DXC Technology migrates to zero trust network access in just 90 days to drive virtual-first strategy

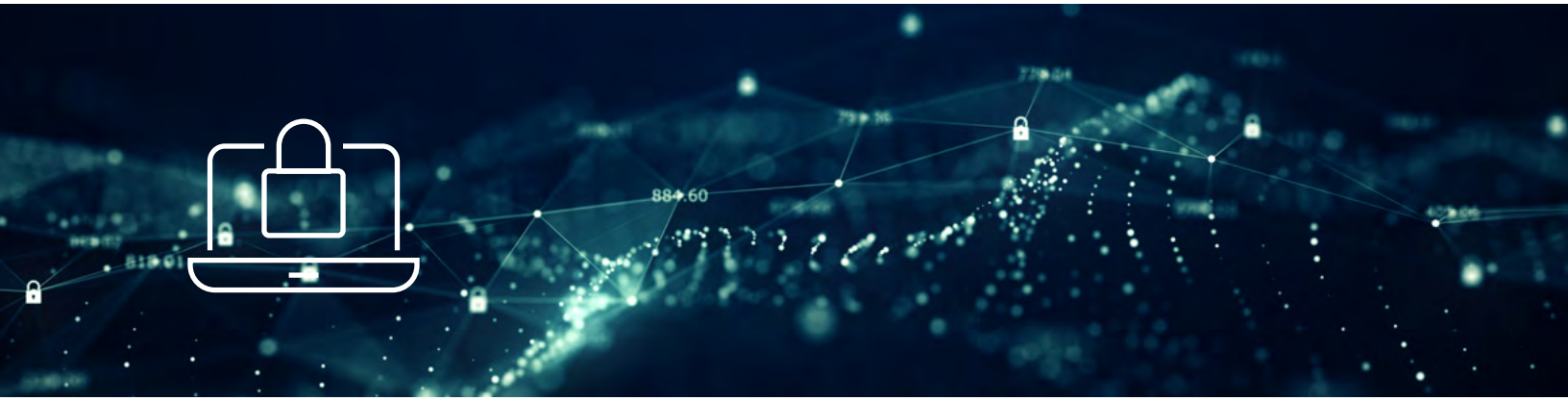
DXC Technology secures internet and SaaS access for 130,000+ global users and powers operational efficiency with the Zscaler Zero Trust Exchange

Challenges

- Secure internet and SaaS traffic for the global DXC workforce
- View and manage bandwidth in real time
- Migrate from an on-prem to a zero trust security model

Results

- Secured business at scale for more than 130,000 people, with more than 40 billion transactions and 1,982 terabytes of traffic processed in 3 months
- Boosted security posture, preventing 1.3 billion policy violations and blocking 9.2 million threats in one quarter
- Reduced business risk, detecting and blocking 1.6 million threats hidden in encrypted traffic in 90 days
- Deployed in just 90 days to drive virtual-first goals



"The positive outcomes we've experienced from Zscaler not only benefit us but also our customers, as they embark on their digital transformation journeys."

— Mike Baker
Global CISO, DXC Technology

Leading the modern workplace with zero trust

As a global leader in enterprise IT services, DXC Technology strives to be an exceptional business partner for our customers, as well as an exceptional employer for our workforce. Meeting these goals in today's competitive business environment requires supporting both in-office and remote collaboration.

DXC's strategy of enabling a virtual-first work model for our people called for a shift from the traditional perimeter-based security architecture of firewalls and VPNs. Shifting to a zero trust architecture, DXC adopted the Zscaler Zero Trust Exchange, the world's largest inline security cloud platform, to empower our global workforce and enterprise customers with the remote work environment they need to collaborate securely.

Zscaler fully supports the five pillars of the zero trust security model — identity, devices, network, data, and applications and workloads — and provides a data-centric approach with granular controls and policies. Mike Baker, global chief information security officer at DXC, explains the move: "We started by adopting the Zero Trust Exchange for specific security use cases and soon realized we had a powerful platform that could grow with us. From there, we forged a collaboration with Zscaler that would transform the future of work for DXC and our customers. Working with Zscaler enables us to meet our zero trust goals as our program matures and evolves to meet the challenges of today's threat landscape."

"From a people perspective, we prioritize remote work and evaluate what processes and technologies we need to adopt or change to keep our employees safe and secure regardless of location. I'm pleased to say we chose the right technology in the Zero Trust Exchange to support our zero trust journey."

— Suresh Gumma
Deputy CISO,
DXC Technology

Zero trust supports the future of work

As a global leader in enterprise IT services, DXC understands the challenges customers face as they navigate the endless options in cybersecurity — and that enabling remote work requires a fundamental shift in mindset. For secure remote work, DXC needed to leave behind the traditional location-centric model and adopt an identity-centric approach.

The zero trust model is the most comprehensive way to protect identity, devices, data and applications. Suresh Gumma, deputy CISO at DXC, encouraged his team to think about zero trust as a strategy wrapper to articulate the security program: "Zero trust is a great methodology in terms of bringing together people, processes and technology, and ensuring security that is frictionless and provides a great user experience."

The DXC security architecture is anchored on the U.S. Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model (ZTMM), among other leading standards, which provides a comprehensive approach to zero trust modernization. Adopting the ZTMM and supporting technologies helps DXC prevent unauthorized access to data and resources, regardless of location or device, by enforcing granular controls.

"From a people perspective, we prioritize remote work and evaluate what processes and technologies we need to adopt or change to keep our employees safe and secure regardless of location. I'm pleased to say we chose the right technology in the Zero Trust Exchange to support our zero trust journey," Gumma says.

Secure internet connections improve visibility and security posture

More than 130,000 DXC employees support large enterprises in 60+ countries. Every day, employees remotely connect to DXC environments, requiring secure access and authorization to sensitive data. The security team needed better visibility into how users accessed these environments, as well as a more consistent way to secure that traffic to prevent data loss and the spread of malware.

To secure internet and SaaS application access, DXC deployed cloud-native Zscaler Internet Access (ZIA), a core part of the Zscaler Zero Trust Exchange that enables SaaS application connectivity and intelligent traffic routing from any device, anywhere.

With ZIA, DXC can inspect TLS/SSL traffic at scale and at lightning speed in order to detect and prevent advanced attacks and malware and stop data loss in real time. DXC has dramatically reduced the risk of threats hidden in encrypted traffic, detecting and blocking 1.6 million such threats in a single quarter.

Using Zscaler Sandbox, DXC intelligently detects, quarantines and analyzes unknown threats and suspicious files to prevent compromise across all users and devices. Real-time security updates are sourced from trillions of

"Zero trust is a great methodology in terms of bringing together people, processes and technology."

— Mike Baker
Global CISO, DXC Technology

daily signals to separate the malicious from the benign. Near-instant delivery of known benign files keeps DXC users safe and productive.

With Zscaler Bandwidth Control, the DXC IT team enables granular policies to prioritize critical business applications and optimize bandwidth by use case. "From the Zscaler dashboard, the security team now has real-time visibility into device, application, and network performance and usage. These deeper insights and metrics help us quantify risk and communicate DXC's security posture to senior leadership, which is something we couldn't do before," explains Gumma.

Expanding our zero trust strategy with cross-platform integration

The DXC security team implemented CrowdStrike for endpoint device visibility and management and then integrated Zscaler with CrowdStrike to leverage the combined threat intelligence from endpoint to application. From ZIA, DXC can configure policies to authorize or block access to applications based on CrowdStrike's dynamic Zero Trust Assessment (ZTA) score for the devices we manage. The ZTA score is fed to Zscaler, which modifies device access policy in real time based on its security posture.

DXC also deployed Okta to authenticate users and verify partner and employee access rights for authorized applications. The security team integrated Zscaler and Okta for a complete zero trust solution at the identity level. Once Okta verifies a user's identity, Zscaler inspects device traffic and provides access only to required resources based on identity and context, using the principle of least-privileged access. The Zscaler–Okta integration provides DXC users with fast, secure access to the internet and SaaS applications anywhere. The combined intelligence and protection from these integrations enable the security team to act with greater confidence.

"With Zscaler providing visibility into web and SaaS traffic, CrowdStrike on the endpoint, and Okta as our identity layer, the DXC security team has a wealth of tools to conduct targeted investigations when incidents arise, allowing us to respond faster," explains Baker.

Improving employee retention, hiring and productivity

To reach our goal of attracting and retaining leading technology talent, DXC prioritized improving the user experience. Wherever our employees are located globally, DXC wants to ensure they have the same secure, seamless access to the internet and SaaS applications.

To reach our goal of attracting and retaining leading technology talent, DXC prioritized improving the user experience. Wherever our employees are located globally, DXC wants to ensure they have the same secure, seamless access to the internet and SaaS applications.

In addition to improving the user experience, DXC's shift to zero trust has also had a positive impact on recruitment: "Zscaler makes it easy for users to work from any location and supports DXC's efforts to hire from anywhere in the world. The consistent experience and reliability give DXC a real competitive advantage," Baker explains. "Everyone loves the flexibility of a virtual-first environment."

To support a safe and secure work environment, DXC blocks non-essential or inappropriate websites. "At times, users treat their corporate devices like personal devices, consuming bandwidth on non-essential sites. Zscaler blocks inappropriate and malicious sites and enables HR to set policies that help prevent incidents and access to unsanctioned content," shares Baker. "Not only has this boosted security, but it has also significantly improved productivity."

Sharing knowledge and gaining customer confidence

Soon after implementing ZIA, DXC configured our Zero Trust Exchange deployment to coexist and communicate with our customers' Zscaler environments. With just a few clicks, DXC employees can connect seamlessly and securely with customers' resources to collaborate on their IT modernization projects. "We initially invested in Zscaler to protect DXC, but we quickly realized that it instilled even more confidence in our customers because they know we're protected with the same level of security as they are," Baker says. "Moreover, we can now leverage the knowledge we have gained from our deployment to help our security customers launch and manage a Zscaler zero trust implementation. The positive outcomes we've experienced from the Zero Trust Exchange platform not only benefit us but also our customers as they embark on their digital transformation journeys."

From secure internet access to strong collaboration

DXC's successful collaboration with Zscaler has led to a strong alliance between the two security solution leaders.

"As a key collaborator, Zscaler has a deep knowledge of DXC's business and our goals. We've enjoyed a strong relationship with senior leadership at Zscaler. The level of attention and detail is uncommon for a vendor its size," Baker says. "Because we have realized significant risk reductions with the platform, we are constantly engaging with Zscaler to look at opportunities to expand the relationship."

Maturing a virtual-first strategy with enhanced capabilities

Building on our improved security posture, significant risk reductions and strategic innovation, DXC is exploring more Zscaler capabilities.

With securing customer data always at the forefront, the DXC security team is looking at Zscaler Data Protection to augment the company's data protection capabilities. Zscaler Data Protection provides consistent, unified data protection across endpoints, inline and in the cloud, following remote users and the SaaS and public cloud applications they access. Leveraging innovative machine learning–driven data discovery, it automatically locates and classifies data. Zscaler Data Protection will help DXC better understand data behaviors and risks, especially when users are handling sensitive customer information.

DXC is also exploring Zscaler Risk360™ to quantify and visualize cyber risk across the company's users, applications, assets and large ecosystem of technology collaborators. Combining data from DXC's Zscaler environment, external sources and security research from Zscaler ThreatLabz, Risk360 can provide a detailed view of DXC's risk exposure, actionable insights for remediation, potential financial impacts and executive-level reporting to guide cyber risk management and decision making.

"As a key collaborator, Zscaler has a deep knowledge of DXC's business and our goals. We've enjoyed a strong relationship with senior leadership at Zscaler. The level of attention and detail is uncommon for a vendor its size."

— **Mike Baker**
Global CISO,
DXC Technology

"We started by adopting the Zero Trust Exchange for specific security use cases and soon realized we had a powerful platform that could grow with us."

— **Mike Baker**
Global CISO,
DXC Technology

Delivering for our workforce, our customers and our organization

DXC's goal to become a virtual-first company required a seamless way to protect internet-bound traffic for more than 130,000 remote employees around the world. The organization began by deploying ZIA in just 90 days and now secures all internet and SaaS access from any location and any device.

With visibility across all web traffic, DXC sets policies for granular bandwidth control to prioritize critical business applications, ensure inline protection for all traffic and provide deep insights to reduce our worldwide physical footprint. With the Zscaler Zero Trust Exchange, DXC is powering the secure modern workplace.

Learn more at **dxc.com/security**

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services to drive new levels of performance, competitiveness, and customer experience across their IT estates. Learn more about how we deliver excellence for our customers and colleagues at **DXC.com**.