

CSC Secures App Access and Saves A\$200,000 Annually with the Zero Trust Exchange



Commonwealth Superannuation Corporation (CSC)

www.csc.gov.au

Location: Canberra, Australia

Industry: Federal & Government

Customer Size: Serving over 700,000 individuals

For over 100 years, the Commonwealth Superannuation Corporation (CSC) has provided financial advice, retirement planning, superannuation, retirement, finance, investment, and insurance services to Australian Government employees, employers, and Australian Defence Force members and their families.

Remote employees hindered by connectivity and security issues

Before the COVID-19 pandemic hit, Commonwealth Superannuation Corporation (CSC) was already struggling with providing appropriate remote access to ensure its employees could assist customers with fulfilling their retirement goals.

“At the time, we were relying on traditional VPNs [virtual private networks] and firewalls for secure access to our internal applications,” explained John Pratezina, Senior Network Operations Administrator. “Application performance was terrible, and the burdens on user devices constantly caused people to be knocked offline. We needed a modern solution for keeping remote workers connected and secure.”

Embracing zero trust as a foundation for SSE

As the CSC’s charter is delivering financially stable futures to over 700,000 government and military employees and their families, operating securely, effectively, and efficiently is integral to the agency’s mission.

With remote work an essential part of the CSC employment model and cloud adoption rapidly accelerating, the agency determined it was time to move away from data centers, VPNs, and Symantec Secure Web Gateways by adopting a zero trust architecture for building a security service edge (SSE) ecosystem.

CHALLENGE

Replace VPNs and firewalls with zero trust access for secure business transformation and exceptional application performance.

SOLUTION

- Zscaler Zero Trust Exchange™
- Zscaler Internet Access™ (ZIA™)
- Zscaler Private Access™ (ZPA™)
- Zscaler Digital Experience™ (ZDX™)
- Advanced Cloud Firewall
- Advanced Cloud Sandbox
- Cloud Access Security Broker (CASB)

OUTCOMES

- Realizes an ROI of over A\$200,000 annually
- Reduces infrastructure complexity by 90%
- Decreases overall management overhead by 30%
- Improves user experience by up to 70%
- Speeds help desk issue resolution by 30%
- Prevents an average of 7M policy violations monthly

For streamlined and secure access to replace its hardware-based approach, CSC investigated multiple solutions, including Cisco Umbrella and Netskope. Of the contenders, the agency selected the Zscaler Zero Trust Exchange for its comprehensive and integrated suite of solutions.

“Zscaler provided the foundation for a holistic SSE ecosystem that included solutions for users, devices, and workloads,” Pratezina said. “The Zero Trust Exchange went beyond a point-based solution approach for our immediate needs to meeting future requirements as we evolved. We wanted to move away from giving everyone, whether employees or contractors, broad access to our network.”

Simpler, faster, and more secure access

CSC’s Zero Trust Exchange deployment includes a range of Zscaler for Users services, which the agency implemented with the help of a local partner, A23.

The journey began with Zscaler Internet Access (ZIA) for fast, direct, and secure connectivity to the internet and SaaS applications regardless of location. The agency also implemented Zscaler Private Access (ZPA). It provides high-performance, VPN-free secure zero trust access to critical private business applications residing in CSC’s hybrid IT environment, including running on Amazon Web Services (AWS).

In addition, CSC deployed Zscaler Digital Experience (ZDX) to proactively detect and resolve issues before they impact user experiences.

Unified protection in the cloud: CASB, sandbox, and firewall

CSC also adopted multiple other services within the Zero Trust Exchange, such as Cloud Access Security Broker (CASB) for safeguarding data-at-rest by looking inside Software-as-a-Service (SaaS) applications and Infrastructure-as-a-Service (IaaS) offerings.

“When we started our zero trust journey, we lacked any CASB capabilities,” said Pratezina. “As we were becoming more cloud-centric, Zscaler provided us with superior CASB capabilities for protecting cloud applications and environments.”

CSC relies on Advanced Cloud Sandbox to stop patient-zero attacks using artificial intelligence (AI)-based analytics and quarantines, along with Advanced Cloud Firewall for security and access controls, without the cost, complexity, and performance limitations of next-generation firewalls, for all web and non-web traffic.

“We’ve improved user experiences up to 70% and reduced complexity over 90%. Overall, we’ve lowered management overhead 30% and are saving A\$200,000 annually with Zero Trust Exchange.”

– John Pratezina
Senior Network Operations
Administrator
CSC

“The Zscaler Advanced Cloud Firewall enabled us to standardize on one solution and decommission multiple separate appliances,” Pratezina said. “This reduced firewall infrastructure, management, and licensing complexity by over 90%. It was a real breath of fresh air.”

Nearly a 70% user experience improvement

Upon completing its Zero Trust Exchange deployment, CSC increased remote user productivity by enabling faster access to critical applications.

“We have one legacy business solution that our users log into multiple times a day,” he said. “With legacy VPN technology, remote users clicked on the application and then walked away from their computer for an average of 15 minutes while the VPN connected and the application loaded. What’s more, the VPN connection would frequently fail, requiring users to repeat the process.”

Today, CSC has cut load time for the application to less than five minutes, which improves user experiences by nearly 70%. This results in the agency gaining back an hour or more of productivity for every user, every day.

For business users, accessing applications directly without needing to go through the VPN gateway, firewalls, or network access control lists, speeds performance by eliminating bottlenecks. “We’ve seen a significant increase in application performance from the users’ perspective,” said Pratezina.

Accelerating retirement funds investing

With the Zero Trust Exchange, CSC investment managers gain considerable efficiencies so they can make time-sensitive trades faster and maximize retirement goals for each of their customers.

“In the past, it could take a week or two for a senior IT engineer to unblock a website that investment managers required,” said Pratezina. “This sometimes caused investment managers to access a blocked site with off-network devices, where there was no protection at all.”

“Today, with ZIA and its comprehensive controls and remediation capabilities, our investors can confidently use the websites they need to complete transactions, no matter where they are,” he added. “Further, we are able to proactively monitor their experiences in real-time using ZDX, and rapidly resolve any device, network or application issues that may affect their productivity.”

“We’re preventing an average of 7 million policy violations monthly, including types of violations our legacy solutions allowed through.”

– **John Pratezina**
Senior Network Operations
Administrator
CSC

ZDX empowers IT to eliminate bottlenecks for users

CSC is also reaping multiple benefits from ZDX, which provides rich analytics and insights for investigating and resolving issues faster.

"We now have a much easier way to work out where these blocks are, what's causing them, and where to start looking in order to resolve these problems," said Pratezina.

"By incorporating Zscaler Digital Experience into our ecosystem, we have empowered our service desk with better visibility over the way users are accessing applications," he observed. "We've easily had a 30% reduction in the time spent on service desk tickets."

Millions of policy violations and threats thwarted

As security is built into the core of the Zero Trust Exchange, all connections—regardless of user, endpoint application, or encryption—are inspected. This is enabling Pratezina and this team to tighten up security in numerous ways.

"We've come across malicious websites that our old proxies were not only allowing, but also had not flagged," remarked Pratezina. "Today, with Zscaler, we're preventing an average of 7 million policy violations per month."

Expansions advance a secure transformation

Looking ahead, CSC is excited about adding services, like Zscaler Deception for an extra layer of defense against ransomware, supply chain attacks, advanced persistent threats (APTs), and other sophisticated intruders.

The agency is also evaluating Zscaler for Workloads services for securing cloud workloads and reducing the progression of lateral threats. This includes Zscaler Workload Communications for secure internet access between applications, and Zscaler Workload Segmentation for further reducing attack surfaces through segmenting workloads, identifying risks, and applying identity-based protection.

"We feel that including these products in our current Zero Trust Exchange ecosystem will allow us to meet even more of our security requirements in a more unified and synergistic way," said Pratezina.

"The Zero Trust Exchange provides a holistic SSE ecosystem. It's been a real breath of fresh air."

– John Pratezina
Senior Network Operations
Administrator
CSC

Reducing overhead 30% while saving A\$200,000 annually

Since adopting the Zero Trust Exchange platform, CSC has seen a nearly 30% reduction in overall management overhead, freeing up the team to spend time on more strategic activities.

In addition, minimizing expenditures for on-premises appliances, and the license costs associated with them, is netting the agency an estimated return on investment of close to A\$200,000 annually.

Furthermore, with the collaboration of the Zscaler support team, deployment was seamless and helped CSC get the most from its solutions. “The biggest benefit of working with Zscaler has been its amazing support,” said Pratezina. “Our representatives are always quick to respond and have provided excellent suggestions to meet our needs.”

With its zero trust transformation well underway, CSC has already seen game-changing results that touch everyone involved with the organization—its business users, the IT team, and its customers. “The success we’re having with the Zero Trust Exchange demonstrates that partnering with Zscaler is a great choice,” Pratezina said.

“The success we’re having with the Zero Trust Exchange demonstrates that partnering with Zscaler is a great choice.”

– **John Pratezina**
Senior Network Operations
Administrator
CSC

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](https://www.zscaler.com) or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

