizations can dynamically adjust access controls based on evolving risk conditions—such as detecting excessive permissions, misconfigurations, or behavioral anomalies.

3. Assume Breach

Plan as if an attacker is already inside your network. Use segmentation, encryption, and continuous monitoring to limit potential damage and respond quickly. Using security exposure insights, teams can continuously identify vulnerabilities, prioritize remediation efforts, and automate responses to strengthen defenses before a breach occurs.

A Zero Trust strategy, when paired with proactive exposure management, allows you to assess risk in real-time, prioritize remediation, and continuously strengthen your security posture.



Steps to Move Forward with a Zero Trust Model

To fully realize the benefits of a Zero Trust model, organizations need to adopt a proactive approach, integrating continuous security posture management tools to assess, prioritize, and mitigate security exposures.

1. Proactively Manage Your Security Posture

Security posture is not static, it requires continuous analysis of assets, attack surfaces, and emerging threats. Organizations must:

- Understand asset relationships and the attack paths adversaries may use.
- Detect and prioritize security exposures before they lead to breaches.
- Automate misconfiguration detection and remediation to enforce Zero Trust policies dynamically.

Security exposure insights help teams move beyond reactive security approaches, ensuring risk reduction is proactive, not just responsive.

2. Understand Your Current Security Posture

Leverage scoring tools to measure your security posture against industry benchmarks and best practices. Continuous monitoring of risk-based security scores helps your team instantly understand:

- Which assets are most vulnerable
- How security misconfigurations impact overall risk
- What actions to take to reduce exposure

By incorporating measurable security insights into reporting and compliance tracking, organizations can demonstrate continuous improvement and risk reduction to stakeholders.

3. Take Advantage of Visibility and Analytics

Continuous monitoring across various attack vectors detects potential security gaps before they can be exploited. AI-driven risk analysis allows organizations to:

- Identify risky configurations, outdated policies, and excessive access permissions.
- Analyze breach likelihood based on real-time telemetry data.
- Automate security optimizations to reduce manual intervention.

With comprehensive visibility into risk, organizations can pinpoint vulnerabilities, prioritize mitigation efforts, and enforce Zero Trust policies more effectively.

4. Undergo Risk Assessment and Reduce Attack Surface

Security risks such as configuration drift, missed patches, and access control gaps create opportunities for attackers. AI and automation enhance visibility, allowing teams to:

- Identify and remediate overprivileged accounts, misconfigurations, and outdated security controls.
- Apply historical risk insights to improve Zero Trust implementation.
- Automate security hardening across cloud, hybrid, and on-premises environments.

By proactively closing security gaps, organizations can enforce Zero Trust principles at scale while optimizing security and compliance.

The Zero Trust model is a proactive, integrated approach to securing the modern digital estate. It explicitly and continuously verifies every access request based on dynamic context, enforces least-privilege access across users, devices, and resources, and leverages real-time intelligence, advanced threat detection, and automated responses to mitigate risks and protect organizational assets.

Benefits of a Robust Security Posture with Zero Trust

Improving your security posture through a Zero Trust and continuous exposure management strengthens the resilience against cyber threats while driving measurable business benefits including:

1. Demonstrating Impact to Leadership

Using tools like security scores and analytics, you can provide quantifiable risk reduction metrics using security scores, risk assessments and exposure analysis to present clear security improvements and clear actions to improve security posture, the effort required, and the user impact to your stakeholders including your board of directors.

2. Driving Innovation with Partners

A Zero Trust model protects against insufficient vendor security practices and partners by consolidating security policies, ensuring appropriate access for all external users, partners, and third-party applications regardless of location, device, or network. This strengthens partner relationships while protecting critical assets.

3. Increasing Security Team Morale

Empower your security team to apply Zero Trust principles across environments and quickly identify and address concerns. Security teams can shift from reactive security monitoring to proactive threat reduction by leveraging AI-driven automation and security posture insights.

4. Enabling Agile Response to Business Needs

A Zero Trust security posture provides automated security visibility, adaptive risk assessments, and centralized policy enforcement, allowing organizations to respond faster to security incidents without impacting productivity.

Leverage AI to Rapidly Modernize Your Security Posture

AI accelerates the modernization of security posture, helping organizations keep up with evolving threats and demands. By processing vast amounts of security data in real time, AI provides deeper insights, uncovers vulnerabilities, and enables faster, more precise threat response. Within a Zero Trust strategy, AI automates tasks like risk assessment, anomaly detection, and incident response, allowing security teams to focus on strategic priorities. It dynamically adapts defenses by analyzing telemetry and updating policies in real time, staying ahead of emerging threats.

AI enhances agility and resilience by enabling rapid gap assessments, actionable insights for stakeholders, and compliance with changing regulations—all while supporting collaboration, innovation, and growth. By integrating AI-driven risk management with Zero Trust principles, organizations can:

- Process vast security data in real time to detect and mitigate threats faster.
- Automate Zero Trust policy enforcement based on security posture changes.
- Provide real-time breach likelihood analysis to prioritize remediation.

With AI-powered automation and continuous risk assessment, organizations can stay ahead of emerging threats while continuously improving their security posture.

Modernize Your Security Posture for a Resilient Future

In today's fast-paced digital environment, modernizing your security posture is essential to safeguard your people, data, and systems. As organizations embrace hybrid work and face evolving cyber threats, a modern security strategy ensures proactive risk reduction, seamless security monitoring, and strong resilience against sophisticated attacks—all while enabling collaboration, agility, and growth.

By integrating advanced tools, AI, and Zero Trust principles, organizations create a proactive and adaptive defense framework that protects critical assets without slowing down business operations. A Zero Trust model, reinforced by continuous security exposure management, ensures:

- Attack surface minimization and automated threat response.
- Real-time security visibility and adaptive policy enforcement.
- Stronger resilience against evolving cyber threats.

Security is no longer just about blocking attacks—it's about empowering your organization to thrive with confidence, agility, and resilience in an ever-changing digital landscape.

Start Your Zero Trust Journey

With a Zero Trust security model, organizations can modernize their security posture, mitigate risk proactively, and drive long-term business resilience. To learn more about how AI and Zero Trust can support agile security and business operations, visit Agile Business, Agile Security: How AI and Zero Trust Work Together.

Agile Business, Agile Security: How AI and Zero Trust Work Together

To help your organization take the next step, here's a step-by-step guide to implementing Zero Trust with proactive security management and continuous risk assessment using Microsoft tools:

1. Continuously Assess and Reduce Security Exposure:

Identify and mitigate security gaps in your environment before attackers can exploit them. Use **Microsoft Security Exposure Management (MSEM)** to conduct continuous security assessments of identities, endpoints, cloud environments, and workloads. Prioritize vulnerabilities based on attack paths, exposure risks, and business impact. Automate remediation to reduce misconfigurations and enforce Zero Trust policies dynamically. Use **Microsoft Defender for Cloud** to conduct a security assessment across your hybrid and multi-cloud environment, providing actionable insights and recommendations for improvement.

2. Secure Identities with Continuous Risk-Based Protection:

Use **Microsoft Entra ID** to protect user identities. Leverage features like **adaptive MFA**, password-less authentication, conditional access policies, and continuous identify risk monitoring to detect and mitigate compromised accounts proactively to ensure secure and seamless identity verification across all devices and applications.

3. Strengthen Endpoint Security and Reduce Attach Surface:

Deploy **Defender for Endpoint** to monitor device health, detect and prioritize vulnerabilities, and enforce compliance policies in real time. Use advanced threat intelligence to block sophisticated malware and ransom threats. Automate endpoint remediation to maintain compliance with Zero Trust principles.

4. Enforce Least-Privilege Access and Prevent Lateral Movement:

Implement **Azure AD Identity Governance** and **MSEM** to continuously evaluate and adjust permissions based on exposure risk and usage patterns. Enforce features like just-in-time (JIT) access and just-enough policies to help minimize exposure to potential threats while maintaining productivity. Detect and remediate over privileged accounts before they become security risks. Conduct automated access reviews to eliminate unnecessary permissions and prevent escalation.

5. Enhance Threat Detection with AI-Powered Analytics:

Use **Microsoft Sentinel**, a cloud-native SIEM and SOAR solution, to continuously analyze security telemetry across endpoints, identities, networks, and applications. Detect anomalous activity and insider threats with AI behavioral analytics. Automate incident response and security policy enforcement to mitigate attacks faster. Correlate threat intelligence and security exposure date to prioritize the most critical threats.

6. Leverage AI to Automate Security and Reduce Manual Efforts:

Incorporate AI-driven tools like **Microsoft Security Copilot** and **MSEM** to optimize Zero Trust policies, detect anomalies and remediate misconfiguration and security gaps, and accelerate response times. Copilot uses AI to streamline complex tasks, enhance threat intelligence, and provide actionable insights, enabling IT teams to respond faster and more effectively.

7. Simplify Compliance:

Streamline regulatory management and reporting with **Microsoft Purview Compliance Manager** to meet compliance requirements and track progress.

8. Secure Hybrid and Multi-Cloud Environments:

Deploy **Microsoft Defender for Cloud Apps** to protect data and ensure visibility across SaaS and multi-cloud activities.

By implementing Zero Trust alongside **Microsoft Security Exposure Management**, organizations can proactively reduce attack surfaces, strengthen security posture, and improve resilience against evolving threats.