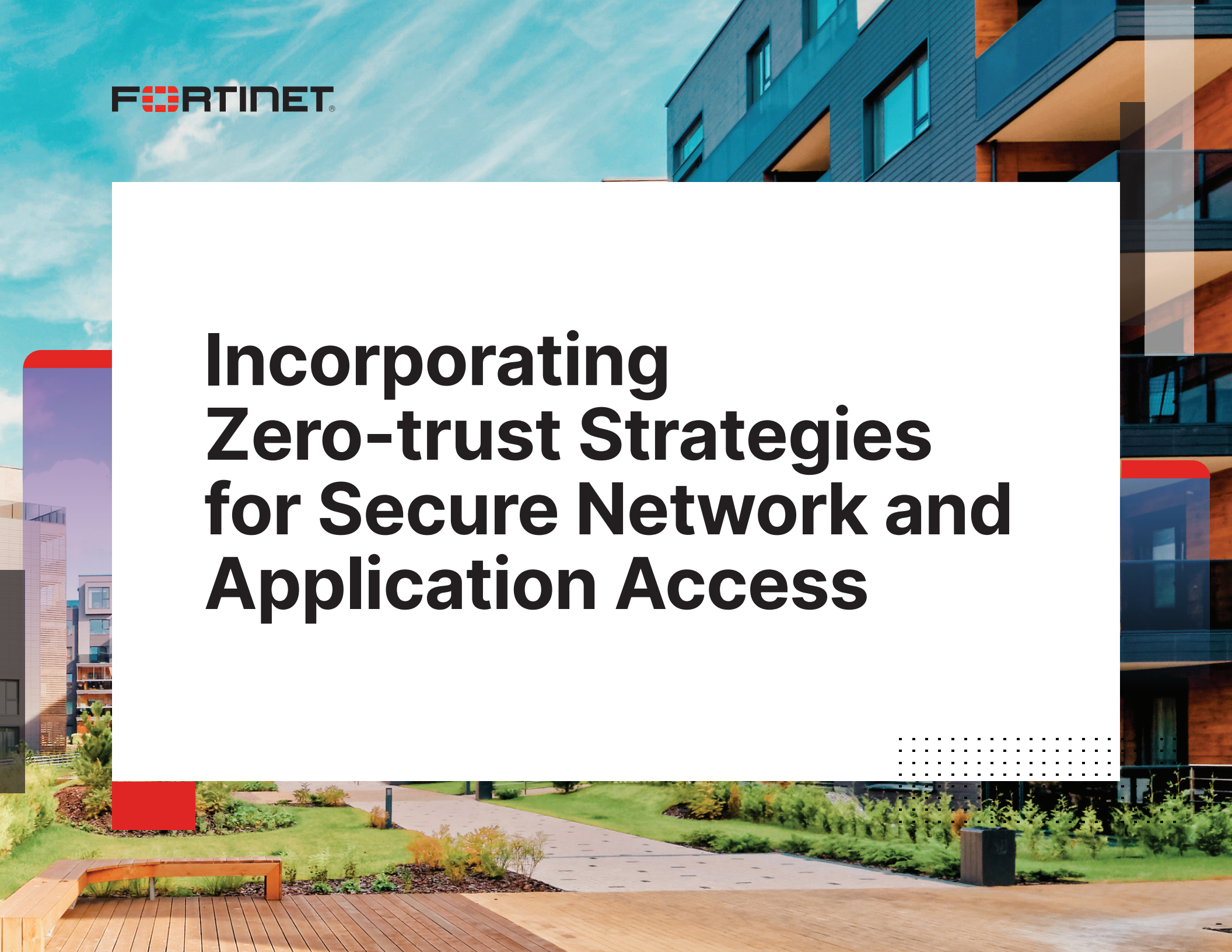

Incorporating Zero-trust Strategies for Secure Network and Application Access

Executive Summary

As businesses continue to embrace digital innovation, cloud applications, and work-from-anywhere initiatives, networks become ever more complicated and dispersed with an increasing number of “edges.” And as the traditional network perimeter continues to dissolve and the more people and devices that connect to a network, the less secure a traditional perimeter-based approach to security becomes.

Every time a device or user is automatically trusted, it places an organization’s data, applications, and intellectual property at risk. CISOs need to shift the fundamental paradigm of an open network built around inherent trust to a zero-trust model. This zero-trust strategy needs to incorporate rigorous access controls that span the distributed network so devices, users, endpoint, cloud, Software-as-a-Service (SaaS), and the infrastructure are all protected.

Fortinet offers a tightly integrated collection of security solutions that help organizations identify and classify all users and devices that seek network and application access.

Introduction

As more companies shift their networks to accommodate remote workers, multi-cloud architectures, and digital innovation, their approaches to security need to change as well. Today, organizations need to establish secure and trustworthy access from any location to a wide variety of cloud-based services and enterprise resources.

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 when either is compromised, whether intentionally or unintentionally.

The increase in bring-your-own-device (BYOD) and Internet-of-Things (IoT) initiatives have led to a proliferation of access points and endpoint devices, so the traditional network perimeter has been eliminated. Attackers, malware, and infected devices that bypass edge security checkpoints often have free access to the network inside.

This zero-trust approach shifts the fundamental paradigm of open networks built around inherent trust to a security model where the assumption is that no user or device is trustworthy, and no trust is granted for any transaction without first verifying that the user and the device are authorized to have access. This strategy leverages adoption of rigorous network access controls to identify, authenticate, and monitor users and devices, both on and off the network.

Only 15% of organizations have completed a transition to a zero-trust security model, which does not automatically assume that anyone inside the network perimeter is trusted.[1]

The Keys to an Effective ZTA Strategy

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, security leaders should assume that every device on the network is potentially infected. Further, any user is capable of compromising critical resources, intentionally or inadvertently.

An effective zero-trust access (ZTA) strategy addresses both network connection and application access based on the underlying 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. Implementing the ZTA model requires focusing on three key elements.

1. Know every device that's on the network

Because of the expansion of the network perimeter from the increase in applications and devices, potentially billions of edges must now be managed and protected. Network access control (NAC) tools deliver visibility into the network environment.

2. Know every user that accesses the network

To establish an effective ZTA strategy, it's critical to determine who every user is and what role they play within an organization. The zero-trust model focuses on a "least access policy" that only grants a user access to the resources that are necessary for their role or job.

3. Know how to protect assets on and off the network

An effective ZTA strategy addresses the challenge of protecting off-network devices by improving endpoint visibility. Because of increased mobility and remote work, users can inadvertently expose their devices and company resources to threats. After being online elsewhere, once they rejoin the network these users can inadvertently expose company resources to viruses and malware they may have picked up.

The frequency of attacks against endpoints is increasing and detection is difficult. 68% of respondents say the frequency of attacks has increased over the past 12 months.[2]

Fortinet Zero Trust Solutions

To implement ZTA, 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. They can assess their state of compliance with internal security policies, automatically assign them to zones of control, and continuously monitor them, both on and off the network. Additionally, Fortinet also offers Zero Trust Network Access (ZTNA), which extends traditional ZTA network access to per-application usage, so systems administrators not only know who is on the network but even which applications they are currently using, with transactions and usage constantly being monitored and inspected.

1. Endpoint access control

Endpoints are often the target of an initial compromise or attacks. In fact, a recent study found that 30% of breaches involved malware that was installed on endpoints.[3] Fortinet strengthens endpoint security through integrated visibility, control, and proactive defense. The ability to discover, monitor, and assess endpoint risks helps to ensure endpoint compliance, mitigate risks, and reduce exposure. Fortinet FortiClient endpoint access solutions:

- Support secure, encrypted connections across unsafe networks with support for split tunneling and secure access service edge (SASE) services
- Provide continuous endpoint security telemetry data, including device operating system (OS) and applications, known vulnerabilities, patches, and security status
- Support ZTNA remote access, which simplifies secure connectivity, providing seamless access to applications no matter where the user or the application may be located

2. Identity and access management

Today's enterprise identity environments are made up of various systems of record 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. Additionally, many of today's most damaging security breaches have resulted from compromised user accounts and passwords that were then exacerbated by users being given inappropriate levels of access. Securely and effectively managing identity authentication and authorization for all systems and applications is crucial to minimize security breaches. Fortinet identity and access management (IAM) solutions are used to:

- Establish identity through login, multi-factor authentication (MFA), and certificates, which may evolve to add continuous contextual authentication
- Provide role-based information from an authentication source for use in privileged access
- Establish and enforce role-based least access policies
- Provide added security with support for single sign-on (SSO) to help improve user compliance and adoption
- Verify ZTNA connections for devices and users on a per-session basis to individual applications

3. Network access control

Network access control is a zero-trust network access solution that helps organizations keep up with today's ever-expanding attack surface. It delivers visibility into the network environment for enforcement and dynamic policy control. Whether devices are connecting from inside or outside the network, FortiNAC can automatically respond to compromised devices or anomalous activity. With FortiNAC, organizations can:

- Identify, profile, and scan all devices for vulnerabilities
- Establish and ensure ongoing network control
- Establish and enforce policies that limit network access to only what is needed for that device
- Maintain automated response and network orchestration

4. Application access control

In the zero-trust model, application access should be controlled on a per-session basis, and each user and device should be verified whether they are connecting remotely or from an owned network. Application access should be mapped to the individual's role so that only those applications that are relevant to the user are available. Applications can reside in on-premises servers, private clouds, or public clouds and still be controlled using zero-trust mechanisms. ZTA focuses on role-based access control to the network, and ZTNA relates to brokered access for users to applications. With Fortinet ZTA solutions, application access control can be used in a variety of deployment scenarios, including with SASE services or with on-premises appliance or virtual machine (VM) firewalls. These solutions:

- Verify users and devices for each application session
- Control user access to applications based on policy
- Enforce application access policy no matter where the user is located
- Create a secure, automatic connection between the user and ZTNA proxy point
- Work with firewalls, VM firewalls, and SASE services

For many organizations, the attacks highlighted the need for better approaches—including zero-trust models—for protecting their networks against threats posed by workers connecting from weakly protected home networks.[4]

Key Benefits of the Fortinet ZTA Framework

For effective security, organizations have to shift from protecting security perimeters to protecting data spread across the billions of edges, users, systems, devices, and critical applications. The Fortinet platform provides comprehensive visibility and protection across devices, users, endpoint, cloud, SaaS, and infrastructure. Fortinet Zero Trust solutions offer these key benefits:

- Complete and continuous control over who is accessing applications, no matter where those applications reside or where the users are
- Complete and continuous control over who is on the network
- Complete and continuous control over what is on the network
- Integrated ZTA and ZTNA solutions that leverage the Fortinet Security Fabric, which works equally both on-premises and in the cloud over a local-area network, a wide-area network, and remote tunnels
- A complete, integrated solution from a single vendor

Summary

With decades of experience in helping enterprises maintain security coverage for their rapidly expanding networks, Fortinet offers highly effective Zero Trust solutions that deliver visibility and control in four key areas: application access, users on the network, devices on the network, and the offline activities of those users and devices.

[1] "2019 Zero Trust Adoption Report," Cybersecurity Insiders, November 2019.

[2] Larry Ponemon. "The state of endpoint security risk: it's skyrocketing," Ponemon Sullivan Privacy Report, May 2020.

[3] "2020 Data Breach Investigations Report," Verizon, May 2020.

[4] "Global Threat Landscape Report," FortiGuard Labs, August 2020.

FORTINET

www.fortinet.com

July 21, 2021 8:33 AM

885304-B-0-EN