Persistent | zscaler™

Defending Your Enterprise Through Zero-Trust Security

A Practical Approach from Persistent and Zscaler

Table of Contents

Today's sophisticated cyber threats can easily circumvent IT strategies focused on securing the edge. In the current IT landscape, internal and external users dynamically access data and applications across borders through devices and networks not directly controlled by security teams. A perimeter-centric approach in traditional security practices presumes a monolithic IT structure, even though most IT environments are now highly distributed, even shared, with the ubiquity of the cloud and the move to a hybrid work culture.

Moreover, bad actors are not invariably outside the enterprise either. Per Verizon's 2023 Data Breach Investigations Report, 74% of security breaches can be traced back to an employee either purposefully doing something they shouldn't or falling prey to bad actors attaining access or information from them. Access to applications and data can no longer be contingent on a network. Gartner predicts that in another three years, seven in every 10 employees will access confidential company data via applications, devices, or networks outside the purview of IT teams — up from 4 in 10 in 2022.

These changing circumstances require a recalibration of enterprise security strategies.

The emerging approach presupposes a breach will happen or has happened, denies access to users by default, and blocks lateral movement within an enterprise network. Working on the principle of least-privileged access is a pivot away from traditional security practices that allow blanket access to anyone inside the perimeter.

This framework, known as Zero-Trust, does not treat security as an overlay. Rather, it proactively embeds security into the heart of the network by inspecting data in transit everywhere within the enterprise. Application access is contingent on user identity, device, profile, and prior authorization, even if the network access is granted.

Just like digitization, implementing a Zero-Trust security architecture is a journey. It requires stakeholder coordination, management buy-ins, and a strategic outlook toward tooling, access policies, security guardrails, and the overall corporate security mindset. It democratizes enterprise security and holds all employees, third-party agencies, guest users, and executive leadership accountable.

Persistent embarked on the Zero-Trust journey five years ago, which allowed us to prioritize security across our global enterprise of 23,000+ knowledge workers. We partnered with Zscaler, an enterprise security solutions leader, to deploy a Zero-Trust Network Architecture (ZTNA).

Since then, we have implemented Zscaler's ZTNA across clients, and through our product engineering mindset, we have deconstructed this journey down to a science.

We have a Zscaler playbook highlighting best practices to ensure a seamless and high-performance ZTNA implementation. We currently have more than 160 Zscaler-certified professionals who help our enterprise clients take the first steps toward Zero-Trust security.

This white paper provides a snapshot of our own journey with Zscaler and our Zscaler success stories across industries – from heavily regulated to data-intensive – that demonstrate the business benefits of pivoting to a Zero-Trust security architecture.

Implementing Zero-Trust Security

As Persistent grew in revenue, size, and distributed scale, it needed to adopt a security strategy commensurate with changing business realities. A proxy network did not serve its security needs. Most users had admin access, and there was no way to pre-empt errors that could expose internal applications. Persistent's security architecture was a combination of tools gathered from more than 19 vendors, which resulted in high maintenance and alert management costs due to multiple tools handling similar information. While the security costs escalated, the company was still vulnerable to constantly evolving cyberattacks.

To ensure all resources are accessed securely, regardless of location or network, Persistent must strictly define and enforce access policies,closely log, monitor, and inspect network traffic, and provide users with dynamic, per-connection, policy-based access.

A multi-tool, multi-vendor perimeter-centric security architecture could not support this level of visibility and dive-deep into application access management.

There was a need to pivot to a different mindset that secures not just the network edge but every node, connection, and user access within that network — in other words, a Zero-Trust approach.

Persistent evaluated four vendors to steer its Zero-Trust journey, including Zscaler, a leader in enterprise security and Zero-Trust digital transformation. Zscaler emerged as an obvious choice for its security tools, fine-grained network control even in the extended enterprise, and its product roadmap and network security mentality to kickstart Persistent's Zero-Trust security journey.

Persistent Onboards Zscaler's Zero-Trust Network Access

Persistent started with keeping the Identity and Access Management (IAM) configuration up-to-date, which was vital in deciding which user profiles should have access to which applications. It then deployed Zscaler's Internet Access (ZIA) solution as an alternative to a proxy network.

The solution provides robust protection for users, workloads, and devices accessing SaaS applications and the internet through a Zero-Trust switchboard, effectively thwarting attacks and data loss while eliminating the need for a perimeter network.

Persistent users get clean and secure internet access without a Virtual Private Network (VPN). This led to infrastructure optimization and the sunsetting of more than a dozen tools, resulting in cost-takeout.

Persistent also evaluated the existing network to determine which components needed to be replaced or modified. This process ensured all critical applications were onboarded with additional Zscaler modules, comprising Zscaler Private Access (ZPA) and Zscaler Digital Experience (ZDX). ZPA restricted access to only Persistent users, thus reducing attack surfaces and lateral movement. ZDX monitors the end-to-end connection from users to applications and can quickly isolate any issues and resolve them quickly, often before users notice them. Additionally, Persistent implemented CrowdStrike, which is integrated with the Zscaler platform, to provide advanced endpoint security and forensic capabilities.

Persistent Secures 85% of its Threat Exposure

Persistent improved its overall security posture by 85% and saved more than $2 million annually by optimizing its security tools and infrastructure.

Pivoting to a Zero-Trust security architecture significantly reduced the threat exposure, ensured secured access to verified users, and provided significant potential savings in breach risks.

With a location-agnostic security framework, Zscaler ensured access to clean internet anytime, anywhere.

Persistent also gained visibility into bandwidth utilization, with relevant insights into online traffic in near real-time, helping orchestrate bandwidth to support business-critical applications. Zscaler enabled content filters based on custom policies, which was important to secure workloads for clients from heavily regulated industries such as banking, insurance, and healthcare. Authorized access to sensitive data and relevant restrictions on data uploads to personal domains enabled Persistent to build and capitalize on client trust.

Client Successes with Zero-Trust Security

Large Retail Pharmacy Chain Ensures Day-One Security

As a carve-out entity from a larger organization, our client had to set up a standalone tech stack from the ground up, including a fully independent network, infrastructure, data, applications, and IT endpoints, such as laptops and mobiles.

Since this was the first time the client would operate as a new company, ensuring secure access to data and applications from Day One without business interruption or impacting employee experience was a key concern.

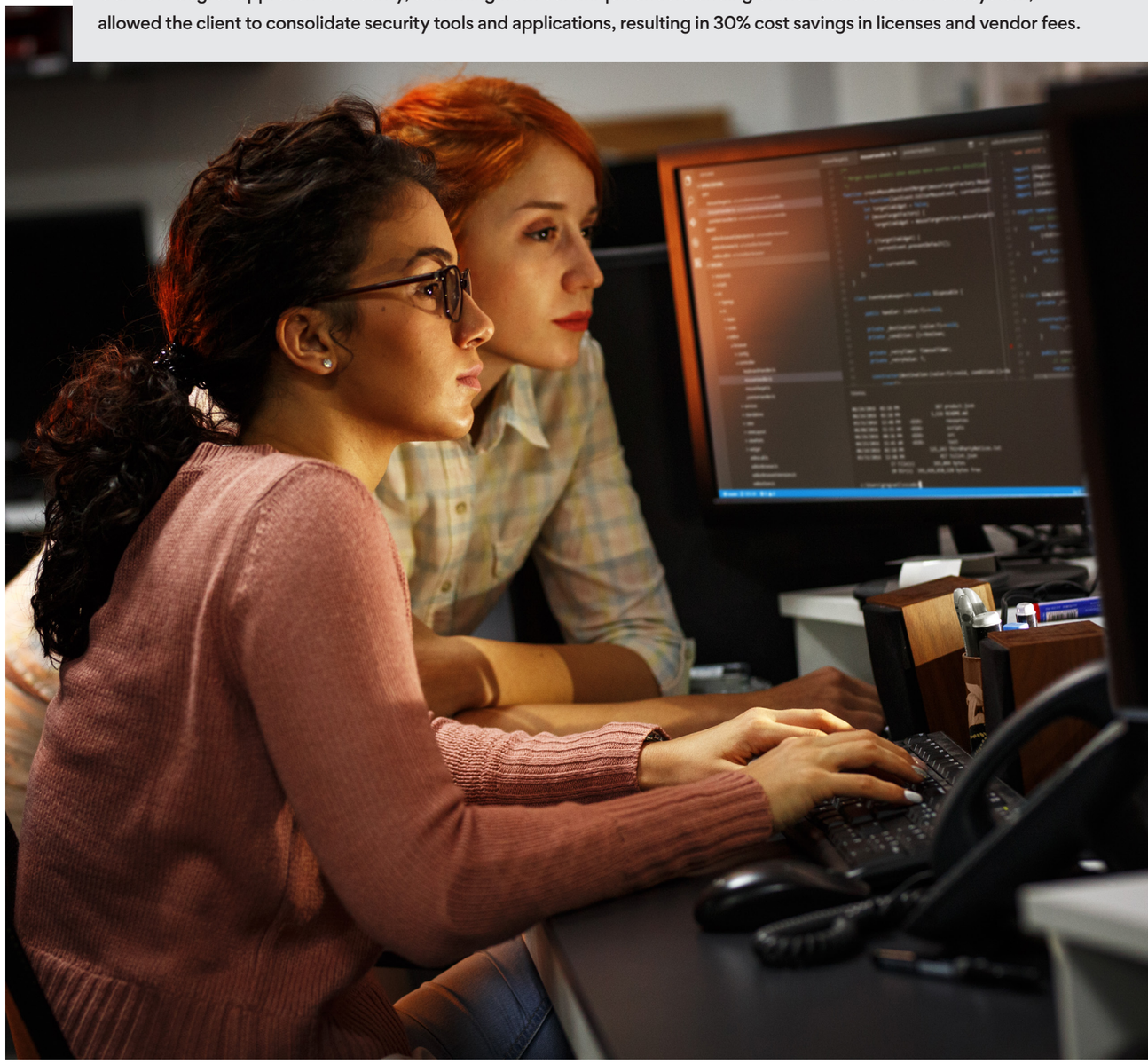
A stringent Transitional Service Agreement (TSA) mandated that the client move its IT applications out of the parent company's data centers. This was a significant challenge as most applications had yet to be migrated to the new company's cloud servers hosted on Amazon Web Services (AWS), which was scheduled to take six months after the network separation phase. In this interim, the client risked losing access to these applications.

The client entrusted Persistent with transitioning its tech stack from the parent company's data centers to AWS servers, prioritizing Day One security.

Secure and Uninterrupted Access to Business Applications

By working with the client to seed a Zero-Trust approach to security, Persistent secured more than 1,500 IT applications and endpoints. Furthermore, with our app connector solution, the client was able to comply with TSA obligations, ensuring its employees uninterrupted access to business applications. With the right access to the right users, the client ensured application access was secure and verified without hampering end-user experiences.

Our 360-degree approach to security, stemming from our unique understanding of the Zscaler solution ecosystem, allowed the client to consolidate security tools and applications, resulting in 30% cost savings in licenses and vendor fees.



Implementing Zscaler Zero-Trust Network Architecture Suite

As a new company with greenfield IT infrastructure and network services, the client was ideally placed to pivot to a Zero-Trust security architecture. Working on the principle of least-privileged access, Zero-Trust bolsters enterprises' security postures by denying access by default. This helps combat increasingly sophisticated attack vectors from inside and outside an IT environment far too spread out for traditional, perimeter-centric security practices.

Persistent advocated for a Zero-Trust approach to ensure Day One security, led by the Zscaler solution suite.

Our strategic partnership with Zscaler allows us to map the right security solutions to address clients' unique business needs. We implemented a comprehensive security architecture for our client by leveraging our multi-vendor expertise and our extensive experience with the Zscaler ecosystem.

To ensure a holistic security approach, we integrated endpoint detection and response solutions with various security counterparts, such as Security Information and Event Management (SIEM), to enhance visibility, analysis, and response capabilities across endpoints, workloads, users, and networks. Additionally, we incorporated Microsoft Defender, Azure AD, IBM QROC, Office 365, Rapid7, Fortinet firewalls, Meraki switches, and access points to create an end-to-end secure environment.

While the new company's environment was being built on the AWS cloud, the client's users needed access to applications in the parent company's data center.

The Persistent team developed an ingenious idea of connecting users to applications through the AWS ecosystem using Zscaler. The new company's AWS infrastructure was linked to the parent company's AWS instance through a peering connection for secure data transfers. Persistent hosted the Zscaler App-Connectors on the new company's AWS tenant within a virtual private cloud, with access to the parent company's AWS instance to the data center application segments.

The parent company's applications were integrated with Zscaler Private Access (ZPA) through the app connectors, creating a secure way to access applications using the Zero-Trust framework. This eliminated the need for credentials or reliance on a building's network for access. The deployment, including user acceptability testing, was completed within two weeks, helping the client ensure business continuity.

Defense Supplier Onboards Zero-Trust Security Architecture

Today, the defense industry relies heavily on IT systems, data, and sensors to manage on-ground surveillance and run communication systems that allow the secure sharing of data. These applications comprise highly sensitive data that must be guarded against unauthorized access since a potential lapse could lead to massive disruptions and potential risks.

Our client, a leading manufacturer of defense supplies, wanted to upgrade its existing IT security architecture and gain more control over how its users access data and internal applications.

The client also wanted to enable a security framework that accommodates the needs of its hybrid workforce

The client's traditional, proxy-driven approach to security fell short of safeguarding its intellectual property and critical data in transit against evolving cybersecurity threats.

— adapting to changing work environments while bolstering its security posture at the core.

The company turned to Persistent to overhaul its IT security architecture to better respond to changing business needs and shifting on-the-ground realities.

Persistent Sets the Stage for Zero-Trust Security with Zscaler

The client struggled with security issues like the ones we experienced before onboarding our own Zero-Trust security architecture powered by Zscaler. Persistent reviewed the client's security framework and identified critical asset and data protection vulnerabilities. We created a High-Level Diagram (HLD) and Low-Level Diagram (LLD) mapped to use cases that addressed vulnerabilities across the IT stack.

Our client embarked on a greenfield implementation of Zscaler's Zero-Trust Network Architecture (ZTNA), starting with the Zscaler Internet Access (ZIA) to ensure only authorized access to internal applications, effectively reducing the attack perimeter with proactively established access controls authorized on each login request. This also helped the client set up restrictions and policies that blocked blanket access to applications or data and regulated access with greater control over lateral movement within the network.

With Zscaler Private Access (ZPA), Persistent further bolstered the client's security posture. Unlike traditional security practices, such as VPNs or firewalls that protect the network periphery to ward off bad actors, a Zero-Trust approach denies access to applications by default, even to users within the network, and authenticates user identity for each application that a user accesses. This ensures that applications and data are secured, even if the network is infiltrated. ZPA allows the client to ensure resources are accessed securely, regardless of the user's location, device, or network. This enabled the client's workforce to operate in a hybrid environment without exposing data or applications to potential threats.

As an added security layer, Persistent implemented the Zscaler Digital Experience solution (ZDX) to secure endpoints so the client can closely monitor laptops or mobile devices used to access applications and data. The solution gives insights into device compliance status, traffic trends, and outage-based instances logged in a dashboard that provides visibility into incident severity, root cause, and possible remediation. Persistent further bolstered the client's security posture with Zscaler's Deception technology, leveraging smokescreens, honeypots, and threat-hunting technologies — providing the ability to locate potential threats before they cause any security issues.

Zscaler Secured Web Traffic, Improved User Experiences

The client successfully secured 93% of their web traffic by implementing advanced threat and malware protection, as well as a staggering 60% improvement in end-user experience with Zero Trust Network Access, which comes with advanced data protection using Cloud Access Security broker (CASB) and Data Loss Prevention (DLP). Zscaler's Deception technology also provides an upper hand against attackers by detecting, intercepting, and diverting threats away from critical assets by distributing a collection of traps and decoys across the IT infrastructure.

Zscaler provides all employees secure internet and SaaS application access from anywhere while promoting greater security awareness among users through granular access permissions.

The client has secured IT assets and endpoints and has achieved a modern hybrid workplace with a seamless and secure user experience by replacing the traditional VPN.

Partnering for Client Security

Persistent collaborates with Zscaler as a Zenith-level partner, the highest level in its partner program. Persistent leverages this alliance to help customers stay secure and agile by protecting them from sophisticated cyber threats and data loss.

Zscaler is one of the leading and most innovative cloud-native platforms with groundbreaking capabilities to experience true Zero-Trust security. We also leverage best practices from our Zscaler implementation for our clients' benefit.

Our Strengths

360 Degree Relationship

\ Industry-aligned solution development

\ Consortium of technology partners for cyber-resilience

\ Persistent services for Zscaler

\ Significant Zscaler deployment at Persistent

\ CEO partnership sponsors

Zenith Partner

\ Joint thought leadership programs

\ Pro-serv, managed services and RE

\ Review of technology roadmap

\ Customized trainings for customers

\ Direct L3 access for customer issues

\ 135+ certifications

Execution Capability

\ Practitioner led model

\ Expertise in multivendor security ecosystem

\ Broad security focus with recognized IAM market leadership

\ Improved customer experience with Automation IP's and accelerators

IP's and Accelerators

\ Automation

- ZPA app-onboarding tool
- Chatbot for support

\ Accelerators

- Playbooks and SoPs
- 3rd party integrations