White Paper

# Delivering Unparalleled Security with Superior Economic Value

## The Power of the One True Zero Trust Platform

In today's world, people are working in and out of offices and connecting via videoconferencing, apps are moving to the cloud, and devices are everywhere. This hyper-distribution of resources creates a dangerously wide attack surface, and yesterday's perimeter-based security architectures are simply no match for today's advanced threats.

For the past three decades, organizations have been building complex, wide-area hub-and-spoke networks to connect their users to the data center. These networks were secured with an array of point security solutions, including firewalls and virtual private networks (VPNs), all positioned at the corporate network perimeter. This model, known as castle-and-moat security, worked well when most or all applications resided within the enterprise's data center, but it's not suitable for today's dynamic, distributed computing ecosystems. Extending corporate networks to enable cloud deployments and remote connectivity simply expands the attack surface and increases the difficulty and cost of securing data.

Data breaches and their corresponding costs continue to grow due to an overreliance on perimeter-based cybersecurity. In the U.S., the FBI's Internet Crime Complaint Center received an average of 2,300 reports of cybercriminal activity each day in 2021, the highest volume on record. On a global scale, cybercrime is estimated to have inflicted damages costing more than $6 trillion in 2021, and global losses due to cybercrime are forecasted to grow at least 15% year-over-year for each of the next five years. A study conducted by the Ponemon Institute on behalf of IBM projects that the global cost of data breaches could reach up to $10.5 trillion by 2025.

### Relying on perimeter-based security architectures exposes organizations to higher costs in four key areas:

- **Increased exposure to data breaches** that lead to possible ransoms, legal fees, noncompliance fines, time-consuming remediation efforts, and more
- **Capital expenditures and management overhead** from purchasing and operating wide-area, hub-and-spoke networks, as well as security point products such as firewalls and VPNs
- **Decreased productivity** due to poor user experiences that stem from inefficient VPNs and traffic being backhauled to the data center when connecting users to the cloud
- **Delays in realizing the benefits of mergers, acquisitions, and divestitures** due to the complexity of IT integration

Adopting a zero trust approach can mitigate the cybersecurity risks posed by the current threat landscape while improving user experiences and reducing cost and complexity. Zero trust security means consistent adherence to the principle of least-privilege access for all applications, workloads, users, and devices—at all times. Every transaction or connection is treated as though it may contain a threat, and every access request is dynamically evaluated before a connection is established to avoid exposing corporate assets to potential risk. For this reason, 94% of companies have identified zero trust as a strategic business initiative.

For any victim of a data breach, there is enormous financial harm. Corporate resources are wasted by the resulting operational disruption and downtime, incident response and recovery efforts, requirements to notify customers of the breach, legal fees and regulatory fines, and efforts to acquire new customers to make up for those who lost trust—not to mention the brand damage.

However, the costs associated with perimeter-based security architectures extend far beyond those that stem directly from breaches. Such architectures are inherently more complex than modern ones, demanding greater administrative effort and requiring larger investments in maintenance and infrastructure. They also erode employee productivity by creating poor user experiences. These challenges are amplified during periods of economic uncertainty, which places additional pressure on IT and security teams to find more modern ways to equip their organizations while reducing cost, complexity, and risk.

With the Zscaler Zero Trust Exchange™, companies can protect users, data, and apps, no matter where they're located, while ensuring superior user experiences and reduced administrative overhead—all with one integrated platform. Shifting away from traditional networks and security to the cloud native Zscaler platform not only improves agility and security but reduces cost and complexity, as well, delivering significant economic value to organizations.

In this paper, we'll look at these economic benefits in greater detail and demonstrate how the Zscaler Zero Trust Exchange helps organizations stop breaches, reduce complexity, improve user experience, streamline M&A integrations, and, ultimately, reduce costs.

## The rising cost of data breaches

Today's cyberattacks are more prevalent and sophisticated than they were even a few years ago. Threat actors have AI-driven tools to use and a network of cybercriminals to call upon, and they've become increasingly persistent as a result. Legacy castle-and-moat architectures can't deliver the necessary visibility or control to proactively defend against these modern threats. On the contrary, they expand the attack surface via firewalls and VPNs, enable compromise as passthrough architectures that lack the scalability needed to inspect encrypted traffic, and permit threats, once inside, to move laterally on the network to attack high-value assets.

For businesses, security lies at the heart of the economic value chain, and cyberattacks can lead to multiple forms of loss:

- **Revenue losses** stemming from brand damage and the resulting distrust of customers, partners, and suppliers
- **Direct costs** including ransoms paid to criminals, legal fees, recovery costs, and compliance penalties
- **Operational disruption** due to the organization-wide impact of downtime

**How Zscaler solves this problem**
With the Zero Trust Exchange, all users, workloads, and devices are secured using a cloud native architecture that eliminates the enterprise attack surface by making applications invisible from the public internet and, therefore, invisible to malicious parties.

Simultaneously, every connection is brokered individually to ensure that identity and context are verified before the appropriate level of access is granted; this eliminates "trusted" internal network zones that can be breached during a cyberattack. The Zero Trust Exchange is built on a scalable, proxy-based architecture that inspects all content (including TLS/SSL-encrypted content) in real time, detecting and stopping threats and data loss that firewalls and other passthrough solutions miss. It also scans your clouds for sensitive data and threats at rest, risky or unauthorized sharing, and misconfigurations that could lead to breaches or data leakage.

Our zero trust model also eliminates the possibility of lateral threat movement. App access is extended only to users and workloads that need it (as defined by business policies) and access to the network as a whole is prevented, leaving bad actors with nowhere to go even if they should reach the corporate network.

## Customer success highlights

**Baker & Baker**
A leader in the European convenience bakery segment, Baker & Baker operates across seven countries and produces 2,500 bakery products. Confronted by a multitude of ransomware attacks, the company decided to replace its legacy MPLS architecture with Zscaler and a modern software-defined wide-area network (SD-WAN). As a result, the company was able to:

- Improve overall security by 90% while reducing troubleshooting time from months to seconds
- Prevent 4 million policy violations and block 14,000 threats monthly
- Retire VPNs, save 70% on costs, and boost application performance

**Mobility ADO**
Mobility ADO is a global transportation provider based in Mexico City operating in eight countries across three continents. As the company and its user base grew, it needed to deliver fast, highly secure access to the internet to its employees as well as increase its cloud application portfolio. Mobility ADO replaced its legacy network architecture with the Zscaler Zero Trust Exchange, making it possible to:

- Block 42,509 novel threats within a three-month period
- Prevent 25.4 million policy violations during that same period
- Reduce management overhead and save time

Additionally, the Zero Trust Exchange provides advanced threat protection powered by artificial intelligence (AI) and machine learning (ML) that automatically adapts and enforces dynamic, risk-based security and access policies, which greatly decreases the risk of a successful cyberattack. Leveraging AI and ML also allows you to automate menial, manual tasks while surfacing high-fidelity alerts, saving your team hours of work per week and reducing the need for dedicated resources.

In a recent study, ESG found that organizations that transition from traditional perimeter- and appliance-based security to the Zero Trust Exchange experience a 65% reduction in virus and malware infections, an 85% reduction in successful ransomware attacks, and a 27% decrease in the likelihood of a data breach.

## The cost and complexity of perimeter-based security

Not only are castle-and-moat security architectures more vulnerable to breaches than those built according to a modern zero trust model, they're also more complex. With hub-and-spoke networks growing more complicated due to cloud app and remote work adoption, it's become more difficult, time-consuming, and expensive to enforce consistent policies with disjointed point products.

Perimeter-based security architectures also drive significant increases in hardware costs. Namely, the more locations and users you have, the more physical security appliances you'll need to protect them all (which also leads to greater power consumption). This demands high upfront capital expenditures (CapEx), and forces CIOs to conduct extensive, ongoing capacity planning and predict their future requirements with pinpoint accuracy. Underestimation can lead to poor performance, and overestimation to unused capacity and elevated, unnecessary costs.

When security appliances are located at the network perimeter, installing, configuring, provisioning, testing, troubleshooting, and managing them is costly and time-consuming irrespective of whether they're physical or virtual. This demands intensive labor from highly skilled people who are experienced in getting disparate solutions to work together.

Additionally, MPLS networks are expensive to maintain, and bandwidth costs are high. Backhauling traffic to your data center in order to connect to software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), or platform-as-a-service (PaaS) applications running in the public cloud will consume a great deal more bandwidth than connecting to them directly. Solutions like VDI and private network link services like ExpressRoute for Azure and Direct Connect for AWS add layers of additional expense to an already costly infrastructure.

**How Zscaler solves this problem**
With the Zero Trust Exchange, it's easy to enforce consistent policies across hybrid ecosystems. Our platform delivers fast, secure, direct-to-cloud access, eliminating the need for costly MPLS networks with complex routing, switching, and network segmentation requirements.

The Zero Trust Exchange is built in the cloud, meaning there are no underlying appliances to manage and you can leverage the internet as your corporate network, removing the expense of point-to-point network hardware. Security and connectivity are delivered together as a service, with Zscaler applying patches and updates on your behalf. Shifting from an upfront CapEx model to an ongoing operational expenditure (OpEx) one means that your costs will be much more predictable. Simple, subscription-based pricing makes it easy to right-size your security and connectivity budget, even as your organization grows.

As a holistic platform that connects and secures all apps, users, and devices, the Zero Trust Exchange eliminates the need to integrate, maintain, and monitor a lineup of point products and their associated consoles, alerts, and policies—bringing operational costs down.

It's no longer necessary to duplicate policies across different dashboards or recreate them for multiple products with disparate capabilities, making it possible for highly skilled IT professionals to spend their time on strategic initiatives rather than day-to-day tasks associated with maintaining uptime.

A recent economic value study showed that the Zero Trust Exchange can reduce hardware costs by as much as 90%. In addition, using the single, cloud-delivered platform (instead of multiple point products) can free up security employees' time by as much as 74%.

## Customer success highlights

**The Commonwealth Superannuation Corporation (CSC)**
The Commonwealth Superannuation Corporation (CSC) provides financial and retirement planning services to the Australian Defense Force, government members, and their families. Its firewall- and VPN-based security architecture couldn't keep pace with cloud adoption or provide fast, reliable application connectivity to remote workers. CSC selected Zscaler for zero trust and achieved multiple benefits:

- A 90% reduction in infrastructure complexity
- A 30% decrease in overall management overhead
- A 70% improvement in application load time with a more stable connection than VPN, enhancing user experience and productivity

**L&T Finance Holdings**
L&T Finance Holdings is a leading non-banking financial services company with more than 195 branches and 24,000 employees. As part of its transformation from a paper-based company to a digital enterprise, it adopted the Zscaler Zero Trust Exchange as a comprehensive, cloud-based, zero trust solution. Zscaler enabled the company to streamline and achieve multiple benefits:

- Eliminate approximately 110 resource-intensive threat management and security appliances
- Realize significant savings on hardware, software, and maintenance
- Achieve nearly a 40% improvement in endpoint security while reducing access-related support tickets to almost zero

## Loss of productivity and collaboration due to poor user experience

Securing legacy hub-and-spoke networks often requires VPNs for backhauling remote users' traffic to a central data center, where it flows through the organization's security stack. Sending traffic from these users to the corporate data center and then out to the cloud—and following that path again in reverse—adds significant latency. Additionally, VPNs are frustrating from an end user perspective, as they cause timeouts and require constant reauthentication. Naturally, this degrades the user's experience and throttles their productivity and ability to collaborate. Even when they're hosted in the cloud, tools like virtual firewalls don't improve the situation, as all network traffic still has to flow through a centralized choke point. The only difference is that the choke point is now located in the cloud.

This problem is compounded by the fact that today's employees are highly dependent upon collaboration tools like video conferencing software that have high bandwidth and network performance requirements. Backhauling traffic creates performance issues and network outages that are much more damaging when people need Zoom or Microsoft Teams to get their jobs done.

The rapid shift to hybrid and remote work has also created new challenges for IT teams, who have struggled to maintain visibility across increasingly complex networks and infrastructure. As applications move from the data center to the cloud and are accessed by an "anytime, anywhere" workforce, IT teams can no longer control the underlying technology stack or maintain end-to-end visibility over the user experience. This means that performance issues that arise from SaaS or cloud application availability, network path outages, or network congestion are not easily isolated and diagnosed. To make matters worse, traditional monitoring and fault detection solutions optimized for use in data centers or on endpoints will leave visibility gaps.

Left with only disjointed tools that don't provide a full picture, IT teams have to rely on complex combinations of multiple dashboards with disparate logs, making it nearly impossible to diagnose and fix the root cause of performance issues—particularly for remote users.

**How Zscaler solves this problem**

Unlike legacy approaches, the Zero Trust Exchange allows for direct-to-app connectivity that eliminates the need to backhaul traffic to the data center and greatly reduces latency, improving application performance and the user experience overall. Additionally, intelligent traffic routing ensures the shortest path of communication between users and apps, no matter where they're hosted or located.

The Zero Trust Exchange is delivered at the edge, employs multiple services simultaneously, and scans all content in a single pass without copying packets. This is fundamentally different from the chained model employed with physical or virtual appliances, whereby each security tool independently processes packets, incrementally adding more latency at each hop.

The Zero Trust Exchange also provides end-to-end visibility via integrated digital experience monitoring, enabling proactive detection and troubleshooting from a single dashboard with comprehensive logging, which is just as effective for diagnosing issues for remote workers on hotel or home Wi-Fi as it is for employees in the office. This speeds incident resolution time for IT and lowers the costs associated with application downtime and poor user productivity.

## Customer success highlights

**Ciena**
A networking systems, services, and software company delivering best-in-class technology within high-touch consultative relationships, Ciena needed to advance its digital transformation to turn IT into a competitive advantage for the business. In particular, it needed to enhance digital experiences for greater user productivity, while finding ways to cut costs. By deploying the Zscaler Zero Trust Exchange, Ciena was able to:

- Quickly resolve 95% of user experience issues, up from 25% prior to Zero Trust Exchange adoption
- Reduce application latency by 20%
- Cut MPLS costs and help desk tickets by 50%

**Falkirk Council**
A local government authority in Scotland providing comprehensive services for approximately 160,000 residents, the Falkirk Council found itself needing to fast-track its cloud and digital transformation in order to continue meeting residents' needs during the COVID-19 pandemic. The Falkirk Council turned to the Zero Trust Exchange to create a holistic zero trust environment with work-from-anywhere (WFA) application access. The organization was able to:

- Provide users with stable, reliable, high-quality videoconferencing and other collaboration tools
- Establish VPN-free, zero trust, WFA access to internal apps and the internet to significantly boost productivity
- Reduce infrastructure and cybersecurity costs by 50%

## Increased time-to-value of mergers, acquisitions, and divestitures

Mergers and acquisitions (M&As) and divestitures have traditionally been a major source of stress and disruption for IT teams. Such business changes seek to create value by opening new opportunities to drive growth, enhance margins, increase agility, and improve performance. But to accelerate time-to-value, companies have to merge IT systems quickly and effectively.

It's common for merging entities to rely on different networks, architectures, and systems. As such, achieving full integration can be extraordinarily complex and, thanks to unanticipated scope creep, more expensive than initial assessments. This often extends integration timelines, leaving employees with disparate, siloed systems that don't always lend themselves well to cross-organizational communication and collaboration. Teams attempting to integrate legacy networks and security architectures often resort to "creative" ways to get users access to resources on disparate networks—sometimes poking holes in firewalls, using unsanctioned file sharing sites, or disabling secure access protocols. These makeshift solutions increase risk, create user productivity issues, and make troubleshooting more difficult—all of which waste resources. Ultimately, delays in integration hamper the achievement of the financial business case that was behind the acquisition in the first place.

Solutions that make for quick, simple, secure integration can dramatically decrease time-to-value within the combined organization.

**How Zscaler solves this problem**
The Zero Trust Exchange significantly accelerates time-to-value during mergers and acquisitions by streamlining the integration of disparate IT systems. In fact, by establishing direct connectivity, wherein users connect to applications rather than to a corporate network, IT may never need to complete a full network integration between the two entities. Once a user is added to a policy and application authorization is granted, that user can be given secure access to any application via the Zero Trust Exchange in either organization's domain—without requiring network access or integration. Instead, the internet is used as a connectivity backbone for all corporate assets, minimizing the complexity and security risks associated with integrating separate network infrastructures and their respective access policies.

With the Zero Trust Exchange, both entities involved in a merger, acquisition, or divestiture will benefit from the reduction in security risk that our platform delivers. With no internet-visible attack surface and no means for attackers to move laterally across their environments, organizations can expect better security outcomes. Both entities will also benefit from consistent, seamless user experiences made possible by the Zero Trust Exchange, including low-latency connectivity to popular SaaS and cloud providers.

## Customer success highlights

### West Fraser

West Fraser is one of the world's largest diversified wood product companies and North America's largest lumber producer. In recent years, the company has grown significantly through acquisition, creating a need to provide new internal users with rapid secure access to resources and cloud apps. With the Zscaler Zero Trust Exchange, the company was able to:

- Grant new M&A employees access to apps in hours instead of weeks
- Filter approximately 3.5 billion events, prevent more than 745,200 policy violations, and block over 37,000 threats—all within one year
- Deploy zero trust work-from-anywhere access globally within weeks

### Careem

An innovative transportation services company headquartered in Dubai, Careem pioneered the ride-hailing economy in the Middle East. With the goal of replacing its legacy security architecture to power high-velocity growth, Careem chose the Zero Trust Exchange platform. This enabled the organization to:

- Enable M&A activities and reduce geopolitical and compliance complexities
- Reclaim 20,000 engineering hours annually and lower costs approximately 55%
- Improve user experience issue resolution time by 62%

## The Zscaler Zero Trust Exchange: The One True Zero Trust Platform

The Zero Trust Exchange has a highly scalable, cloud native proxy architecture that improves security by eliminating the attack surface, stopping compromise, and preventing lateral threat movement. It enables organizations to cut costs by allowing them to retire VPNs, costly MPLS, and bespoke networking and security architectures. At the same time, it increases efficiency for IT operations and end users who need fast, reliable application access to get their jobs done. For M&As and divestitures, it increases business agility by accelerating time-to-value.

The Zero Trust Exchange makes it possible to realize a true zero trust security architecture with a single, cost-effective platform—one that's quick to implement and easy to manage. It eliminates the cost and complexity associated with perimeter-based security, enabling organizations to stay secure, agile, and competitive, even during periods of economic uncertainty.

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. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.