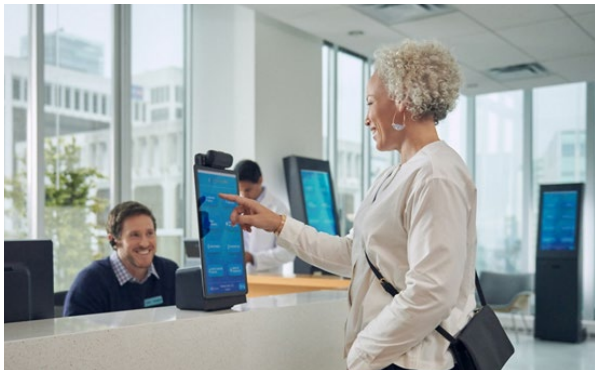
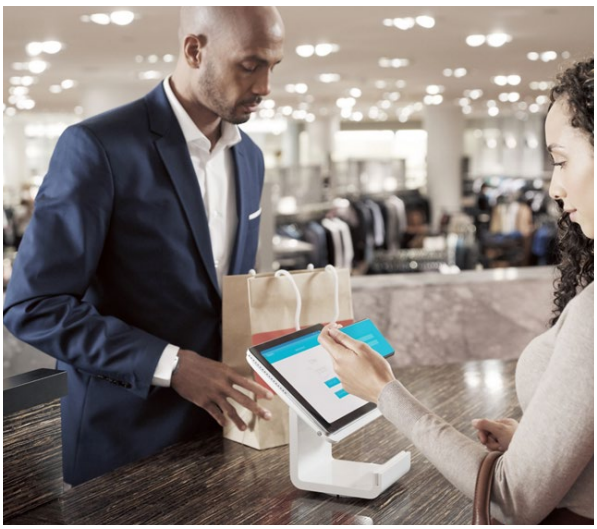
AT&T Business

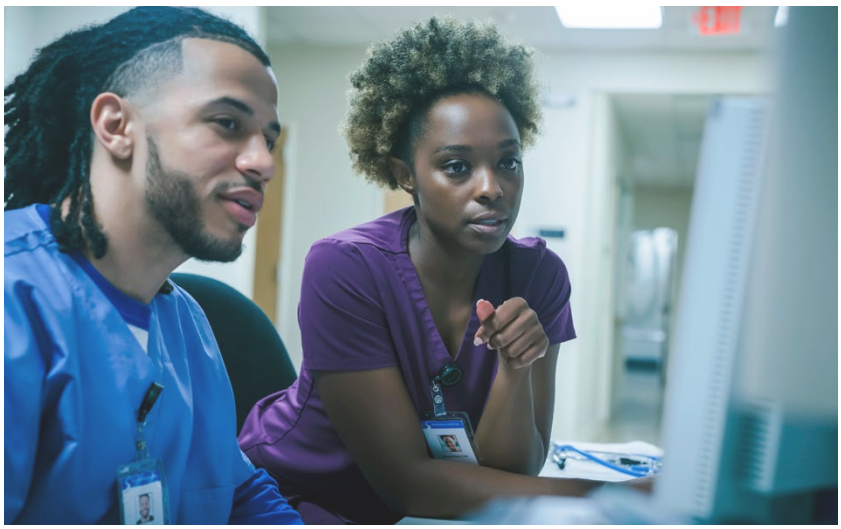
zscaler™

AT&T Cybersecurity

Three essential elements for zero trust success

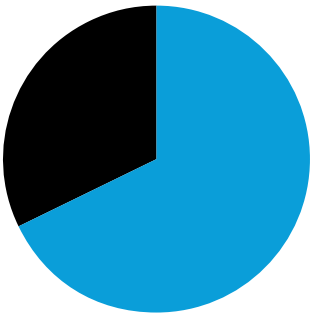




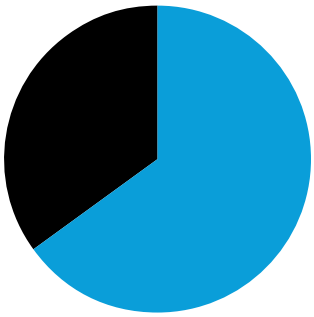


The drive for agility and improved data flow has fundamentally changed the way modern businesses operate. Employees have left the corporate office, working and accessing applications and data from everywhere and at all times. Applications have moved out of the data center and into the cloud in the form of software-as-a-service (SaaS) applications, such as Microsoft 365, and private applications hosted in AWS, Azure, and Google Cloud Platform. Not surprisingly, a majority of companies say their sensitive data is now located outside of the enterprise data center.[1]

The shift to cloud-based applications has drastically expanded the attack surface, exposing businesses to new threats. Traditional security architectures, focused on protecting the network and users within it, are no longer relevant. To address these challenges, organizations are rethinking 30 years of network and security methodology and migrating to a model based upon **zero trust**.



68% of companies say that more applications are consumed from SaaS than from enterprise infrastructure[1]



65% of companies say that more sensitive data is located outside of the enterprise data center than inside[1]

72% of respondents from a 2021 global survey reported that they have plans for adoption of zero trust in the future or have already adopted it.[2]

What is zero trust?

The concept of zero trust has been around for more than a decade, and it is not applied through one single technology or application. To secure today's organizations, zero trust begins with the following assertion: **No user or application should be inherently trusted.**

A zero trust security platform depends on the following key principles:

- Principle #1: **Connect users to applications and resources**, not the corporate network
- Principle #2: Make **applications invisible** to the internet, to eliminate the attack surface
- Principle #3: Use a **proxy architecture**, not a passthrough firewall, for content inspection and security

Let's take a closer look at each.

Principle #1

Connect users and applications to resources, not the corporate network

Traditionally, users and applications connect to the corporate network, with access to all applications and data within that network segment. The first principle of a zero trust approach is to provide access only to the applications and resources needed and nothing else.

The challenge with traditional security

Employees, contractors, and other third parties need access to SaaS and private applications to be productive. They expect their access to be seamless, no matter what device they use, or where they connect. Traditional virtual private networks (VPNs) and firewalls place users on the network for application access, via inbound connections. These inbound connections create holes in your security, increasing risk for your users and your organization. Once on the network, users are designated as trusted, and are typically granted full access to the network segment and all enterprise applications and data hosted within it. Such broad permissions often exceed those required to complete job duties. Bad actors can have free rein on the network, which needlessly exposes sensitive data to exfiltration. This inherent trust placed in network users also provides opportunity for malware to propagate freely once the connection is made, leading to more widespread damage across the enterprise.

In the face of this new perimeter-less world, how do organizations provide the access users need AND defend themselves against malware and advanced threats?

What to look for in a zero trust approach

Productivity should not require businesses take an all-or-nothing approach with user access to applications. A zero trust approach means securely connecting authenticated users only to a specific authorized application. This zero trust access is based upon least privilege principles (user gains access only to resources needed), using identity, real-time context, and business policy—without ever putting the users on the corporate network.

Instead of a network-centric approach to security, zero trust focuses on securing the connection between the user and the application. Decoupling network access from application access naturally isolates users. This approach eliminates the need to deal with the complexities of network segmentation and prevents the lateral movement of malware in the event of compromise, ultimately reducing business risk.

Principle #2

Make applications invisible to the internet

The migration to cloud applications has greatly expanded the attack surface, challenging traditional security. Global spending on information security is expected to exceed $170 billion in 2022 and with the increase in cyberattacks, where businesses spend that money is significant.[3]

Traditional firewalls broadcast the location of applications to facilitate onnectivity. That means the very tools organizations have implemented to protect the network are actually creating a massive security vulnerability. The unfortunate result is an increased exposure to risk, the exact opposite of your security team's best intentions.

The second principle of a zero trust approach is to make applications invisible to the internet, avoiding exposure of the corporate network.

The challenge with traditional security

Legacy security architectures were designed to connect users to the corporate network. The inbound connections created by users connecting via VPNs and network firewalls expose network and application Internet Protocol (IP) addresses to the internet. While this may help users to connect to the applications and data they need to do their jobs, it also allows **anyone** to ping the network, regardless of whether they are an authorized user—including cybercriminals searching for potential attack vectors. Making IP addresses visible increases the potential attack surface and leaves organizations vulnerable to internet-based threats.

What to look for in a zero trust approach

Adversaries can't attack what they can't see. The goal, therefore, should be to make the network and applications invisible to attackers and accessible only to authorized users. This requires a solution that is designed to:

- Conceal source identities
- Obfuscate IP addresses

This approach shields network resources from being exposed to the internet, keeping them hidden from unauthorized users.

The result? A greatly reduced attack surface, protection against distributed denial-of-service (DDoS) and targeted internet-based attacks, and secure access to applications—on the internet, in SaaS, or in public or private clouds—wherever users connect.

Principle #3

Use a proxy-based architecture for content inspection and security

Encryption has become the status-quo for securing traffic to the internet and cloud applications. According to Google, 95% of the traffic across their platform is encrypted.[4] Unfortunately, as the volume of SSL traffic continues to increase, attackers are finding ways to hide threats within encrypted traffic.

Today nearly half of all malware is encrypted to evade detection[5], which means that if businesses are not inspecting SSL encrypted traffic, they cannot effectively prevent data exposure and misuse.

The third principle of a zero trust approach is to assume all traffic is potentially threatening and inspect all of it, through a proxy-based architecture.

The challenge with traditional security

Next-generation firewalls were not designed to decrypt and inspect encrypted traffic at scale. This reality forces organizations to choose between availability or slowing down traffic to allow the firewall to enforce security protocols. **Availability always wins.** As a result, organizations end up bypassing the inspection of encrypted traffic, increasing the risk of cyber threats and data exposure.

Further complicating matters, firewalls use a "passthrough" approach that allows unknown content to reach its destination before any analysis is complete. An alert is sent if a threat is detected, but that may be too late.

What to look for in a zero trust approach

Protecting users and data requires inspection of all traffic, including SSL. Look for a solution that uses a proxy architecture, not a pass-through firewall. To ensure effective threat protection and comprehensive data loss prevention, the solution must be designed to:

- Natively decrypt and inspect SSL sessions
- Analyze the content within transactions
- Make real-time policy and security decisions before allowing traffic to reach its destination

The solution needs to do all of this at scale to automatically keep up with changing business demands—without performance degradation, no matter where users connect.

Are you ready for zero trust?

Digital transformation makes enterprises more agile and efficient—but it requires them to rethink their network and security architectures. Zero trust provides the foundation for cloud-first organizations to accelerate digital transformation and empower employees to work productively and securely from anywhere. A zero trust approach helps businesses enable the new and evolving workplace while addressing its networking and security challenges.

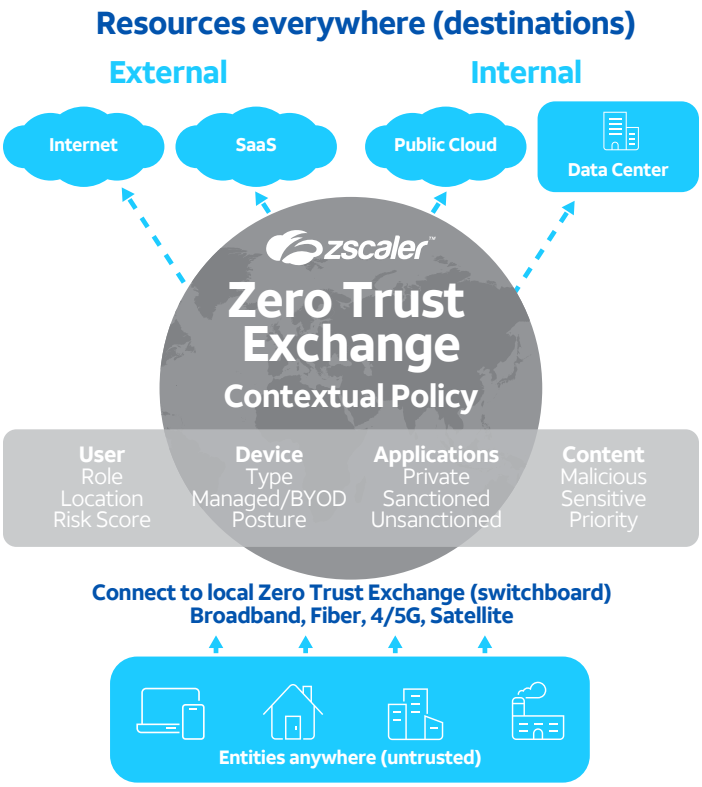
How zero trust tackles three of today's most difficult challenges:

Security	Networking	Enabling the modern workplace
Prevents cyber threats Zero trust delivers cyber threat protection for users, cloud workloads, servers, and SaaS applications.	**Simplifies user and branch connectivity** Zero trust allows users to securely connect to virtually any destination directly over the internet, regardless of where the user connects.	**Secures work-from-anywhere** A zero trust solution should let employees safely and seamlessly work from anywhere—without worrying about the network or a VPN connection.
Prevents data loss Zero trust provides a holistic approach to preventing data loss, whether intentional or not.	**Secures cloud connectivity** Zero trust lets workloads connect to other workloads, reducing the risk of lateral movement inherent to traditional site-to-site VPNs.	**Optimizes user experiences** Zero trust helps organizations consistently enable productivity by delivering a great user experience.

As businesses begin their journey, keeping these key principles in mind will align them for success.

- First, select a platform that uses identity and business policy to establish trust, and **connects users to resources without placing them on the corporate network.**
- Second, **protect applications by making them invisible** to adversaries and accessible only by authorized users.
- And finally, **use a proxy architecture, not a passthrough firewall,** to secure data and ensure effective cyber threat protection.

Together, AT&T and Zscaler simplify the adoption of zero trust and enable enterprises to confidently accelerate their digital transformation and address the challenges of moving applications to the cloud.



Zero trust solutions from AT&T powered by Zscaler provide uncompromised threat protection and data loss prevention and help securely connect users to the applications and data that they need to be productive—anywhere they work.

This solution comprises these two elements:

- **AT&T Secure Remote Access, powered by Zscaler**
- **AT&T Secure Web Gateway, powered by Zscaler**

Offered as a fully managed or co-managed service, zero trust solutions from AT&T powered by Zscaler simplify IT by eliminating the technical debt of legacy security architectures and reducing the burden on in-house IT teams. The scalable cloud-based platform enables fast, secure connections and allows employees to work from anywhere, using the internet as the corporate network. By combining the flexibility of AT&T Managed Services with the strength of these zero trust solutions powered by Zscaler, enterprises can reduce risk, simplify IT, and deliver a great user experience with a cloud-delivered zero trust architecture.

Take the first step:

Discover how **zero trust solutions from AT&T powered by Zscaler** can help you implement zero trust and secure your workforce in today's work-from-anywhere world.

To learn more about **AT&T Secure Remote Access, powered by Zscaler**, go to: https://cybersecurity.att.com/products/secure-remote-access

To learn more about **AT&T Secure Web Gateway, powered by Zscaler**, go to: https://cybersecurity.att.com/products/secure-web-gateway

1 IDG Survey, "Network Security Approaches and the Case for Zero Trust", November 2020. https://info.zscaler.com/industry-report-leading-cxo-and-it-leaders-see-it-future-in-zero-trust

2 Mlitz, K. 2021. Organizations' views on adopting zero trust IT models worldwide 2021, Statista.com, May 28, 2021. Retrieved June 15, 2021 from https://www.statista.com/statistics/1228254/zero-trust-it-model-adoption/

3 Morgan, Steve. 2019. Global Cybersecurity Spending Predicted to Exceed $1 Trillion From 2017-2021. Cybercrime Magazine, June 10, 2019. Retrieved June 14, 2021 from https://cybersecurityventures.com/cybersecurity-market- report/

4 Google. 2021. Transparency Report. Retrieved June 14, 2021 from https://transparencyreport.google.com/https/overview

5 Vijiyan, J. 2021. Nearly Half of All Malware Is Concealed in TLS-Encrypted Communications. Dark Reading, April 22, 2021. Retrieved June 13, 2021 from https://www.darkreading.com/vulnerabilities---threats/nearly-half-of-all- malware-is-concealed-in-tls-encrypted-communications-/d/d-id/1340792