Microsoft

Cracking the Code to Secure Productivity in Two Steps

How a Zero Trust foundation empowers productive work experiences

Contents

Introduction

Don't stretch with the growing threat landscape—grow ahead of it

Today's threat landscape is growing fast, with sophisticated threats like identity attacks, ransomware, and endpoint attacks putting data and IT infrastructure at risk. The reality of modern work has put increased pressure on IT teams, who often find themselves stretched thin trying to cover a growing number of vulnerabilities.

With **67%** of IT professionals reporting being overwhelmed trying to manage remote work, getting ahead of threats is crucial to avoiding costly breaches and downtime.[1] Stretching IT teams thin makes it easier for attackers to be successful, which can have serious financial and reputational consequences.

The key to thriving in this expanding threat landscape isn't to demand even more of IT teams—rather, it's to establish a strong baseline of security in the form of a Zero Trust security model. This foundation of security relieves the pressure on IT teams and helps decrease the risk and severity of attacks—but that's just where the benefits begin.

This e-book examines the common security barriers in the modern era and discusses how implementing Zero Trust security helps organizations break past them. We'll also discuss the positive ripple effect created by having a Zero Trust security model and how it impacts team productivity and AI-readiness.

Top security challenges

Cyber adversaries are getting more sophisticated and organized, with malicious actors using advanced tools and tactics to find and exploit weaknesses. When cybercriminals are successful, the victim's reputational and financial damages can be severe—especially if the breach involves sensitive or personal data. Externally, the loss of trust from customers, partners, and investors can cause decreased market share, customer churn, and lowered valuation. Internally, cyberattacks disrupt operations, causing downtime, reduced productivity, and lost revenue.

The growing financial damage caused by cybercrime

$23.84T

The estimated cost of cybercrime worldwide is expected to reach **$23.84 trillion** by 2027.[2]

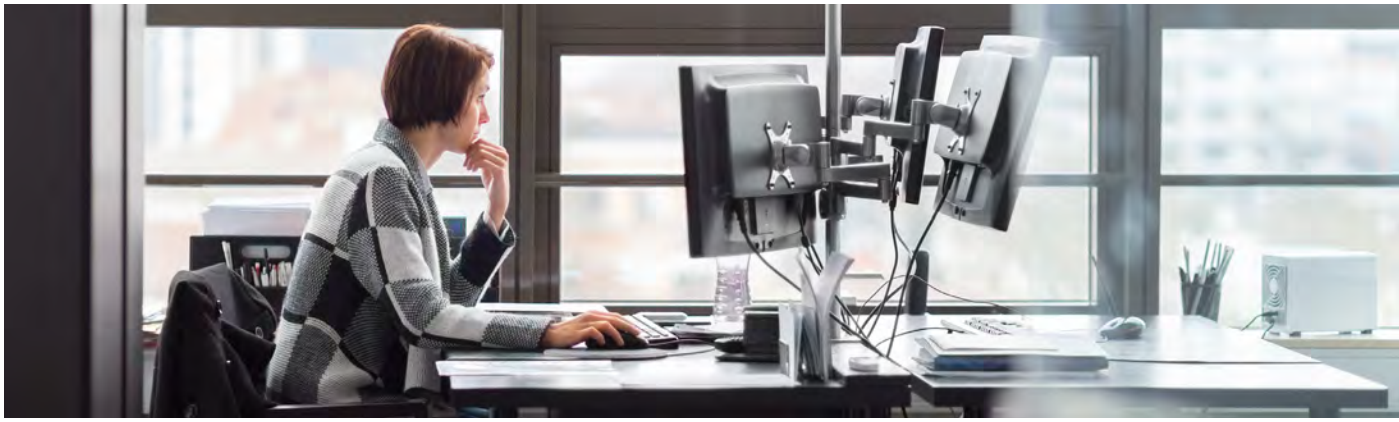
Key security concerns of the modern work era

In the face of these dire consequences, IT teams find themselves running up against several key challenges.

Verifying identity
Attackers use different techniques like phishing, malware, and domain spoofing to capture user credentials. These credentials (passwords, user IDs, emails, etc.) are then used to gain access to company resources, steal data, or compromise accounts.

1,287
Password attacks occur every second.[3]

31M
Phishing attacks rose to **31 million** per month in the past year.[4]



Protecting a modern workforce
Many businesses' work models have undergone rapid changes in recent years, with **12.7%** of full-time employees now working from home and **28.2%** using a hybrid model.[5] These employees don't always take the right precautions to defend against threats, which provides cybercriminals with more exploitable vulnerabilities. Meanwhile, working with outdated hardware and unmanaged devices that aren't compliant increases IT complexity, leaving organizations more vulnerable to attacks.

80–90%
Of successful ransomware compromises originate through unmanaged devices.[6]

71%
Of workers are more likely to be infected on an unmanaged device.[7]

86%
Of security leaders say outdated PC hardware leaves organizations more vulnerable.[8]

Protecting information

Cybercriminals will try to gain a competitive advantage by disrupting an organization's operations or stealing intellectual property like trade secrets, patents, trademarks, and copyrights. IP theft might be motivated by financial gain, economic espionage, or industrial sabotage. The more "table stakes" security issues an organization must deal with—software and firmware patches, hardware upgrades, and internal and external security vulnerabilities—the less time and effort they have to prepare for attacks targeting their most precious data.

70%

Of organizations have been compromised by unsanctioned software, apps, and services.[9]

62%

Of staff don't spend enough time on strategic work like security strategy or preparing for sophisticated attacks.[10]

Organizations must adopt a proactive and resilient approach to cybersecurity to navigate this complex and evolving threat landscape. Today, that means shifting from a traditional, reactive framework to a proactive, Zero Trust framework.

Step one
Establish a Zero Trust security foundation

Zero Trust is a security model that operates under the motto, "**Never trust, always verify.**" It recognizes that trust is a vulnerability that can be used to find exploitable points of entry and requires that you put up guardrails that ensure cybercriminals aren't unintentionally allowed through your defenses.

Never trust
Never implicitly trust any entity, whether internal or external.

Always verify
Require continuous verification of identity, device, data, and network.

Principles of Zero Trust

Instead of assuming everything behind your corporate firewall is trustworthy, Zero Trust security assumes that any entity (internal or external) trying to access organizational resources is a potential threat. This assumption makes it necessary to apply three principles: verify explicitly, implement least-privileged access, and assume breach.

Verify explicitly
The first principle is designed to make sure the person trying to access your network is who they say they are. Every access request to a resource is authenticated and authorized based on several factors, including the user's identity, their device, their location, the service or workload they're accessing, data classification, and any identified anomalies or risks. This ensures that valid users and devices can access to company resources, while suspicious entities are blocked or questioned.

Implement least-privilege access
This principle ensures that users get access to the resources they need to complete their tasks—and nothing more. This approach limits the exposure of sensitive data and resources to unauthorized or compromised users and devices and restricts the extent of damage an attacker can inflict within the network. Methods like just-in-time and just-enough access (JIT/JEA) policies, adaptive policies based on risk assessment, and data protection strategies help to enforce this principle.

Assume breach
This principle aims to minimize the damage a breach can do. Assuming breach involves segmenting access to resources, ensuring data encryption in transit and at rest, and using analytics for visibility, threat detection, and defense enhancement. This strategy is crucial to shrinking the blast radius of an attack and preventing attackers from moving laterally within the network if they happen to gain access.

Best practices for implementing Zero Trust principles: Protecting identities and endpoints

Building a secure foundation requires a modern productivity solution like Microsoft 365 E3. It includes built-in Zero Trust, AI, and automation capabilities to quickly verify identities, grant access to authorized users, and monitor for threats across multiple platforms. To establish Zero Trust security, look for comprehensive solutions with this critical foundation for protecting identities and endpoints to enable the best—and most secure—productivity for your workforce.

Protect identities

Employ multifactor authentication: Require users to confirm their identity through a second source (like a phone or token) before being granted access.

Enable passwordless authentication: Have users verify their identity without entering a password by requesting another form of evidence, like a fingerprint or a unique code.

Implement Single Sign-On (SSO): Remove the need to manage multiple credentials for the same person so workers encounter fewer sign-in prompts when using different applications.

Enrich your Identity and Access Management (IAM) solution with more data: Feed more data into your IAM solution to gain more visibility into who's accessing corporate resources.

Protect endpoints

Block legacy authentication: Prevent apps or devices from using old protocols that don't support modern security features so malicious actors can't gain access to resources using stolen or reused credentials.

Perform real-time risk assessments: Continuously verify and evaluate the risk level of every access request using AI, automation, and analytics to ensure anomalies are detected and mitigated in real time.

Continuously assess and optimize your security posture: Keep ahead of sophisticated threats by consistently assessing your identity and security posture to see how well your environment aligns with current best practices.

Benefits of implementing a Zero Trust security model

How applying the "never trust, always verify" model keeps you safer from cyberthreats

Achieve a stronger security posture
By minimizing the attack surface and blocking unapproved access, Zero Trust reduces the number of exploitable vulnerabilities caused by everyday operations. Plus, if a malicious actor manages to gain access, Zero Trust security helps detect their presence and proactively limit the damage they can do.

Enhance your ability to adapt a modern work productivity model
Zero Trust caters well to hybrid work models, offering secure access regardless of where or how employees work. This helps prevent productivity from grinding to a halt because workers can't access resources when they work in a new location or switch devices.

Simplified security management
Zero Trust simplifies security management by offering a comprehensive solution that covers identity, apps, devices, infrastructure, and data under consistent security and governance policies. Plus, by adding AI and automation to tasks like threat monitoring and risk assessment, Zero Trust helps simplify management even further, taking the pressure off IT teams so they have time to focus on strategic initiatives and innovation.

Respondents to a Foundry Zero Trust survey reported that implementing a Zero Trust model resulted in benefits impacting productivity, risk reduction, and compliance.[11]

Key benefits reported by survey respondents:

- Protecting customer data
- Continuous access and authentication
- Managing access to cloud apps and devices
- Facilitating the move to remote work
- Solving the security skills shortage
- Reducing the complexity of integration
- Reducing time to breach detection
  Delivering both security and an excellent end-user experience

Step two
Streamline endpoint management

After your organization has established a Zero Trust security foundation, you'll be able to adopt a simplified framework that allows IT admins to streamline endpoint management.

Endpoints encompass a range of devices used in everyday work operations, including desktop computers, laptops, tablets, mobile phones, IoT devices, and cloud solutions. The number of endpoints has been increasing by the year, with the average enterprise now having about **135,000** devices.[12] Managing and securing all of those diverse endpoints is a large (and expensive) task, with about 30% of IT help desk costs devoted to solving endpoint issues. Using a cloud-based productivity suite like Microsoft 365 E3 helps simplify endpoint management and reduce IT costs, even as the number of endpoint devices keeps growing.

What can you achieve with streamlined endpoint management?

Enhance employee experiences and productivity. Provide support for a wide range of apps, peripherals, devices, and self-service options so employees can work efficiently from anywhere.

Improve control of endpoint performance, health, and security. Keep devices updated with the latest operating system and security policies based on identity, location, compliance, and risk factors.

Reduce IT complexity. Drive IT efficiency by leveraging the cloud to simplify device and application deployment, configuration, and updates. The result is comprehensive management and security for endpoints across various operating systems, device types, and ownership models.

Once you've completed the two steps of establishing a Zero Trust foundation and streamlining endpoint management, the next objective comes into focus—unobstructed productivity and collaboration.

Microsoft 365 E3: Combining Zero Trust security and unified endpoint management for a powerfully productive workforce

In the past, organizations have had to strike a careful balance between security and productivity. If IT puts up too many security defenses, employees may find their productivity impacted as they struggle to access the necessary information and resources. On the other hand, if too few defenses are put in place, a single successful cyberattack could grind the entire operation to a halt.

Microsoft 365 E3 is a cloud-based productivity solution that offers foundational Zero Trust security, enterprise-grade device and app management, and robust collaboration tools. With built-in AI capabilities, it understands the context of your data and knowledge to empower secure productivity across your organization so employees are focused, connected, and secure at every level.

Microsoft 365 E3 capabilities

Identity and access management from a central location
Enable strong and adaptive access policies that allow users to get the resources they need without meeting friction points.

Information protection and governance
Keep data encrypted whether it's at rest, in transit, or in use, and easily discover sensitive information.

Automated threat protection
Automate updates to keep the software current, deploy patches quickly to reduce exploitable vulnerabilities, and proactively block threats from disrupting business continuity.

Elevating productivity: Microsoft Copilot for Microsoft 365

Using AI involves a lot of data gathered from different sources. Implementing Zero Trust security and seamless endpoint management are crucial steps to ensuring all that data is secure and easy to manage. Once that's accomplished, you'll be able to elevate productivity even further using tools like Microsoft Copilot.

Microsoft Copilot for Microsoft 365 is an AI-powered productivity tool that helps clear hours of mundane work by automating common tasks like creating documents, scheduling meetings, and managing projects. With those freed-up hours, employees have more time and energy for tasks that require focused creativity and innovative problem-solving.

Using AI to make space for creativity

70%

Of people would delegate as much work as possible to AI to lessen their workloads.[13]

Total Economic Impact

In a commissioned study conducted by Forrester Consulting, Microsoft 365 E3 was shown to strengthen security, enhance productivity, and simplify IT management.[14]

Strong security

35%

Reduction in likelihood of a data breach.

Productivity

60HR

Average of 60 hours saved per year with Microsoft 365 E3.

Simplified IT

25%

Reduced time spent deploying and managing new software by 25%.

Empower your enterprise with secure productivity from Microsoft 365.

Learn more ›

[1] IT Trends Report: Remote Work Drives Priorities in 2021. JumpCloud, 2021.
[2] Chart: Cybercrime Expected To Skyrocket in Coming Years. Statista. 2022.
[3] Microsoft Security Copilot: How does it help you protect your data? Intelequia. Apr 2023.
[4] Microsoft Entra: 5 identity priorities for 2023. Microsoft Security. Jan 2023.
[5] Remote Work Statistics & Trends In (2023). Forbes Advisor. 2023.
[6] Microsoft Digital Defense Report. 2023.
[7] Anatomy of a modern attack surface. Microsoft Security Insider. May 2023.
[8] Microsoft Security Signals Boost SDM Research Learnings. Hypothesis Group. Sep 2021.
[9] The State of Attack Surface Management 2022. Randori. 2022.
[10] Microsoft Digital Defense Report. 2022.
[11] Zero Trust Adoption Survey. Foundry. March 2022.
[12] Managing Risks and Costs at the Edge. Ponemon Institute. 2022.
[13] Work trend Index Annual Report: Will AI Fix Work? Microsoft. May 2023.
[14] The Total Economic Impact Of Microsoft 365 E3. A commissioned study conducted by Forrester Consulting, 2022.