ZTNA Everywhere

Unlocking the Power of Universal Zero Trust Access

Think about how many ways people in your organization connect these days. You've got employees on personal phones checking work email, contractors needing access to specific cloud tools, and remote teams logging in from homes and cafes across the globe.

Meanwhile, your applications live everywhere—some in SaaS platforms, others in multiple public clouds, still more in private data centers.

Multiply all of that—distributed users on diverse devices, accessing applications across countless locations and environments—and it gets complicated fast. This modern reality creates significant security and operational strain for IT teams. Just getting simple things done can be a headache.

Many enterprises are still trying to manage this complexity with older tools, hoping they're enough. But the fundamental way we work has changed, and traditional access models, built for a time when the network perimeter was clear and most resources were inside the data center walls, haven't always kept up. Meanwhile, attempting to layer or patch tools together leads to a fragmented approach, blind spots and increased risk.

Navigating the modern digital enterprise requires a fundamentally different approach to access, one built for complexity and scale. This is where Universal Zero Trust Network Access (ZTNA) comes into play.

Universal ZTNA provides consistent, secure access for all users, regardless of their physical location. It's designed to support access to every type of application within your digital environment, from modern SaaS and cloud services to your essential legacy systems, wherever they reside. This is bigger than just securing remote workers; it's about applying zero trust principles to everyone and everything interacting with your digital resources.

In this whitepaper, we'll define the transformative potential of Universal ZTNA, uncover its five core benefits for security and IT leaders, and discuss how your organization can begin the journey towards a more modern, unified access model.

Why traditional access models fall short

Amid today's distributed workforce and diverse application environments, it's becoming increasingly clear that the security tools and strategies built for a different era are struggling to keep up. The way we work has changed, but our access models haven't always evolved at the same speed. This discrepancy leads to significant security and operational strain.

Consider the tools that have long been the standard:

⊗ VPNs (Virtual Private Networks)

For years, VPNs were the go-to for remote access. However, a key limitation is that once a user is authenticated via VPN, they often receive a broad network connection. This lacks the necessary context-awareness for modern threats; it doesn't check why a user needs access to a specific application or server. It's like giving someone the keys to the entire building just so they can get into one office room. Furthermore, scaling VPN infrastructure for a large, remote workforce creates bottlenecks, performance issues, and management headaches.

⊗ VDIs (Virtual Desktop Infrastructure)

While VDIs can offer a seemingly more controlled environment by placing users in a virtual machine managed by IT, they come with their own set of challenges. The infrastructure cost required to run VDI effectively can be significant. Moreover, the user experience is inconsistent, heavily dependent on the user's endpoint device and home internet connection. Trying to quickly scale VDI is costly and complex.

⊗ Perimeter-based firewalls

Traditional firewalls remain critical for network security. However, their primary function is typically to protect the boundary and stop threats coming in from the outside. They are not designed to control access between users and applications that exist outside that old perimeter, such as SaaS applications or resources in the public cloud.

These tools were largely designed for a time when the network perimeter was clearer, and most key applications resided securely within the data center walls. That simply isn't the reality for most businesses today.

And when organizations try to address the complexities of a modern, distributed environment by patching multiple tools together, it results in a fragmented security approach. You end up with different systems and different rules that don't communicate effectively. This leads to gaps, inefficiencies, blind spots, makes managing access policies incredibly difficult, and ultimately increases your actual security risk.

This is precisely why a more strategic, unified approach is needed—one built for today's challenges.

What Universal ZTNA really means

Having explored the limitations of access models built for a bygone era, it's clear a new approach is needed. At its core, ZTNA is built on a powerful, essential principle: "never trust, always verify." It assumes that no user or device, regardless of location or initial authentication, is inherently trustworthy. Access is never granted broadly to the network; instead, it's granted specifically to the required application based on verified identity and context.

Universal ZTNA expands this critical concept significantly. It's not just about replacing VPNs or securing remote workers. It's designed as one unified architecture for secure, context-aware access that extends the zero trust principle across your entire digital ecosystem.

What makes ZTNA universal?

01 Consistent, secure access for all users

Universal ZTNA provides protection and access for every type of user, regardless of their physical location. This includes remote employees, hybrid workers, third-party contractors, partners, and even users on guest networks.

02 Support for every application type

Universal ZTNA is built to handle access to every kind of application within your environment. This spans modern SaaS applications, cloud-native tools residing anywhere in the world, crucial legacy systems still in your data centers, VoIP, server-to-client connections, and even applications hosted by third parties or running in factory IT/OT systems.

03 Access from any location or environment

Whether users are working remotely, in the office, from a branch, or connecting to applications hosted in your data center, a public cloud (AWS, Azure, Google Cloud), or even a partner's environment, Universal ZTNA provides a way to stretch that same zero trust security consistently across all locations and environments.

04 Enforcement of least-privilege policies

Users only gain access to the specific applications or resources they absolutely need, and nothing more. This access is not a one-time event; it's continuously verified. The system performs inline inspection and considers posture-aware controls, checking factors like the user's identity, device health (Is it patched? Does it have malware?), location, and the specific application being requested in real-time before granting or maintaining access.

Essentially, universal ZTNA moves beyond just improving security for remote access, to applying zero trust principles to everyone and everything interacting with your IT resources. It hides your applications and IP addresses from the internet, ensuring users are never placed on the network directly but are connected securely only to the specific applications they are authorized to access. This fundamentally reduces your attack surface and eliminates the possibility of lateral threat movement within your network.

Patching together legacy tools designed for a different world creates gaps, complexity, and significant risk in our distributed, multi-environment reality. Universal ZTNA provides the architectural underpinnings needed to securely and efficiently navigate complexity for security teams, IT, and business leaders alike.

Five ways Universal ZTNA improves access and security

Universal ZTNA offers a unified, strategic approach to access that delivers concrete benefits across security, operations, and user experience. Here are five key ways it reshapes access:

01 Secure access for all users, on any device

Universal ZTNA leverages user identity combined with device context to make real-time access decisions. The system confirms who the user is and checks the security posture of their device. This is particularly critical for BYOD, enabling you to enforce security requirements and provide differentiated levels of access based on how trusted the device is, even if IT doesn't directly manage it. This ensures comprehensive security coverage for your entire user base, irrespective of device ownership or connection point.

02 Context-aware access

Universal ZTNA is designed to provide consistent, secure access to all application types, from your latest cloud services to those crucial older applications still running in your data center, VoIP systems, server-to-client connections, third-party hosted apps, and even IT/OT systems in factory environments. It simplifies this complexity by providing context-aware access, understanding the user's identity, device posture, and the specific application being requested. This means you don't need different access solutions for different app types. Access policies can be applied uniformly, ensuring users only connect to the specific applications they are authorized for, wherever those applications reside.

03 Seamless support for all environments

In a world where applications and users are scattered, your access solution needs to span every environment. Universal ZTNA's comprehensive reach ensures that regardless of where an application is hosted—on-premises, in a multi-cloud setup, or even accessed by your users when hosted by a business partner—the same granular, context-aware access controls are enforced.

04 Simplified segmentation

Instead of building rigid network walls, Universal ZTNA connects users directly to the specific applications they need, creating segmented access pathways. This is achieved at a higher level of abstraction (the application layer), making it easier to deploy and manage compared to wrestling with network infrastructure. By ensuring users are never placed directly on the network and only connected to authorized applications, it reduces your attack surface and dramatically limits an attacker's ability to move laterally within your environment if a single user or device is compromised.

05 A frictionless experience

Managing access policies across disparate legacy tools is notoriously complex, leading to fragmentation and operational strain. Universal ZTNA provides a unified architecture where access policies are managed centrally, from one single console. Policies are defined based on user identity, device, and application, not complex network details like source/destination IPs or protocols. This streamlines policy management and reduces the complexity associated with traditional network routing. The result is a seamless, application-aware experience where users get the resources they need without jumping through hoops. For security teams, the result is centralized visibility into user access patterns across all applications and environments, improving monitoring and incident response. This operational simplicity and improved user experience ensures that security doesn't come at the cost of productivity or lead to users bypassing security for convenience.

Making the shift to a Universal ZTNA model

Implementing Universal ZTNA involves a fundamental transformation of your access and security strategy. Organizations can, and often should, approach this transition incrementally. Start with specific high-risk areas or user groups, gain experience, and then gradually expand the zero trust principles across more users, devices, applications, and environments. This strategic, phased approach makes the complex task of modernizing access more manageable.

Here are key considerations for starting the journey:

01 Identify high-risk access scenarios

Pinpoint the areas of your current access strategy that pose the greatest risk. This may include third-party access, like vendors or contractors connecting to your systems, a frequent weak point. Access originating from unmanaged devices, such as personal laptops or tablets, is another high-risk scenario to address early. Providing secure access to critical legacy applications—especially those not originally designed with modern security in mind—can be a priority. Targeting these specific scenarios first can often yield the most immediate security uplift.

02 Reassess VPN and VDI usage

Honestly evaluate your current reliance on traditional VPN and VDI solutions. Ask whether they remain the most effective and secure tools for the job in your current, distributed environment, or if they are contributing to complexity, inefficiency, or increased risk. Recognizing the limitations of these legacy tools in meeting modern access needs is a necessary step in understanding the value of a ZTNA approach.

03 Align access policy across environments

Work toward establishing consistent access policies that span all your different environments. This means striving for the same rules and level of scrutiny whether users are remote or in-office, accessing applications in your data centers, public clouds, or hybrid setups. Having vastly different access rules for different parts of your infrastructure can undermine the core principles of zero trust and create security gaps.

04 Look for key technical capabilities

When evaluating potential solutions to support your ZTNA journey, consider essential features that enable the "never trust, always verify" principle. Strong integration with your existing identity provider is vital for verifying user identity and ensuring a smooth experience. Broad browser support is important for practical accessibility across various devices and user types. Critically, look for solutions that include built-in threat protection capabilities, such as inline inspection and threat detection, as security enforcement and access control go hand-in-hand in a robust ZTNA model.

Success story: Hastings Direct

Hastings Direct, a leading UK insurance provider, set out to become the nation's largest digital insurer. But it faced significant challenges with its traditional infrastructure, including legacy VPNs and firewalls that caused excessive downtime, increased latency, and lacked granular, role-based access controls. This complexity frustrated employees and increased cyber risk.

Recognizing that the status quo could no longer support its cloud-first operations, Hastings Direct embarked on a phased journey, adopting a cloud-native, comprehensive zero trust architecture. They began by securing internet and SaaS access, gaining crucial end-to-end visibility, and ultimately replaced their legacy VPNs with ZTNA for secure, direct-to-app connectivity.

By eliminating the need to extend network access and hiding applications from the internet, Hastings Direct achieved a significant reduction in attack surface. In just one quarter, it was able to process billions of transactions, preventing 45 million policy violations and blocking over 14,000 security threats. Beyond security, Hastings Direct experienced a material improvement in user experience across performance and stability, enabling secure, work-from-anywhere flexibility without disruption.

> CIO Simon Legg summarized the impact: "In security, there is a constant balancing act between bad friction and good friction. Bad friction stops organizational productivity. Good friction stops the bad actors. Zscaler helps us eliminate the bad and amplify the good."

Redefining access for a smarter, more secure enterprise

The complexities of today's distributed workforce and diverse application landscape demand new access models. Embracing Universal ZTNA represents a fundamental shift in how organizations approach security and connectivity.

This transformation isn't solely focused on reducing risk, although the security benefits—from dramatically reducing the attack surface through simplified segmentation to providing comprehensive security for all users, devices, applications, and environments—are profound. Critically, Universal ZTNA is also about enabling productivity and agility across the modern digital enterprise. By providing seamless, context-aware access to needed resources, regardless of location or device type, it empowers users and streamlines operations for IT and security teams.

Organizations that adopt this forward-thinking approach position themselves for growth, enhanced security, and greater user satisfaction.

We encourage you to evaluate your current access strategy in light of the five principles of Universal ZTNA. Consider the complexity you are currently managing across different users, devices, locations, and applications. How could a unified, context-aware architecture simplify and unify that complexity for your organization?

↗

To explore how Universal ZTNA can specifically address your environment's challenges, request a demo or watch our latest webinar on the topic

REQUEST A DEMO

WATCH THE WEBINAR

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. To learn more, visit www.zscaler.com.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.com