EBook

Want to Secure Your Hybrid Workforce with ZTNA?

Look for these 10 Must-Have Capabilities

Contents

Introduction 3

What is Zero Trust Network Access (ZTNA)? 4

#1: Eliminate the attack surface by making apps invisible to the public internet 5

#2: Enable seamless connectivity from anywhere 6

#3: Enforce least-privileged access 7

#4: Keep users productive by rapidly detecting and resolving app, network, and device issues 8

#5: Prevent lateral movement through application microsegmentation 9

#6: Support secure access for BYOD as well as corporate-owned devices 10

#7: Stop attacks and block threats with complete inline content inspection 11

#8: Seamlessly integrate with a broad array of identity providers and solutions 12

#9: Incorporate integrated deception technology to foil attackers 13

#10: Allow for fast and easy deployment 14

See for yourself why Zscaler Private Access is the world's most-deployed ZTNA platform 15

Introduction

The world of work is changing. How and where employees are most productive is different than it was even a few short years ago. As growing numbers of organizations are embracing hybrid and remote work, they're moving growing numbers of mission-critical applications to the cloud so that they can take full advantage of the flexibility, scalability, and efficiencies it offers.

However, as IT ecosystems transform, new security challenges are being created. Large-scale adoption of hybrid and remote work—along with greater use of the cloud and increased mobile access—can expand the attack surface, especially if these changes aren't accompanied by a move away from legacy security solutions (like VPNs and firewalls) and outdated approaches. In addition to attack surface sprawl, this situation limits security teams' visibility, making it more difficult to investigate incidents and troubleshoot issues.

What's needed is a new model for securing technology environments—one that's better suited to meet today's security and connectivity needs. Zero trust provides exactly this, and it's currently seeing rapid adoption across industries and geographies.

Growing numbers of organizations are choosing Zero Trust Network Access (ZTNA) to strengthen their security posture for hybrid work. ZTNA provides a clear, well-defined framework to follow on the path to zero trust. Analyst firm Gartner reports that the market for ZTNA is expanding at breakneck speed. It's currently seeing more than 60% year-over-year growth.

Organizations cite VPN replacement as their primary motivation for implementing ZTNA.

What is Zero Trust Network Access (ZTNA)?

ZTNA is a set of technologies and functionalities that enable secure access to internal and/or private apps for remote users.

ZTNA operates according to an adaptive trust model, where trust is never implicit, and where access is granted only on a need-to-know, least-privileged basis that's defined by granular policies.

As growing numbers of organizations adopt cloud-delivered apps and infrastructures, many are looking to unify their security services with a single, cloud-delivered platform. This is known as the Security Service Edge (SSE)—comprising secure web gateway (SWG), cloud access security broker (CASB), and ZTNA capabilities. Gartner recommends that security and risk management leaders begin their SSE adoption strategies by adopting ZTNA. In this sense, ZTNA is often a key first step on the road to cloud-delivered security.

Many organizations are turning to ZTNA to replace VPN infrastructures that don't perform well at scale or expose the organization to increased security risk because their presence expands the attack surface. But ZTNA is much more than a VPN replacement—it offers organizations the opportunity to eliminate legacy appliances (along with their management overhead), gives users fast and direct access to apps, scales effortlessly, and enhances administrative control and visibility.

Not every ZTNA product or solution on the market is created equal, though. To achieve all of these benefits and more, look for one that can do all of the following 10 things.

#1: Eliminate the attack surface by making apps invisible to the public internet.

In traditional hub-and-spoke style network architectures, applications can easily be found by any attacker who is able to breach the security perimeter.

Once bad actors are inside the network, applications and other resources are easily discoverable through a simple search.

With a true ZTNA solution, application access is granted on a one-to-one basis through segmentation. This makes it impossible to discover other applications in your environment, even if an attacker gains access to one.

All applications are hidden behind the ZTNA platform, which brokers direct connectivity. Because attackers cannot target what they can't see, a ZTNA solution should hide source identities by obfuscating their IP addresses. In essence, these inside-out connections render your entire application ecosystem invisible. This way, attackers cannot launch targeted attacks against individual apps.

#2: Enable seamless connectivity from anywhere.

77% of today's organizations have adopted or are looking to enable hybrid work.

Legacy network architectures rely on expensive MPLS links between branches and the central data center and connect remote users via VPNs. As hybrid and remote work becomes mainstream, VPN usage creates performance challenges because VPNs cannot scale.

By contrast, ZTNA completely isolates application access from network access, eliminating the need for MPLS links and VPNs. Look for ZTNA that's offered as a cloud-delivered service, since this removes the need to backhaul traffic to the corporate data center. Instead, users get fast, direct access to the applications they need to stay productive.

Keep in mind that a ZTNA provider with an expanded global presence—when it comes to data centers—will be able to find the shortest connectivity path between users and applications. Brokering connections as close to the edge as possible ensures that employees will enjoy top-notch user experiences.

#3: Enforce least-privileged access.

Least-privileged access is a key principle within the zero trust philosophy. Its definition is simple: users are granted only the minimum level of access necessary to perform their job duties, and nothing more.

Building a security architecture that can support this approach can be challenging without the right ZTNA solution. The solution must incorporate robust user identity authentication mechanisms, understand device context, and have the ability to enforce very granular user-to-app segmentation in its controls. To achieve this, ZTNA should offer deep integrations with all major identity provider (IdP) platforms.

Seek out a ZTNA solution that can enforce IT and business policies by connecting verified users only to the applications they're authorized to use, not the network. This access should be extended equally to remote and on-premises users, regardless of location, and security controls should be identical for all users, everywhere.

Zscaler enabled secure remote work for 18,000 employees of the City of Los Angeles.

#4. Keep users productive by rapidly detecting and resolving app, network, and device issues.

Careem improved Mean Time-to-Response (MTTR) by 62% with Zscaler Digital Experience Monitoring.

Adopting zero trust—especially if teams are attempting to implement it using legacy VPNs—requires granular network segmentation.

From an engineering perspective, this is no easy task. When it comes to user experience, though, there are additional obstacles. When networks are segmented in this way, it is difficult, if not impossible, for network and service desk teams to get the insights into end user device and application performance that they need to ensure great end user experiences.

A ZTNA solution should provide key capabilities that help teams overcome this challenge. It should gather metrics on end user device health, network performance, and application availability, and should present them within an easy-to-monitor, pane-of-glass dashboard that makes it possible for user support teams to identify and fix issues before end users notice the problem.

#5: Prevent lateral movement through application microsegmentation.

A ZTNA solution should protect your data, workflows, services, and resources through software-defined microsegmentation. This means that users should be connected directly to apps, not to the network.

If this approach is followed, security teams no longer need to worry about lateral movement across the network. Should a single user account or application ever be breached, there's no way the attacker can move beyond this to compromise other enterprise resources.

With ZTNA, establishing a connection to a single app or resource should never mean that you're automatically granted access to others.

#6. Support secure access for BYOD as well as corporate–owned devices.

Look for a ZTNA solution that can support both agent and agentless access for employees as well as third parties.

Look for a ZTNA solution that can support both agent and agentless access for employees as well as third parties. This way, ZTNA can allow for partners and vendors to seamlessly access your resources, while making it possible for employees to use their own devices (including mobile devices) for work purposes, and to do so securely.

As unmanaged devices become more and more prevalent, it's also important that your ZTNA solution can support clientless access. Otherwise, you'll only be able to protect your own employees on corporate–issued devices. In the modern, mobile–centric world, this is a significant limitation.

#7: Stop attacks and block threats with complete inline content inspection.

For the complete visibility that's needed to block all threats, a ZTNA solution should be able to perform complete inline content inspection.

This means the service will be able to inspect all traffic (including SSL-encrypted traffic, which is used to mask the transmission of dangerous content such as ransomware, spyware, and viruses) and only permit known-legitimate communications to pass through. This inline inspection should be informed by threat intelligence cultivated from a broad array of global signals to ensure it can stop currently-prevalent ransomware, phishing, and zero-day threats, as well as advanced attacks.

Want to know which threats ZTNA should be able to protect against? The OWASP Top 10 represents a broad expert consensus about the most critical security risks for web applications. A ZTNA solution should provide comprehensive coverage of the most commonly-employed attack techniques – including SQL injection, cross-site scripting, environment and port scanners, and cookie poisoning.

Zscaler makes it possible to block the OWASP Top 10 and other known web application security risks, including SQL injection and cross-site scripting.

#8. Seamlessly integrate with a broad array of identity providers and solutions.

Zscaler has deep integrations with identity providers like Microsoft and Okta, and endpoint detection and response (EDR) platforms like CrowdStrike.

Zero trust security starts with verifying the identity of the user who's attempting to gain access to an application or other resource.

As growing numbers of organizations adopt cloud-first strategies to support today's work-from-anywhere environments, they're turning to a broad array of identity and access management (IAM) and identity governance and administration (IGA) partners to support their ability to manage authentication and user identities across their lifecycle.

A ZTNA solution should integrate with your current IAM and IGA partners, of course. But look for a provider that has established strong alliances with all of the industry's best-in-class technology solution providers if you want to future-proof your identity and authentication strategy.

#9: Incorporate integrated deception technology to foil attackers.

Deception technology is a new category of cybersecurity solution.

Using deception technology makes it possible to detect real-world threats quickly with very low false positive rates. It involves deploying realistic decoys (e.g., domains, databases, directories, servers, apps, files, credentials, and breadcrumbs) in a network alongside real assets to act as lures. The moment an attacker interacts with a decoy, the technology begins gathering intel that it uses to generate high-fidelity alerts.

Leveraging deception technology can improve your security team's ability to detect threats, generate better insights into the risks your business faces — in real time — and enable you to better cover what would otherwise be blind spots in your environment. The deception decoys act as tripwires in a zero trust environment, detecting compromised user accounts or attempts to move laterally across the network.

Because this is an emerging technology, few ZTNA vendors have yet to integrate deception platforms, but industry leaders have already made this advance.

KuppingerCole named Zscaler a leader in Distributed Deception Platforms.

#10. Allow for fast and easy deployment.

Unlike other technology solutions that can take weeks or months to deploy, industry–leading ZTNA can be deployed from anywhere in a matter of days.

Zscaler enabled the City of Los Angeles to provide secure work–from–anywhere access to 18K employees in less than two weeks.

See for yourself why Zscaler Private Access is the world's most-deployed ZTNA platform

Zscaler Private Access (ZPA) does all this and more. Built on Zscaler's unique zero trust architecture, ZPA applies the principle of least privilege to give users secure, direct connections to private applications while eliminating unauthorized access and lateral movement. Because ZPA is a cloud-delivered service, it can be deployed in hours, replacing legacy VPNs and remote access tools with a modern, holistic zero trust platform.

Zscaler Private Access delivers:

- **Peerless security, far beyond what legacy VPNs and firewalls can achieve:** Users connect directly to apps, not the network, minimizing the attack surface and eliminating the possibility of lateral movement.
- **The end of private app compromise:** Best-in-class application protection, with inline prevention, deception, and threat isolation, minimizes the risk that user account compromise poses.
- **Superior productivity for today's hybrid workforce:** Lightning-fast access to private apps that extends seamlessly across remote users, corporate and branch offices, and third-party partners.
- **Unified ZTNA for users, workloads, and devices:** Employees and partners can securely connect to private apps, services, and OT/IoT devices within the industry's most comprehensive ZTNA platform.

Want to learn more? Request a free demonstration today.

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.