WEI INSIGHTS
EXECUTIVE BRIEF

CRITICAL SUCCESS FACTORS OF AN INTEGRATED SECURITY STRATEGY

64% of IT decision makers ranked 'improving data security' as a top IT objective, up nearly 20% from the same survey conducted in 2018.[1]

As global industry evolves, digital innovation that features a hybrid, "from anywhere" business environment has become critical to modern workforces. New formats provide employees and external partners with dynamic access to digital resources, no matter when or where they choose to work.

But this new approach creates complications for CISOs and other IT executives because business applications and data leave traditional corporate perimeters. Specifically, it broadens the attack surface of internal networks. Combined with evolving threats, this factor dramatically expands the risk of potential breaches.

This executive brief explores how a zero-trust access (ZTA) approach to security featuring endpoint protection can help. We will show how ZTA provides the best modern approach to network security as user access at the "edge" becomes increasingly essential to business growth and success.

MITIGATING RISK AT THE EDGE

Conceptually, traditional security models feature "gateways" whereby permitted entry means users and devices can be trusted in perpetuity. But unpredictable and broadening access points render this traditional approach obsolete. Bad actors can steal credentials and access networks from any device, for example. This threat increases the complexity and risk of more frequent, more nuanced attacks.

ZTA is therefore critical to security as digital innovation continues. With ZTA, CISOs and other executives can ensure all users, devices, and applications are consistently authenticated, trustworthy, and managed. ZTA ensures users have only the correct frequency and depth of access as well.

WHAT IS ZTA WITH ENDPOINT PROTECTION?

The ZTA framework features a combination of security solutions that continuously and holistically identify, authenticate, and segment users and devices seeking network and application access. With these capabilities, security teams can:

- establish identity through multiple authentication and certificate measures
- enable role-based privileged access
- ensure ongoing network control through automated orchestration and threat response
- optimize the user experience, even with rigorous security measures

But by 2019, only 15% of organizations had completed a transition to a zero-trust security model, indicating a substantial opportunity for growth.[2] What follows are details on the key capabilities and features that make ZTA with endpoint protection a critical aspect of successful integrated security strategies for modern enterprises.

ESSENTIAL ZERO-TRUST ACCESS CAPABILITIES FOR MODERN IT SECURITY

ZTA does more than offer superior security as enterprise attack surfaces expand. Enterprises that incorporate ZTA with endpoint protection as part of their integrated security strategy also enjoy the flexibility to support their business needs, beyond traditional security models.

Next, we discuss three capabilities that optimize security and workflows on expanded networks—helping IT executives uphold their security responsibilities even as business ingenuity continues. Discover how with rigorous access controls, ZTA with endpoint protection enables devices, users, SaaS, and other network elements to remain protected under any circumstances.

1. Authentication for Every Device, Every Time

Unlike traditional perimeter models, a ZTA-based security strategy assumes every user and device poses a risk. In this paradigm, ZTA authenticates every device before access is authorized. Because ZTA provides a seamless experience for users, automated security features can continuously authenticate devices every time a new or familiar device requests access, without adding friction to user workflows.

2. Role-Based Access for Every User

In this paradigm, security teams continuously monitor every user, no matter the user's apparent risk. As part of this approach, security teams have visibility into the role-based access of every user, emphasizing a "least access policy" whereby users only access resources that are necessary for their roles.

3. Asset Protection, On and Off Network

Increased remote and mobile activity among users means that there is a greater risk they will expose their devices to bad actors. In doing so, they expose organizational resources to security threats, whether they realize a risk is present or not.

SOLUTION SPOTLIGHT:

FORTINET ZERO-TRUST NETWORK ACCESS (ZTNA)

Improve Security with a Zero-Trust Access Approach

Fortinet uses a tightly integrated collection of security solutions that help organizations identify and classify all users and devices that seek network and application access, including:

- Endpoint access control
- Identity and access management
- Network access control
- Application access control

4 Key Benefits of the Fortinet ZTA Framework

1. Complete and continuous control over who is accessing applications
2. Complete and continuous control over who AND what is on the network
3. Integrated ZTA solution for Fortinet Security Fabric that works on-premises and in the cloud over LAN, WAN, and remote tunnels
4. A complete, integrated solution coming from one vendor

FORTINET®

The ZTA approach improves endpoint visibility to protect against the risks associated with remote endpoint devices. Endpoint security measures share security telemetry data each time the device reconnects to the enterprise network. This provides security teams with visibility into vulnerabilities and threats, as well as into missing security patches and missing updates to role-based access, when applicable.

5 ESSENTIAL FEATURES OF TODAY'S LEADING ZERO-TRUST ACCESS FRAMEWORKS

Once CISOs and other IT executives understand the rationale behind ZTA frameworks, they must understand the ZTA market and the leading features each solution provides. Generally, a ZTA framework is an ensemble of security solutions that manage network access for users and devices, assess compliance and risk, and streamline role-based access and monitoring, among other capabilities.

Consider the following five essential features as you review the leading solutions available today:

1. Automated Discovery & Classification

Network access control discovers and identifies every device on, or seeking access to, the network. The system automatically scans those devices to ensure they are not compromised, then classifies each device by role and function.

2. Zone-of-Control Assignment

The system automatically assigns users to role-based zones of control where they can be monitored continuously, both on and off network. Network access control micro-segments users in mixed environments featuring vendors, partners, contingent workers, and others in addition to employees, supporting robust capabilities even as companies expand the edge.

3. Continuous Monitoring

This feature is founded on the premise that no single user or device can be trusted—even after authentication, a device may be infected or a user's credentials could have been compromised. ZTA frameworks continuously monitor users and devices, imposing streamlined authentication at every point of access as a result.

4. Secure Remote Access

The ZTA framework provides users with safe but flexible options for VPN connectivity, improving the user experience even as it imposes more robust security features. The framework also ensures internet-based transactions cannot backflow into each VPN connection, which would put the enterprise at risk.

5. Endpoint Access Control

The framework uses proactive visibility, defense, and control to strengthen endpoint security. Discovering, assessing, and continuously monitoring endpoint risk streamlines endpoint risk mitigation, risk exposure, and compliance. The framework supports encrypted connections across unsafe networks and continuously retrieves telemetry data to measure endpoint security statuses as well.

CONSIDER FORTINET FOR A FULLY INTEGRATED SECURITY STRATEGY

As an IT leader, your ultimate responsibility is not only to keep your company, resources, and users secure but also to help users innovate, improve the bottom line with new efficiencies, and generally meet the needs of the business. That's why the experts at WEI recommend Fortinet to IT and security executives who are re-thinking their approach to enterprise security as risks and business requirements evolve.

Fortinet is among the world's leading platforms for ZTA-based security with endpoint protection. Fortinet constitutes a tight integration of security solutions that optimize network and application access as part of a more streamlined and approachable workforce enablement. Featuring comprehensive visibility and control across infrastructure, users, and devices, Fortinet provides security leaders with the capabilities they need to both protect enterprise resources and enable modern workforces—no matter the location of each user or device.

TALK TO WEI TODAY

Navigating the enterprise security technology landscape can be overwhelming given the amount of solutions available today. Consult with the security experts at WEI to help cut through the noise, improve your security posture and find the right mix of solutions to establish an integrated security strategy you can trust. Contact us today to start a conversation.

Sources:

1. IDG Research commissioned by WEI, January 2021.
2. Cybersecurity Insiders. Zero Trust Adoption Report, 2019. https://www.cybersecurity-insiders.com/portfolio/2019-zero-trust-adoption-report.

ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. *Because we go further.*

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 30 years.