LEARNING MADE EASY

4th Fortinet Special Edition

Zero Trust Access

for dummies®
A Wiley Brand

Securing the new hybrid workforce

Reducing the attack surface and lateral movement

Improving application access and security

Brought to you by:

FORTINET

Lawrence Miller

About Fortinet

Fortinet (NASDAQ: FTNT) is a driving force in the evolution of cybersecurity and the convergence of networking and security. Our mission is to secure people, devices, and data everywhere, and today we deliver cybersecurity everywhere you need it with the largest integrated portfolio of over 50 enterprise-grade products. Well over half a million customers trust Fortinet's solutions, which are among the most deployed, most patented, and most validated in the industry. The Fortinet Training Institute, one of the largest and broadest training programs in the industry, is dedicated to making cybersecurity training and new career opportunities available to everyone. FortiGuard Labs, Fortinet's elite threat intelligence and research organization, develops and utilizes leading-edge machine learning and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence. Learn more at https://www.fortinet.com, the Fortinet Blog, and FortiGuard Labs.

Zero Trust Access

4th Fortinet Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

Zero Trust Access For Dummies®, 4th Fortinet Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-39073-1 (pbk); ISBN 978-1-394-39074-8 (ebk); ISBN 978-1-394-39075-5 (ebk)

Publisher's Acknowledgments

Acquisitions Editor: Traci Martin
Senior Managing Editor: Rev Mengle
Senior Account Manager: Cynthia Tweed
Content Refinement Specialist: Magesh Elangovan

Table of Contents

Introduction

As businesses continue to embrace digital innovation, artificial intelligence (AI), and cloud applications and as hybrid work becomes the norm, enterprise networks have become far more complicated and dispersed with an ever-growing number of edges. As a result, the network perimeter has all but disappeared. As more people and devices connect to the network from more places, the traditional perimeter-based approach to security — protecting the trusted corporate network from the untrusted Internet — has grown to be almost ineffective.

To protect this greatly expanded attack surface from modern threats including AI enhanced attacks, organizations must implement a "never trust, always verify" zero-trust model that incorporates rigorous access controls across the distributed network so that users, devices, endpoints, clouds, and infrastructure are all protected.

To successfully implement a zero trust access (ZTA) strategy, organizations must implement tightly integrated security solutions that deliver robust identity and access management, endpoint access control, network access control, and application access control to users and endpoints working from anywhere.

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but this book assumes a few things nonetheless! Mainly, that you're a chief information officer (CIO), chief information security officer (CISO), vice president, architect, engineer, or administrator working on an enterprise security, networking, or infrastructure team. As such, this book is written primarily for technical readers with at least a basic understanding of security and networking technologies and challenges.

If any of these assumptions describe you, then this is the book for you! If none of these assumptions describe you, keep reading anyway! It's a great book and when you finish reading it, you'll have complete trust in your knowledge of zero trust!

Icons Used in This Book

Throughout this book, you will see special icons that call attention to important information. Here's what to expect.

REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with birthdays and anniversaries!

TECHNICAL STUFF

This icon explains the jargon beneath the jargon and is the stuff legends — well, legendary nerds — are made of.

TIP

Tips are appreciated, but never expected — you'll appreciate these useful nuggets of information and helpful advice.

WARNING

These alerts point out the stuff your mother warned you about (well, probably not, but they do offer practical advice to help you avoid potentially costly or frustrating mistakes).

CASE STUDY

Case studies about organizations using ZTA.

Beyond the Book

There's only so much space in this short book, so if you find yourself at the end of this book wondering, "Where can I learn more?" go to `https://fortinet.com`.

IN THIS CHAPTER

- Recognizing modern threats
- Going beyond traditional access control
- Defining zero-trust concepts
- Reaping the benefits of zero trust

Chapter 1
Understanding the Need for Zero Trust

In this chapter, you learn how threat actors take advantage of the disappearing network perimeter and expanding attack surface to bypass traditional access controls, and how zero trust overcomes these challenges.

Surveying the Modern Threat Landscape

In today's digital enterprises, business applications and data are dispersed far and wide, away from corporate data centers, so that users now have greater access to corporate resources using more endpoints from many locations. The rapid growth of Internet of Things (IoT) devices and corporate bring-your-own-device (BYOD) initiatives have led to a proliferation of access points and endpoint devices on the network. As a result, the traditional network perimeter is disappearing — and the attack surface is expanding. At the same time, cyberthreats are growing more prolific, and attackers' tactics and techniques are evolving and becoming more sophisticated.

Semiconductor Digest predicts that by 2030 there will be 125 billion IoT-connected devices worldwide; other industry forecasts project there will be more than 75 billion IoT-connected devices by 2025.

Traditional security models work under the assumption that anything inside an organization's network should be trusted. But automatically extending trust to any device or user puts the organization at risk if either is compromised, whether intentionally or unintentionally. Attackers, malware, and compromised devices that bypass edge security checkpoints often have unrestricted access to the network because of this inherent trust model. Exploits, such as credential theft and malware, enable attackers to gain access to legitimate accounts. Once inside the network, they can move laterally and take advantage of the trusted internal network to target an organization's resources.

WARNING

According to the Verizon 2024 *Data Breach Investigations Report* (DBIR), 65 percent of breaches in the previous year involved external actors — a drop of almost 20 percent from the previous year. Unfortunately, the number of breaches involving internal actors climbed from 20 percent to 35 percent, although almost two thirds of internal involvement was related to errors. However, motivation behind the breaches remaned steady — 95 percent of those breaches were financially motivated. Use of stolen credential remained the top avenue for attackers to access an organization. Ransomware was a close second.

As companies modernize their networks to accommodate remote workers, multicloud architectures, artificial intelligence (AI), and digital innovation, their approaches to security need to change as well.

Recognizing the Limitations of Traditional Access Control

Traditional access control strategies inherently trust a user or device on the network. This notion of trust is often based on the user or device's location: If they're on the network, they're trusted. But as the network perimeter continues to disappear, it becomes increasingly impossible to secure network resources. Users are now accessing the corporate network from home offices

and mobile devices. Corporate resources are also increasingly located in multiple locations, beyond the traditional network, such as on private and public clouds.

To overcome the limitations of traditional access control, organizations need a solution that provides:

- Ongoing verification of users and devices
- Granular segmentation of the network to create zones of control, which helps limit the impact of a breach and establishes more control points
- Least-privilege access for users and devices, so users are only granted the access they need to perform their roles, which helps to limit the impact of a compromised identity or device

WARNING

Today's networks have vast, dynamic, and in some cases, even temporary edges. The fact that many devices are often offline makes continuously assessing risk and trust even more difficult. Because there's no way to verify that users or devices on or off the network can be trusted, you should assume that every device on the network is potentially infected.

Looking at Zero-Trust Basics

The zero-trust model is a concept that was introduced by John Kindervag while he worked at Forrester Research in 2009. The fundamental principle underpinning zero trust is "never trust, always verify." Zero trust challenges the traditional perimeter-based security model in which a firewall protects the trusted corporate network from the untrusted Internet.

To be fair, the perimeter-based model isn't as black and white as labeling things either trusted or untrusted. Over the years, the perimeter-based approach has been tweaked here and there. For example, demilitarized zones (DMZs) are typically created for public-facing websites and applications that are "somewhat trusted" — shades of gray, if you will. Virtual private networks (VPNs) are used to extend (or punch holes in, depending on your perspective) the corporate network to remote and mobile users. And virtual local area networks (VLANs) and access controls are used to segment sensitive departments, such as human resources and finance, from the rest of the network.

But the perimeter-based approach to security has an inherent drawback: It grants excessive implicit trust. Once you're connected, whether directly or using a VPN, you're then trusted alongside the rest of the internal network.

REMEMBER

The zero-trust model moves security away from implied trust that's based on the network location of a user or device. Instead, trust is evaluated on a per-transaction basis and then monitored with ongoing verifications. With zero trust, your network location or IP address no longer conveys an implication of trust. Instead, the zero-trust model requires trust to be explicitly derived from a combination of identity and context-based controls at a very granular level that grants access based on the security principles of least privilege and need to know.

Zero trust starts with a default deny posture for everyone and everything — that is, zero trust. In a zero-trust model, whenever a user or device requests access to a resource, their identity must be verified before access is granted. Verification is based not only on the identity of the user and/or device, but other attributes as well, including context (such as date and time), geolocation, and device security posture.

However, access isn't a "one and done" deal. Just because a user or device has been granted access to a resource doesn't mean they can roam about freely on the network. Access is granted at a very granular level. It's only given to the resource needed to perform a specific function for a limited time — not to the entire network. A key element of the zero-trust model is that trust must be continually reevaluated. If important attributes of the user or device change, the trust may be revoked and access to the resource removed.

Zero trust access (ZTA) builds on the zero-trust model and focuses on knowing and controlling who and what is accessing the network. Role-based access control (RBAC) is a critical component of ZTA. Only by knowing definitively who a user is can the appropriate level of access be granted based on their role. ZTA covers user endpoints where management control and visibility are required. Aligning to the zero-trust model means implementing a least-access policy that grants the user the minimum level of network access required for their role and removes any ability to access or see other parts of the network.

TIP

In addition to knowing who and what is on the network, ZTA incorporates security for what is on the network. The ever-growing number of network-connected devices now includes IoT devices. These "headless" devices don't have usernames and passwords to identify themselves and their roles on the network. Instead, network access control (NAC) solutions can be used to discover and control access for these devices. Using NAC policies, the zero-trust principle of least access can be applied to these IoT devices, granting sufficient network access to perform their role and nothing more.

Zero-trust network access (ZTNA) is an element of ZTA that controls access to applications regardless of where the user or application is located. The user may be on a corporate network, working from home, or someplace else. The application may be hosted in a corporate data center or in a private or public cloud. Universal ZTNA provides consistent security and simplified user experience from all user locations and goes beyond cloud-based ZTNA solutions that focus on remote users.

REMEMBER

ZTNA is the natural evolution of the VPN. Given the complexity of today's networks, ZTNA offers better security, more granular control, and a better user experience than a traditional VPN. You can learn more about ZTNA in Chapter 5.

Realizing the Benefits of Zero Trust

For effective security in the modern threat landscape, organizations must shift from trying to protect dynamic network perimeters to instead protecting applications and data spread across potentially billions of edges, users, systems, devices, and other critical resources. A zero-trust strategy provides comprehensive visibility and protection across devices, users, endpoint, cloud, and infrastructure with a "never trust, always verify" approach to security.

Zero trust delivers the following benefits for organizations:

- **Reduces risk:** When you automatically extend trust to any device or user in your network, you put your organization at risk when either becomes compromised, whether intentionally or unintentionally. Zero trust eliminates

points of vulnerability by limiting network access for users, as well as by adopting extensive identity verification so that they only have access to the data and systems relevant to their role or position in the organization.

- **Increases visibility:** You know who and what is connected to the network at all times.
- **Extends security:** Security can be extended beyond the network with ZTNA. Unlike a VPN, which focuses exclusively on the network layer, ZTNA goes up a layer, effectively providing application security independent of the network.

IN THIS CHAPTER

- Trusting your users with strong authentication
- Using RBAC to enforce least privilege
- Keeping privileged access secure

Chapter 2
Establishing IAM as a Foundation for Zero Trust

The first step in securing your network resources with zero trust access (ZTA) is to trust your users with verification before granting access. In this chapter, you learn why identity and access management (IAM) is the cornerstone of ZTA, how to manage privileged access on the network, and the role of role-based access control (RBAC) in enforcing the principal of least privilege.

Knowing Who Connects to Your Network

Security teams need to know who is on the network at all times. It's critical for organizations to know every user and what role that user plays in the company, so IT can securely grant access to only those resources necessary for each role or job when needed.

However, organizations are at an increased risk from users that connect to their networks with weak passwords. Because so many online accounts today require user credentials, passwords are

often too simple or are reused across multiple accounts, making them easy for attackers to compromise using exploits like phishing and social engineering. Even when organizations require complex passwords for their users, passwords alone aren't enough.

Strong authentication, or multifactor authentication (MFA), refers to using multiple factors to verify that a user is who they say they are through a combination of factors, such as:

- Something you know (for example, a user ID and password)
- Something you have (for example, a hardware or software token, or a digital certificate installed on a device)
- Something you are (for example, a biometric indicator such as a fingerprint or iris pattern)

Adaptive or contextual authentication evaluates additional user attributes during a login attempt, such as time of day, geographic location, and/or network (trusted or untrusted) to assess the risk before allowing access. This technique can be used to either:

- Allow user access when the risk is deemed to be low
- Require two-factor authentication (2FA) when the risk is deemed to be high

For example, using the network attribute of the adaptive authentication, the system won't prompt an onsite user for 2FA because they're on the corporate network. However, the same user logging in from a public or home network and attempting to access corporate resources would be prompted for 2FA to further verify the user's identity.


TECHNICAL STUFF

Fast Identity Online (FIDO) provides the most secure and fastest login experiences for online applications and services. FIDO supports both Universal Authentication Frameworks (UAF, that is *passwordless authentication*) and Universal 2nd Factor (U2F, that is *universal two-factor authentication*).

Another challenge facing organizations today is the geographically dispersed workforce. Employees work from various locations such as the main office, branch offices, and home offices. To support the evolving nature of work — including work-from-home and work-from-anywhere in the wake of the global pandemic and the more recent calls to return to the office — plus

the ongoing move to the cloud, organizations need better ways to securely connect their employees to critical business applications.

WARNING

Attacks against endpoint devices are increasing. According to a recent Ponemon Institute report, 61 percent of respondents say the frequency of attacks against endpoints has increased over the past 12 months.

Today, there is practically no standardization of device configurations for personal mobile devices permitted in bring your own device (BYOD) environments. Network risks associated with BYOD mobile devices include:

- Data leakage
- Unsecured Wi-Fi
- Network spoofing
- Unpatched vulnerabilities on rooted or jailbroken devices
- Malware and spyware
- Broken cryptography
- Improper session handling

Finally, organizations are at risk when access permissions are based on assumed trust of previously vetted devices. Many organizations have been breached by former employees and contractors. A lost or stolen device can reveal passwords that enable a breach on the network. This is why a zero-trust approach to security is so critical. As cybercriminals focus on compromising the broad array of network devices, security teams need better visibility and detection of every device connecting to the network.

Today's enterprise identity environments are made up of various systems that may include networking devices, servers, directory services, and cloud applications. Managing an identity that resides in these various systems can quickly grow into such a large administrative challenge that it negatively affects users, administrators, and application developers. Federated identity is a solution that enables users from a group of linked organizations to share the same user verification method to various applications and resources. It does this by connecting users' online identities across multiple domains and networks. Federated identity solves several common access and security issues for organizations. Organizations can manage user access and provide easy access to

applications by using security tools like MFA and single sign-on (SSO). An example of federated access is an organization enabling users to access partner websites, Active Directory, and web applications without having to log in every time.

TIP

A robust IAM solution should have the following capabilities:

- Establish identity through login, MFA, and digital certificates, which may evolve to add contextual authentication.
- Support both hardware and software token options for MFA, as well as FIDO, UAF, and U2F.
- Provide role-based information from an authentication source for use in privileged access.
- Establish and enforce role-based least privilege access policies.
- Provide added security with support for SSO to help improve user compliance and adoption.
- Leverage Security Assertion Markup Language (SAML) to authenticate users for access to cloud-based software-as-a-service (SaaS) applications.
- Verify zero trust network access (ZTNA) connections for devices and users on a per-session basis to individual applications.

Enforcing Role-Based Least Privilege Access

Managing individual user account permissions for just a few hundred users can be a daunting challenge. In an enterprise with thousands of users it can be impossible to manage. RBAC enables IT administrators to manage the permissions assigned to users more efficiently by assigning sets of permissions to groups or roles. In this way, users in an entire department, for example, can quickly be assigned access to a sensitive financial application or network file share. Additionally, as users rotate through different job roles (for example, due to promotions or transfers), administrators can

easily revoke the permissions associated with the old role and assign permissions associated with the new role. Active Directory frequently plays a key role in RBAC administration.


REMEMBER

However, RBAC can be a double-edged sword. Roles must be clearly defined and assigned only the minimum permissions necessary to perform the required functions for that role. This is the principle of *least privilege.* If roles are too broadly defined, large groups of users may be assigned excessive permissions in an effort to address everyone's needs with a broad brushstroke. Roles that are poorly defined may be easily misunderstood, resulting in users being improperly assigned to roles. Finally, roles must be actively managed to ensure they're revoked and assigned appropriately, and to ensure the permissions associated with roles reflect changes in the organization and/or IT infrastructure. Failure to revoke roles or permissions can cause "permission creep" within the organization, resulting in excessive permissions for large groups of users.

Managing Privileged Access

Accounts that have privileged access permissions associated with them are particularly valuable targets for attackers. These accounts typically have access to critical systems and resources on the network, as well as confidential or sensitive data. Privileged access allows the user to make administrative changes to systems, applications, and network and security infrastructure such as installing software (or malware), altering (or deleting) critical system files or data, creating new accounts, and resetting user passwords. It's important to have controls mechanisms, such as privileged access management (PAM), in place to provide secure access to critical systems and resources and enforce zero-trust principles, such as least privilege.


TECHNICAL STUFF

Privileged access permissions may be assigned to accounts or roles used by humans such as domain administrators, local administrators, emergency "break glass" accounts, superusers, and privileged business users. Privileged access permissions may also be assigned to accounts that are not used by humans such as application and service accounts.

PAM is a subset of IAM. Whereas IAM is used to authenticate and authorize all of an organization's users, PAM is specifically focused on managing and securing administrator and user accounts with elevated privileges (that is, privileged access). PAM tools should go beyond just providing secure access to critical systems and resources; they also need to provide capabilities to monitor privileged access for auditing purposes. Going further still, advanced PAM tools will incorporate ZTNA controls to ensure that the security posture of the user's device meets the organization's requirements before allowing access to critical systems and resources, and scanning any attempts to upload malicious files.

IN THIS CHAPTER

- Exploring the evolving capabilities of EDR
- Making EDR part of a zero-trust strategy

Chapter 3
Leveraging Endpoint Security for Zero Trust

Endpoints — including computers, servers, mobiles, and even Internet of Things (IoT) devices — comprise the single largest attack vector in an enterprise IT environment. Attackers target endpoints because endpoints generally have a wider attack surface and are less robust in terms of security in the data center. Additionally, day-to-day security decisions on the endpoint — such as whether or not to download and install an unknown file, open a potentially malicious email attachment, or click on a suspicious link — are often left to the end user.

In this chapter, you learn how endpoint detection and response (EDR) has evolved from a rudimentary tool for manually investigating incidents to a highly automated detection and remediation endpoint solution, and why EDR is critical to an effective zero-trust strategy.

The Evolution of Endpoint Detection and Response

Endpoint protection has traditionally been focused on preventing malware and other known threats from infecting a desktop or laptop PC. For as long as these devices have been around, users have been admonished to run antivirus software and keep it up to date. Over the years, antivirus software evolved into antimalware software or endpoint protection platforms (EPP) to broadly encompass other forms of malware, including worms, Trojans, spyware, rootkits, exploits, and more. While antimalware tools have improved since their introduction, increasingly leveraging machine learning and behavioral analytics to prevent both known and unknown threats from infecting a PC, the reality is that prevention isn't always possible. This is because attackers are constantly developing new, sophisticated techniques that can bypass signature-based detection, exploit zero-day vulnerabilities, or use fileless and living-off-the-land (LotL) tactics.

REMEMBER

When prevention fails, EDR provides the tools for security teams to detect and respond to threats on endpoints and the network within real time. Unfortunately, early EDR solutions were too slow and complex to operate in a fast-paced and dynamic threat environment. These first-generation EDR solutions required highly skilled security teams to run manual queries to search for specific indicators of compromise (IoCs) and then manually triage and respond to threats. Most organizations simply don't have the skilled resources necessary to effectively operate these EDR tools, which would also produce false positives.

First-generation EDR solutions evolved with the addition of some key bolt-on functionality including:

- **Threat intelligence:** Automated correlation of endpoint telemetry to IoCs from threat intelligence feeds reduces the need for manual queries to detect threats.
- **Attack visualization:** Threats can be mapped to help analysts get a more complete picture of an attack in progress or an attack that has already happened.

- **Automated remediation:** Basic response capabilities typically include the capability to block specific IP addresses and processes, isolate endpoints from the network, and query the endpoint for additional data.
- **Threat hunting:** Advanced search capabilities and access to forensic data enables proactive threat hunting.

TIP

Second-generation EDR solutions offer greater visibility of endpoints and network environment, built-in or tight integration with prevention tools (such as antimalware), and policy-based automated risk mitigation using customizable playbooks. An example of a playbook action could be to block specific outbound attack communications, automatically roll back any system damage from ransomware, or stop lateral movement. These capabilities enable rapid detection and automated remediation of threats in real-time, and complete forensic investigative analysis.

Third-generation EDR is known as extended detection and response (XDR). XDR collects, normalizes, and then correlates data over a variety of security layers, including endpoints, firewalls, email, servers, cloud workloads, and the general network. XDR is a new, alternative approach to traditional detection and incident response, integrating detection and response procedures across multiple environments to reduce the meantime to detect and repair attacks.

Well-designed threats can be hard to detect because they work between security silos, which are multiple security approaches that work in parallel but not necessarily together. Due to their ability to lurk between security silos, such threats can spread or multiply as time goes by. As a result, they may evade the attention of a security operations center (SOC) and end up causing a great deal of damage.

REMEMBER

XDR isolates and dissects these threats. It collects, then correlates each detection according to individual security layers. Each "layer" represents a different attack surface: endpoints, email, network, servers, and cloud workloads.

EDR and Zero Trust

EDR is an essential component in a zero-trust strategy, enabling organizations to extend the "never trust, always verify" security posture of zero trust to their endpoints.

EDR serves as a central tool for collecting, organizing, and analyzing data from the endpoints connected to its network, which can report back their security postures for zero-trust tagging. EDR can coordinate alerts and automate responses to threats. This involves the incorporation of three elements:

- **Endpoint data collection agents** monitor endpoints and collect data. This includes data about processes, activity and alerts on the endpoint, connections to the endpoint, and data transferred to and from the endpoint.
- **Analysis of endpoint data in real time** enables EDR to diagnose threats quickly — even if they don't necessarily match preconfigured threat parameters. Analysis also uses forensic tools to examine the nature of the threat and determine how the attack was executed.
- **Automated incident response** uses custom policy-based rules. The automated response can identify threats and then perform an automated response. For instance, sending an alert that the endpoint's user is infected and will be logged out, logging them out, and then quarantining the endpoint.

These three elements of EDR work together as part of an effective zero-trust strategy to enable detection, investigation, containment, and eradication of threats in your endpoint and network environment.

Detection

When a threat evades the preventive controls on your endpoints and breaches your network environment, rapid detection is critical to minimize damage. However, detection can be challenging, particularly when you're dealing with an advanced threat that has evaded your endpoint protection tools. EDR uses continuous behavior analysis coupled with threat intelligence to rapidly

detect threats. EDR examines each process that interacts with the endpoint and can flag any script, code, files, or other items that may present a threat. Threat intelligence leverages a combination of artificial intelligence (AI) and large repositories of past and current threat data to detect threats that are targeting your endpoints.

Containment

Once a threat has been detected, EDR contains to prevent the threat from spreading across the network. This involves isolating specific areas of the network so that a threat can't infiltrate adjacent network elements. In addition to segmentation, an EDR solution also contains the threat itself by isolating the endpoint. Containment is important when it comes to ransomware. Because ransomware can hold an endpoint hostage, it needs to be contained to prevent other endpoints from getting infected.

Elimination

Although the other facets of EDR provide critical knowledge about the threat, that information is useless if it isn't employed to eliminate the threat — and similar threats in the future. The elimination process depends on gathering information about the threat and then using it to execute an action plan. For example, the system has to figure out where the threat came from and where it went. Information about the threat's origin can be used to enhance future security measures. The system also needs to pinpoint the applications and data, the malicious file affected, as well as whether the file or code has replicated itself to continue its attack.

After this information is collected, EDR actively removes the threat by deleting malicious files, stopping harmful processes, and restoring the system. It also updates security policies and blocks known indicators of compromise to prevent future attacks.

Integration

In the past, EPP solutions were purchased like other security or networking products and operated within their own silos. Remediating threats was made difficult because none of these solutions (including email security, firewalls, network access control,

or others) could talk to or interface with each other. Integrating such solutions using zero-trust architectures enables an EDR to automatically conduct remediation steps such as blocking malicious addresses on firewalls, blocking phishing email addresses, or taking infected devices onto remediation VLANs. Even if your organization doesn't choose to automatically remediate threats, you can automate the response *after* you agree that a threat is malicious. Your EDR can then initiate automated responses that save time, reduce tickets, and ultimately reduce the meantime to detect and repair.

IN THIS CHAPTER

- Knowing what is connected to the network
- Gaining visibility and control of devices
- Implementing automated response and network orchestration

Chapter 4
Bringing Zero Trust to Device Security

If cybercriminals were to write a book titled *The Seven Habits of Highly Effective Hackers*, there would definitely be a chapter called "Begin with the Endpoint in Mind." Endpoints are a preferred initial attack vector for cybercriminals to gain access to more valuable network resources. In this chapter, you learn how to apply a zero-trust strategy to your device security.

Discovering and Identifying Devices

In addition to knowing who is on the network (discussed in Chapter 2), organizations need to know what devices are on the network. These devices include:

- Networked office equipment (such as printers)
- Specialized devices (for example, medical equipment, surveillance cameras, and point-of-sale systems)

- Operational technology (OT)
- Internet of Things (IoT) sensors and devices

REMEMBER

The challenge in protecting all these devices lies in their distributed deployment, the various tools for device management, inconsistent network access controls, and the lack of standard communication protocols in many legacy devices.

The traditional network perimeter has all but disappeared as the proliferation of devices connecting to the network has created an exponentially larger attack surface for organizations to protect, with every device essentially constituting a microperimeter. The result of this explosion of devices and the expanding attack surface is that many organizations are losing visibility and control of the devices connecting to their networks. And because each microperimeter is associated with an individual device, these devices have become prime targets for malware infections and sophisticated exploits.

WARNING

Attacks against IoT devices are increasing, and the scale and impact of a successful IoT attack can be devastating. For example, the Cybersecurity Infrastructure and Security Agency (CISA), working with several industry security firms, recently discovered a vulnerability in millions of IoT smart camera devices that allows an attacker to gain access to the cameras, watch live video feeds, and create botnets.

Cyberattacks on IoT devices are booming as organizations connect more and more smart devices to their networks. Attackers exploit these devices to conduct distributed denial-of-service (DDoS) attacks and other malicious activities.

REMEMBER

To secure end devices, enterprises must have full visibility into what the connected device is, where it is, what it does, and how it connects to other devices across the network topology. Lack of visibility leaves an organization vulnerable to unseen risks, and many organizations don't have a strategy in place to deal with attacks on IoT devices. Security teams must be able to discover and identify all devices at the edges of the network.

Traditional network segmentation makes it tedious to secure network-based segments that can be simultaneously accessible

to all authorized users, devices, and applications and completely inaccessible to all others. Policy-based segmentation enables a more dynamic — and granular — network segmentation strategy that can automatically adapt to ensure least privilege in a zero-trust network.

Ensuring Endpoint Visibility and Control

Fundamental to the security of a constantly changing network is understanding its makeup — you can't protect what you can't see. Modern network access control (NAC) solutions help organizations keep up with the ever-expanding attack surface associated with the proliferation of endpoints and devices on the network. NAC solutions provide visibility into the network environment for dynamic policy control and enforcement. Whether devices are connecting from inside or outside the network, NAC solutions can automatically respond to compromised devices or anomalous activity. With NAC solutions, organizations can:

- Discover, identify, profile, and scan all devices for vulnerabilities
- Establish and ensure dynamic network control
- Establish and enforce policies that limit network access to only what is needed for that device
- Perform automated response and network orchestration (discussed later in this chapter)

A traditional NAC solution relies on traffic scanning, allowing devices to connect to the network during identification. However, the traffic-scanning process can take up to half an hour, during which time the network may be breached by a compromised device or endpoint. A modern NAC solution can automatically discover and profile every device as it requests network access and scan the device for vulnerabilities. The NAC processes can be completed within a few seconds to minimize the risk of device compromise.


TIP

Today, many companies have their networks in a multivendor environment with point solutions, which leads to a complex and fragmented infrastructure with different interfaces, management systems, and compatibility issues, making it harder to manage all

the connected devices cohesively. A good NAC solution needs to support multivendor networks to ensure seamless interoperability, enabling unified security policies and streamlined management across diverse devices and systems and consistent operation across wired and wireless networks.

Providing Automated Response and Network Orchestration

To accelerate and expand the reach and scale of their attacks, cybercriminals leverage extensive automation. Although visibility into the network can help detect potential threats, the response to these threats can be fragmented and ineffective if performed manually. Without predefined automated processes, security teams are often operating at a disadvantage, increasing an organization's risk.

An effective NAC platform provides policy-based security automation and orchestration. After the discovery of every endpoint and network infrastructure device, and the implementation of dynamic network access control based on contextual device insights, a good NAC should continue to deliver the capability to contain a cyberbreach through automated threat response. A good NAC solution would excel in this aspect by continuously monitoring the network, analyzing endpoints, and ensuring they meet their profiles. This enables automatic responses to potential threats, such as isolating compromised devices or blocking unauthorized access attempts. A NAC solution's integration with firewalls and other components of the networking infrastructure can further enhance its remediation capabilities by allowing the enforcement of granular access policies and real-time threat mitigation. Additionally, a NAC solution should be able to support multivendor environments, making it versatile and capable of leveraging existing infrastructure to orchestrate network segmentation and automated remediation effectively.

A HEALTHCARE COMPANY UTILIZES FortiNAC AND FORTINET SECURITY FABRIC TO IMMUNIZE IoT MEDICAL DEVICES AGAINST ATTACK

CASE STUDY

Challenges

Franciscan Health's 29,000 employees rely on various medical devices, which increase the network's vulnerability to cyberattacks. "We have a significant attack surface," says Chuck Christian, VP of Technology and CTO. "We have about 96,000 endpoints, including clinical systems, IoT gear, and medical equipment. Blocking unauthorized access to our corporate network is crucial."

Solutions

The need for a NAC was clear, and FortiNAC was the solution. "We need to prevent devices from connecting if we do not explicitly want to allow them," Christian explains. His team evaluated NAC solutions and found FortiNAC to integrate well with existing equipment. Franciscan Health is currently rolling out FortiNAC across their systems. "We can deny access to unknown devices, shunt them to an Internet-only network, or display a splash screen," Christian says.

A third-party identity solution provider, Ordr, passes data to FortiNAC for additional device visibility, which FortiNAC leverages to set up medical device-specific access rules that can be passed on to FortiGate firewalls, enhancing microsegmentation and applying network access policies more granularly.

Business Impact

Every new device gets a network profile, ensuring access-policy changes apply to all relevant devices. Integration with FortiManager further ensures configurations follow devices, improving overall network security efficiency.

IN THIS CHAPTER

- Recognizing the limitations of virtual private networks
- Introducing ZTNA
- Improving remote access security and user experience with ZTNA

Chapter 5
Reimagining Remote Access with ZTNA

Although virtual private networks (VPNs) have become commonplace, many organizations are now looking for better solutions to securely connect their hybrid workforces. In this chapter, you learn how zero-trust network access (ZTNA) improves security, enables more granular control, and delivers a better user experience than traditional VPNs.

Risks of Laterally Moving Malware and Ransomware

Cyberattacks are by no means a new threat, but one of the rising concerns for network security professionals is attempts at lateral movement after an infection. Lateral movement refers to a group of methods cybercriminals use to explore an infected network to find vulnerabilities, escalate access privileges, and reach their ultimate target. It's called lateral movement because of the way the hacker moves sideways from device to application and so forth. Although VPNs provide secure connectivity, they're architecturally limited to prevent lateral movement. The risks associated with lateral movement of malware become even more critical

in the context of a hybrid workforce, where work-from-anywhere (WFA) employees seamlessly switch between working remotely and on-site.

Building a Secure Remote Connection

ZTNA offers a better remote access solution than traditional VPNs and also addresses application access issues. ZTNA starts with the premise that location doesn't confer trust: Where a user or device is physically located is irrelevant. Any user is capable of malicious behavior and any device can be compromised. ZTNA is based on this reality.

REMEMBER

ZTNA grants access to individual applications and workflows on a per-session basis only after a user and/or device has been authenticated. Users are verified and authenticated to ensure they're allowed to access an application before they're granted access. Every device is also checked each time an application is accessed to ensure the device meets the application access policy. Authorization uses a variety of contextual information, including user role, device type, device security posture, location, time, and how a device or user is connecting to the network or resource.

With ZTNA, once a user and device are properly authenticated — for example, using a combination of multifactor authentication (MFA) and endpoint validation — they can securely connect to an application for a single session. With ZTNA, the user only gets access to that application, thereby restricting their capability to traverse the network. To get to another application, the user will need to go through another set of ZTNA verification checks.

ZTNA operates in terms of identity rather than securing a place in the network, which allows policies to follow applications and other transactions end to end. By establishing greater levels of access control, ZTNA is a more efficient solution for end-users and provides policy enforcement wherever it's needed.

TIP

Although the ZTNA authentication process provides points of authentication, unlike a traditional VPN, it doesn't specify how that authentication takes place. As new or different authentication solutions are implemented, they can be seamlessly added to the ZTNA strategy.

Today, there are two primary approaches to implementing ZTNA:

- **Client-initiated ZTNA:** Sometimes called endpoint-initiated ZTNA, the client-initiated ZTNA model was initially known as a software-defined perimeter and is based on the Cloud Security Alliance (CSA) architecture. This approach uses an agent that is installed on a device to create a secure tunnel. When a user wants to access an application, the agent gathers information like the user's identity, device location, network, and the application being used, and it builds a risk profile to assess the overall security posture. It then connects back to an application gateway or enforcement point, and if the risk profile meets the organization's policy requirements, the user and device are granted access to the application for the session. Applications can be hosted on premises or in the cloud. Using the client-initiated model can be challenging because managing the agents on devices can become a headache for IT, unless it's a unified agent covering many capabililities with a central management console that can coordinate deployment and configuration.
- **Service-initiated ZTNA:** The service-initiated ZTNA model uses a reverse-proxy architecture, which is also sometimes referred to as application-initiated ZTNA. Based on the BeyondCorp model, the biggest difference from client-initiated ZTNA is that it doesn't require an endpoint agent. It uses a browser plug-in to create a secure tunnel and perform the device assessment and posture check. A key disadvantage is that it's limited to cloud-based applications. Because the application's protocols must be based on Hypertext Transfer Protocol (HTTP)/Hypertext Transfer Protocol Secure (HTTPS), it limits the approach to web applications and protocols, such as Secure Shell (SSH) or Remote Desktop Protocol (RDP) over HTTP. Although a few newer vendors are offering additional protocol support, the model isn't suited to companies that have a hybrid combination of cloud and on-premises applications.

WARNING

Organizations should be careful to select ZTNA solutions that provide protections for all locations where their employees will work. Some ZTNA solutions were developed during the pandemic and work well for remote users but not for office users. Select a universal ZTNA solution that can provide all the checks and verifications for all locations. ZTNA shouldn't be a remote-only

solution, and it shouldn't introduce latency and create poor user experiences. Done right, ZTNA provides quicker access to an application with less security friction, thereby creating a better user experience.

Seeing the Advantages of Universal ZTNA

Adopting a zero-trust approach to security is a process that touches many systems and may take years for some organizations to fully implement. But addressing remote access is a good first step toward implementing the zero-trust security model. ZTNA solutions offer many advantages over traditional VPNs, including:

- **Organizations can extend the zero-trust model beyond the network.** Unlike a VPN, which operates at the network layer, ZTNA focuses on the transport layer, effectively providing application security independent of the network.
- **ZTNA works transparently in the background, which improves the user experience.** For users, ZTNA is easier to manage than a VPN. Users no longer have to remember when to use the VPN or go through the process of connecting. There's also no risk of tunnels accidentally being left open because someone forgot to disconnect the VPN client. With ZTNA, a user simply launches the application and immediately gets a secure connection whether the application is on premises or in a cloud. This encrypted tunnel is created on demand and in the background — so that the user doesn't even know it's happening. Because the corporate network is no longer an implicit zone of trust, the same tunnel is created whether the user is on the network or off the network.
- **Users and devices are verified and validated before access to an application or resource is granted.** This process includes a security posture check that verifies that the endpoint is running the right firmware and endpoint protection software to verify it's safe to connect to the application. The verification is granular, per session, using the same access policy whether a user is accessing resources that are on premises or in the cloud. Verifications are also continuous, even after a session has been established. The

same policy also controls who can access that app based on the profile of the authenticating user and device.

- **Because ZTNA focuses on application access, it doesn't matter what network the user is on.** Universal ZTNA automatically creates secure connections to applications, no matter where the user is located. For every application session, ZTNA verifies the security posture of both the user and device — even when users are in the office.
- **ZTNA reduces the attack surface by hiding business-critical applications from the internet.** On the application side, because the user is connecting back to the enforcement point and then proxying that connection to the application, the application can exist on premises or in a cloud, hidden from the internet. The application only needs to establish a connection with the enforcement points, keeping them safe from cybercriminals.

REMEMBER

More organizations are recognizing the need to transition away from traditional VPNs. ZTNA is proving to be a better solution that is easier to use and provides better application security.

HOW ZTNA IS TAKING FLIGHT AT A PRECISION-EQUIPMENT MANUFACTURER

CASE STUDY

Overview

Founded in 1857 to build springs for bicycle manufacturers, Barnes Group has grown rapidly through acquisitions. It now consists of 17 different companies, employing around 6,500 people with over 100 locations across North America, Europe, the Middle East, Africa, and the Asia Pacific region.

Challenge

Throughout this widely dispersed corporate infrastructure, the company's IT and security teams are focused on minimizing the company's cyberattack surface. That is a significant challenge since Barnes manages about 8,500 endpoints globally across over 100

(continued)

(continued)

locations and must meet the demands of many different compliance regimes, including GDPR and other countries' data privacy rules.

In addition, Barnes surveyed employees in advance of the cloud transition and learned that the lack of security standardization was creating serious challenges for the company's end-users. Barnes determined that it needed to give every user the same experience. It wanted to have single sign-on, and for the login experience to be the same, regardless of where a person is in the world.

Choosing a ZTNA Solution

Barnes has been on a path toward zero-trust security to better manage the expanding attack surface. It decided that a ZTNA approach would offer more effective security across the company's locations around the world and in the cloud. It also saw ZTNA as a means of improving both the end-user experience and the efficiency of security administration. Barnes considered several technology options, ultimately deciding to extend its Fortinet infrastructure by deploying Fortinet Universal ZTNA.

"If we were deploying ZTNA from a different vendor, the complexity would be off the charts. We required a solution where we could deploy a uniform global policy in a streamlined way, and Fortinet provides that. The Fortinet environment gave us the best bang for our buck," said their Global Cloud Infrastructure Manager.

Business Outcomes

By working with Fortinet Professional Services, the Barnes Group is implementing ZTNA more confidently and cost effectively than it could otherwise. Fortinet Universal ZTNA, integrated with robust endpoint and network protection, provides consistent and easy-to-manage security policy enforcement. At the same time, the solution streamlines audits, reduces Barnes's IT hardware and administrative costs, and is expected to shorten new business IT integration time by more than 50 percent.

IN THIS CHAPTER

- Adapting networking and security to hybrid work challenges
- Defining secure access service edge (SASE)
- Recognizing the benefits of a single vendor solution
- Introducing Fortinet Unified SASE

Chapter 6
Exploring Secure Access Service Edge (SASE)

In this chapter, you learn about modern networking and security challenges associated with hybrid work models, how a secure access service edge (SASE) can help your organization deliver a consistent networking and security experience for your users everywhere, why you need a unified SASE solution to optimize your networking and security operations, and how Fortinet Unified SASE extends the unified SASE approach to enable different use cases.

Recognizing Hybrid Work Challenges

The modern hybrid workforce has introduced new networking and security challenges that organizations must address to ensure a robust security posture and a performant network infrastructure that meets the dynamic needs of the enterprise and its users.

Often, network and security teams address different business needs with "one-off" point solutions, such as a standalone router

to provide Internet connectivity at a branch location and a small firewall appliance to provide secure connectivity to the Internet, the public cloud, and the corporate data center.

Unfortunately, these approaches often create gaps in the organization's security posture and introduce other challenges, such as:

- **Inconsistent security policies and controls:** Lack of a centralized management console for siloed security tools often leads to inconsistent — and potentially insufficient — enforcement of security policies and application of security controls. Applying and enforcing consistent policies, whether a user is on-network or off-network, is challenging. This negatively impacts user experience and productivity.
- **Inefficient use of network resources:** Multiple direct Internet access (DIA) links are often provisioned for branch locations to ensure connectivity if a link fails. Depending on the networking equipment used, these configurations may not support load balancing, traffic prioritization (that is, quality of service or QoS), automated failover/failback, and other advanced networking capabilities.

  Having different firewalls and other security tooling on the various DIA links also creates many security challenges.
- **Lack of onsite expertise:** Branch locations don't always have local IT resources to troubleshoot networking and security issues when they inevitably arise. Practically every organization today must work with limited budget resources and workforce shortages, especially within the security profession. Remote access options may be limited for many point solutions, requiring IT staff to get creative with third-party remote access tools which may introduce new risks to the enterprise IT environment.
- **Increased complexity:** Managing disparate solutions from different vendors is challenging. It requires limited IT and security staff to learn specialized skills and new interfaces to operate each of the various tools. Complexity leads to a greater risk of security misconfigurations and requires more time to troubleshoot when issues arise.

Addressing Hybrid Work Challenges with SASE

To ensure consistent connectivity and security for hybrid users everywhere, networking and security solutions must converge at the edges and in the cloud. SASE consolidates networking and security capabilities and functions in a single, cloud-delivered solution that includes the following:

- **Secure software-defined wide-area networking (SD-WAN):** SD-WAN enables organizations to use their networks more effectively and economically — empowering users to better engage customers, optimize business processes, and innovate.
- **Secure web gateway (SWG):** SWG provides a secure web experience to protect users, devices, and applications from both internal and external threats. Using one solution rather than several disparate point products offers a number of benefits, including simplified management and reduced costs, while maintaining a strong security posture. SWG capabilities provide an end-to-end secure web experience with uniform resource locator (URL) filtering, data loss prevention (DLP), and advanced malware protection.
- **Firewall-as-a-service (FWaaS):** FWaaS is a firewall solution delivered as a cloud-based service that allows companies to simplify IT infrastructure. It provides next-generation firewall (NGFW) capabilities like web filtering, advanced threat protection (ATP), intrusion prevention system (IPS), and DNS security.
- **Zero trust network access (ZTNA):** ZTNA provides granular secure access to applications based on per-session validation of user and device identity, continuous device posture validation, and granular application access control policy. ZTNA provides simplified user experience with single sign-on (SSO) to applications and improves security posture compared to a virtual private network (VPN). Universal ZTNA extends ZTNA beyond remote access to consistent, secure application access for users from any location (branch, campus, remote) to any application (on-premises data center, public cloud, software-as-a-service [SaaS]).

- **Digital experience monitoring (DEM):** DEM facilitates troubleshooting by providing insight into what users are actually doing and the real problems they're encountering. It observes the health and performance of all devices across any network. DEM provides end-to-end visibility from endpoint to application access, monitoring the status and health of end-user devices. This high degree of visibility helps IT teams pinpoint where issues arise.
- **Cloud access security broker (CASB):** A CASB is software (or hardware) that sits between users and their cloud services to enforce security policies as they access cloud-based resources (SaaS). CASB differs from firewalls that organizations use to monitor and filter their network. CASBs can identify strange or unusual user activity and provide organizations with cloud access control. Unlike firewalls, CASBs provide deep visibility into cloud environments and offer granular control of cloud usage.
- **SaaS security posture management (SSPM):** SSPM is a category of automated security tool used for tracking security threats in SaaS applications. Misconfigurations, unused user accounts, excessive user rights, compliance hazards, and other cloud security problems can all be detected by SSPM. SSPM solutions execute routine and critical security configuration processes in an intelligent and efficient manner — using technologies like artificial intelligence (AI) and machine learning.

Defining Unified SASE and Its Benefits

Achieving consistent connectivity and security can be difficult when trying to integrate solutions from different vendors. Instead, a platform-centric, unified SASE solution enables the consolidation of technologies and converges networking and security functions to drive operational efficiency. Management, optimization, and policy enforcement are all controlled through a single interface.

Ideally, a unified SASE solution should interoperate across distributed networks, seamlessly handing off connections between the cloud and on-premises devices. This allows access and security

policies to follow users and applications end to end, rather than terminating connectivity and control at either edge of the network. Other key capabilities and benefits of a unified SASE solution include the following:

- **Unified agent for all SASE features:** Onboarding different agents for every use case can quickly become too complex and expensive to maintain. A SASE solution should offer a single agent that supports multiple use cases, including ZTNA, CASB, DEM, and endpoint protection, while automatically redirecting traffic to protect assets and applications through cloud-delivered security.
- **Secure Internet access:** With remote work becoming the new normal, users with DIA greatly expand the enterprise attack surface. An effective solution must be able to follow, enable, and protect users no matter where they (or their applications) are located.
- **Flexible, secure private access:** A unified SASE solution should provide secure connectivity to business applications, whether deployed in a private data center or the public cloud, through a zero-trust architecture and/or SD-WAN intelligent routing and steering.

  Integrated ZTNA provides explicit per-application access to authenticated users without requiring a persistent tunnel. ZTNA's capability to grant access based on identity and context, combined with continuous validation, ensures effective control over who and what is on the network.
- **Secure SaaS access:** An effective SASE solution must enable secure access to SaaS applications, regardless of where devices and users are located — a function vital to a hybrid workforce that regularly moves between campus, branch, home office, and mobile environments.
- **Visibility and control with DEM and analytics:** A good solution offers a deep look into your users' digital experiences. This should be available no matter where the user resides or where an application is hosted. This allows your IT team to quickly troubleshoot issues.
- **Flexible consumption with simplified onboarding:** The right SASE solution can help organizations shift their

business consumption to an operating expenditure (OpEx) model. To do this effectively, it should offer simple tiered licensing that enables organizations to predict a cost-to-business growth correlation and use of security.

- **Simple cloud-based management:** A cloud-based SASE management system should provide comprehensive visibility, reporting, logging, and analytics. This helps ensure efficient security operations while reducing meantime to detection (MTTD) and remediation (MTTR).


REMEMBER

Organizations need unified SASE that seamlessly integrates into their existing networking and security architectures to ensure secure and reliable connectivity and deliver superior user experience wherever needed.

Evolving to Unified SASE to Secure Everything

Fortinet Unified SASE combines SD-WAN and security service edge (SSE) from a single vendor under unified management. Unified SASE expands the single-vendor SASE solution to local area network (LAN)/wireless LAN (WLAN), SD-WAN private access, digital experience monitoring, and Internet of Things (IoT)/operational technology (OT) device access control, to make Unified SASE the most comprehensive solution for hybrid environments with a flexible licensing model.


TIP

Key elements of Unified SASE include the following:

- **Unified management and DEM:** Unified SASE provides visibility across on-premises and remote users, securing the modern hybrid workforce. Unified SASE includes DEM functionality, which provides unified visibility into users' experiences as they interact with applications and devices, enabling organizations to obtain a comprehensive view of the user experience.
- **Seamless secure SD-WAN on-premises integration:** Secure SD-WAN is integrated with FortiSASE to offer an integrated, simpler, more automated, and more easily

consumable service. FortiSASE Secure Private Access (SPA) enables broad, seamless access to applications at private data centers or in public clouds by automatically finding the shortest path to each application and enabling superior user experiences everywhere.

- **Expanded edge integration with wireless, OT/IoT, access points, and switching:** FortiAP secure access points, FortiBranch SASE devices, FortiExtender WLAN, and FortiSwitch next-generation switches all integrate with Unified SASE.
- **Unified agent and universal ZTNA:** FortiClient is a single agent used for fabric integration, secure access, and endpoint protection. The unified agent provides endpoint visibility through telemetry and ensures that all security fabric components have a unified view of endpoints to provide tracking and awareness, compliance enforcement, and reporting. Automatic ZTNA tunnels provide secure remote connectivity.
- **Usage-based consumption with FortiFlex:** FortiFlex provides usage-based licensing that gives organizations the flexibility to right-size their services and spend in securing their cloud and hybrid environments. FortiFlex simplifies deployment decisions with the freedom to dynamically deploy, scale in/out, and scale up/down without needing to size for exact services and solutions ahead of time.

Unified SASE enables many business benefits including:

- **Secure the modern hybrid workforce.** A hybrid workforce is the new reality for many businesses today. At the same time, the number of applications and services that organizations have migrated to the cloud to gain greater efficiency, cost-savings, and elasticity has grown significantly. Protecting today's rapidly evolving hybrid work environments calls for robust, purpose-built security — such as Unified SASE.
- **Converge networking and security.** Modern networks are nothing like the networks most security solutions were originally designed to protect. Many security and IT teams have become accustomed to overlaying point security solutions onto their hybrid networks. Yet doing so has led to increased management complexity, performance bottlenecks, poor user

experience, and the potential introduction of new exploitable gaps or vulnerabilities. Unified SASE converges security and networking, allowing organizations to adapt to today's rapid pace of new priorities and evolving business needs.

- **Consolidate vendors and reduce operational complexity.** Working with different vendor products and services is complex and costly. Different vendors have different licensing models, maintenance contracts, support fees, and more. IT and security teams must also learn different operating systems, admin interfaces, and command syntaxes across these siloed point solutions. Finally, correlating events across different security tools requires deep integration and automation that may not be possible with siloed tools. Unified SASE helps IT and security teams drive operational efficiency, reduce costs, and eliminate needless complexity.
- **Enforce consistent security and deliver a superior user experience.** Unified SASE easily integrates into an organization's larger network and security architecture, enabling seamless interoperability. Consistent network operations and security controls enable a superior user experience for workers — no matter where they are working from or what device they're using.

IN THIS CHAPTER

- Assessing the business process criticality of your assets
- Understanding what applications are used
- Applying role-based access controls
- Verifying on a continuous basis

Chapter 7
Ten Steps on the Journey to Zero Trust

Implementing a zero-trust strategy for your organization is a journey. This chapter offers ten key steps to help you on your journey to zero-trust access (ZTA).

Assess Your Assets

You can't protect every asset on your network at the same level. It's important to prioritize your efforts by first determining which assets are most critical to your business processes. Once you've determined where to start, you can begin implementing your ZTA strategy to protect your most critical assets first.


TIP

The criticality of your business processes (and the systems and applications they depend on) will drive other important decisions such as additional security policy controls and recovery point objectives (RPOs) for business continuity and disaster recovery.

Identify the Users/Entities

Identifying every user and entity on your network is critical to establishing a ZTA strategy. Once identity is established, access policies are determined by a user's role in the organization. A least-privilege access policy is used to grant access to only the resources necessary to perform a specific role or job. Access to additional resources is provided on an as-needed basis.

Identify the Devices on Your Network

The next step in adopting a zero-trust strategy is to discover and identify all the devices on your network — whether that's an end-user's laptop, a server, a network printer, or an Internet of Things (IoT) device. The proliferation of applications and devices is expanding the network perimeter, creating billions of edges that must be managed and protected. Network access control (NAC) tools deliver visibility into the devices on your network.

Identify the Applications Used by Your Organization

Applications are at the heart of business operations and processes. Today, these applications include not only those that are installed on endpoints or servers in your data center but also software-as-a-service (SaaS) offerings and application workloads hosted in the cloud.

Create Zones of Control

Network segmentation has been used to limit traffic in certain areas of the network and to provide additional security controls within the network. Segmentation firewalls establish visibility and control within the network and provide the ability to scan, protect, and block traffic.

REMEMBER

End-to-end visibility, granular segmentation, and strategically deployed control points (firewalls) are key to a successful zero-trust strategy.

Apply Role-Based Access Controls to Your Assets

Role-based access controls (RBAC) are used to efficiently manage the permissions that groups of users are granted to a specific asset, based on their job or role within the organization.

WARNING

Organizations focus on ensuring group memberships are properly maintained and accurate. Although this is an important aspect of RBAC, it's just one side of the coin. Equally important is ensuring that the permissions assigned to a role aren't excessive. The scope should be limited to the specific resource that is required by the role and only the permissions necessary to perform a function within that role should be granted (that is, least-privilege access).

Control Where Devices on Your Network Can Communicate

A zero-trust security approach uses microsegmentation to create granular trust zones around individual resources, which helps to enforce least-privilege access. Users and entities are only granted access to the resources that are needed to perform a specific role or job. Microsegmentation prevents users (and attackers) from roaming freely on the network.

TECHNICAL STUFF

Microsegmentation adds a dynamic, policy-based element to traffic segmentation, enabling much more granular control than regular network segmentation.

Extend Control of Devices

Enhanced workplace mobility and an increased emphasis on remote work — including work from anywhere (WFA) — has led to increased interest in endpoint security, including endpoint visibility, control, scanning, patching, and web filtering off the network. At the same time, the number of applications and services now running in public clouds has grown significantly, making traditional network architectures that backhaul Internet

traffic through a centralized perimeter-based firewall extremely inefficient. Universal zero trust network access (ZTNA) provides secure access to applications from any location based on continuous endpoint posture validation in addition to user/device identity and granular application access control.

A cloud-delivered secure access service edge (SASE) platform converges networking and security capabilities in a single solution that enables organizations to extend security and compliance controls to devices and employees, regardless of where they are working.

REMEMBER

SASE combines networking and security capabilities and functions in a unified solution that includes software-defined wide-area networking (SD-WAN), secure web gateway (SWG), firewall-as-a-service (FWaaS), ZTNA, cloud access security broker (CASB), and more. SASE's goal is to support the dynamic, secure access needs of today's organizations. SASE plays a critical role in ensuring that security can be delivered anywhere, including at the WAN edge, cloud edge, data center edge, core edge, and endpoint devices used by today's hybrid workforce.

Apply Application Access Control

An effective ZTA strategy addresses both network connection and application access based on the assumption that no user or device is inherently trustworthy. No trust is granted for any transaction without first verifying that the user and the device are authorized to have access.

Continuously Verify and Authenticate Users and Devices

ZTA requires continuous authentication, verification, and monitoring of users and devices that are connected to the network. Logging into the network doesn't grant a user or device unrestricted access to the resources on your network. Further authentication may be required to access certain sensitive resources in restricted zones and the duration of user sessions should also be limited. This ensures that sessions can't be hijacked and that appropriate controls can be enforced if, for example, the device state changes during the session and its risk posture becomes unacceptable.

Get started with a zero trust access strategy today

Every time a device or user connects to your network and is automatically trusted, your organization's applications and data are at risk. The traditional perimeter-based approach to security in which everything inside the network is trusted and everything else is not trusted is no longer effective. In a world of work from anywhere organizations need to shift to a zero-trust access strategy, based on the principle of "never trust, always verify," to ensure they know every device and user that accesses the network and how to protect their assets on and off the network.

Inside...

- Know and control who connects to your network and applications
- Know and control what devices connect to your network and applications
- Enforce risk-based explicit access with continuous validation
- Use Zero Trust principles to secure all endpoints, edges, networks, and cloud applications

FORTINET

Lawrence Miller has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 200 *For Dummies* books on numerous technology and security topics.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-394-39073-1
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.