safous

THE FUTURE OF CYBERSECURITY:

How MSPs Can Stay Ahead with Zero Trust

Table of Contents

Introduction

Businesses of all sizes face an onslaught of increasingly sophisticated cybersecurity threats, from malware and ransomware attacks to data breaches caused by third-party vendors. For managed service providers (MSPs), the stakes are especially high. As trusted IT partners to their clients, MSPs have extensive access to sensitive systems and data – and a cyberattack can disable multiple client networks at once.

To protect their clients in today's climate, MSPs need robust security solutions tailored to their unique environment. That's where Zero Trust Access (ZTA) comes in. ZTA is transforming traditional network security models and enabling MSPs to become trusted security advisors to their customers. In this guide, we'll explain how implementing a zero-trust framework can help MSPs secure access points, counter advanced threats, and position themselves as true cybersecurity partners.

How Is the Cybersecurity Threat Landscape Evolving?

Cyber threats aren't just growing in sophistication – they're growing in scale. Attackers are using advanced techniques like social engineering, credential stuffing, and ransomware to infiltrate corporate networks and extort businesses globally. Consider these statistics from 2023:

Cybercriminals used malware in **45% of reported cyberattacks,** with **56% of organizations** suffering a data breach as a result.[1]

Ransomware affected **66% of businesses** – and in **30% of attacks** where data was encrypted, data was also stolen.[2]

The average ransomware payout also increased dramatically, reaching **$1.5 million in 2023** from $812,380 in 2022.[3]

1. https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2023-q3/
2. https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf
3. https://www.varonis.com/blog/cybersecurity-statistics

The Role of Third-Party Vendors in the Threat Landscape

Third-party vendors like MSPs play a pivotal role in this evolving landscape. MSP teams need privileges to manage client systems and infrastructure, but this broad access also creates security risks. **Nearly 50% of organizations experienced a third-party data breach in 2022,**[4] highlighting the need for MSPs to ensure customer security by strengthening their own cybersecurity posture.

For MSPs, unsecured network access can damage client relationships and reputation overnight. An exploited MSP credential can grant attackers access to hundreds of customer networks. And once inside an MSP's critical systems, malware can spread downstream and disable the business operations of all affected clients.

4. https://security.imprivata.com/rs/413-FZZ-310/images/SL-Ponemon-Report-state-of-cs-and-third-party-access-risk-1122.pdf

What Is Zero Trust Access (ZTA)?

Zero Trust Access (ZTA) is a new security paradigm that overcomes the pitfalls of implicit trust models. As the name suggests, ZTA does not implicitly trust entities based on their apparent identity. Instead, it combines powerful authentication methods, network segmentation, least access policies, and more to help businesses:

Minimize the Attack Surface

By segmenting access and minimizing lateral movement across networks, ZTA reduces exposure to unauthorized access.

Reduce Data Breach Damage

ZTA solutions release only as much access needed to fulfill each request to ensure hackers can't compromise other data or systems.

Centralize Security Management

With ZTA, IT admins can control security and remote access policies company-wide from a central location.

Secure Hybrid Workforces

ZTA goes beyond traditional network perimeters to protect the entire workforce, regardless of where remote teams connect from.

How Does ZTA Represent a Paradigm Shift for MSPs?

For MSPs, adopting a zero-trust security approach opens new opportunities to better serve and protect their clients. Here's how:

Stronger Defenses

At its core, ZTA allows MSPs to improve security for client systems and data. Verification controls and least privilege access principles limit exposure from compromised credentials or endpoints, and its identity-based approach also contains threats before they can spread.

Differentiation

ZTA also allows MSPs to differentiate their offerings in a competitive market. Its cloud compatibility and focus on seamless user experience are key to helping businesses strengthen remote workforce security without compromising productivity or flexibility.

Revenue Opportunities

MSPs can create new revenue growth opportunities by transitioning clients to advanced zero trust-enabled security platforms. Plus, providing ongoing management services of zero-trust environments creates recurring revenue streams.

How Does ZTA Represent a Paradigm Shift for MSPs? (cont.)

Regulatory Compliance

ZTA solutions help MSPs and their clients aligns with many regulatory standards through its identity-centric access controls, comprehensive monitoring and logging capabilities, and data protection measures. By leveraging ZTA, MSPs can easily satisfy evolving data privacy regulations by demonstrating compliance with mandates for secure access, privileged action monitoring, and consistent enforcement of security policies across client environments.

Supply Chain Security

With ZTA solutions, MSPs can create secure and controlled IT and OT network environments for their clients that minimize the risk of supply chain attacks. ZTA enables businesses to continuously verify identities, restrict third-party access, segment critical systems, and more to reduce the attack surface and contain threats before they can propagate across the supply chain ecosystem.

Positioning MSPs as Trusted Security Partners

By embracing ZTA, MSPs can establish themselves as indispensable cybersecurity partners that clients depend on to navigate the evolving threat landscape. Follow these three steps to cement your MSP business as a security leader:

01

Secure Your Access Points

By segmenting access and minimizing lateral movement across networks, ZTA reduces exposure to unauthorized access.

02

Adopt Proactive Security

Continuously assess your and your clients' IT infrastructure and access policies to identify weaknesses before attackers do. Special care should be taken to detect and prevent the spread of ransomware.

03

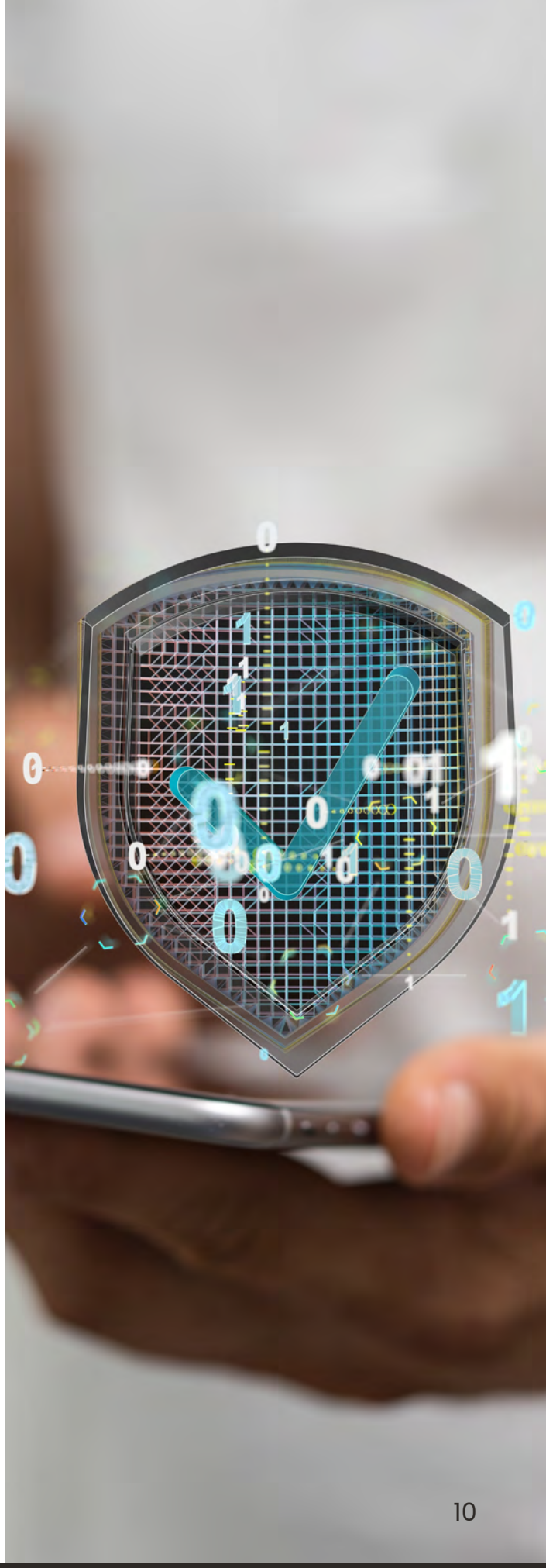
Offer Zero Trust Solutions

Help your clients protect their businesses with scalable zero trust cybersecurity solutions – from identifying vulnerable attack surfaces with a security assessment to safeguarding access points with Safous ZTA.

How MSPs Can Secure the Future With ZTA

Malware, ransomware, and third-party attacks are growing more frequent – and causing major financial and reputational damage to businesses of all shapes and sizes. As trusted partners, MSPs need to embrace more advanced solutions tailored for modern work environments to keep client networks, data, and systems secure.

ZTA has emerged as a security approach built to overcome the weaknesses of implicit trust models in today's dispersed IT ecosystems. By implementing continuous verification, granular access controls, and identity-centric policies, ZTA enables MSPs to provide adaptive security for their clients' hybrid workforces and cloud-centric environments.



Benefits of ZTA for MSPs

Leveraging a zero-trust approach to security helps MSPs:

Strengthen Security to Build Trust

Attackers capitalize on third-party vendor access, including MSPs, to gain a foothold in client systems and spread malware. Implementing ZTA solutions helps MSPs strengthen their security posture, reducing the risk of compromise and mitigating the potential for lateral movement within their networks and those of their clients.

Create Revenue Opportunities

Zero trust has become a popular buzzword in cybersecurity, and many end users are seeking solutions to implement this security model for their businesses. By positioning themselves as zero-trust experts, MSPs can create new revenue streams while addressing a critical cybersecurity need for customers.

Protect All Network Entry Points

In addition to third-party vendor access, MSPs must also secure privileged access management systems, remote maintenance solutions for industrial control systems (ICS) and operational technology (OT) environments, and any other points of entry into client networks. A zero trust architecture helps MSPs secure all potential attack vectors by enforcing strict access controls, continuous monitoring, and the principle of least privilege.

Why Should MSPs Partner With Safous for ZTA?

Safous offers MSPs a unified zero trust platform that secures the IT environment, operational technology (OT) systems, and public APIs within a single product. We specialize in critical access management, providing detailed access controls and audit trail features that aren't available in other ZTA solutions – and we go beyond zero-trust access to cover security assessments and automation capabilities.

By partnering with Safous for zero trust security, MSPs get:

- **Holistic Zero Trust Solutions:** Our ZTA platform provides a comprehensive security framework for MSPs, including those with a limited focus on cybersecurity.
- **Proactive Security Measures:** Leveraging our zero trust expertise enhances security offerings for more proactive threat prevention and a reduced burden on MSP partners.
- **Collaborative Partnership Model:** We promote a collaborative partnership model that fosters shared responsibilities and reduces over-dependence on our team.
- **Rapid Response and Resolution:** Our commitment to resolving issues quickly improves our MSP partners' operational efficiency and after-sales support to their clients.
- **No Unnecessary Upselling:** By delivering solutions tailored to meet end users' organizational needs, agents no longer need to frustrate customers with unnecessary upselling.
- **Open Access to Information:** We support interoperability and open standards, ensuring MSPs have unrestricted access to information about our ZTA platform.

SAFOUS:

The Complete Zero Trust Security Suite for MSPs

As a leading cybersecurity solutions provider, Safous offers a complete Zero Trust suite tailored for MSPs:

Security Assessment

Help your clients quickly identify and address security risks, eliminate weaknesses, and eliminate vulnerabilities with a **Safous Security Assessment.** In minutes, they'll receive a score-rated report that breaks down the security level of each attack surface on a domain-by-domain basis, plus the option to access specialized consulting from our security team.

Safous ZTA

Protect your clients' networks from cybersecurity threats with **Safous Zero Trust Access (ZTA)**, a zero-trust security platform designed to provide secure, seamless access to remote and hybrid employees. Our scalable ZTA solution combines legacy and modern systems to grow alongside your MSP offerings and support any sized project. Plus, it's easy to implement and configure, without requiring any additional endpoint software, browser plug-ins, or specific operating systems.

Ready to explore Safous' Zero Trust security suite – and see how we can enhance your cybersecurity posture?

Request a demo or **become a partner** today.

www.safous.com