zscaler™

WHITE PAPER

Comparing the Business Value of Zscaler's Workload Communications against Cloud and Virtual Firewalls

Executive Summary

Modern digital businesses are powered by an ever-expanding array of workloads running in various environments ranging from on-premises data centers to public and private cloud infrastructures. The business's profitability, operational continuity, and ability to deliver high-quality customer experiences all depend upon the availability and security of these mission-critical workloads. Securing them against cyberattacks (including ransomware), lateral threat movement, and data loss is imperative.

However, many organizations still rely on legacy solution architectures to protect business-critical workloads. Typically, this entails implementing multiple third-party solutions, such as firewalls, secure sockets layer (SSL) and transport layer security (TLS) inspection engines, and data loss prevention (DLP) tools, for multiple layers of protection. To achieve consistent inspection and policy enforcement across all egress traffic, many organizations are still backhauling their public cloud workload traffic to an on-premises data center. By doing so, they make their architectures more complex, add costs, and impede performance. Poor performance, of course, means that end users and customers have less-than-ideal experiences.

Other enterprises now rely on the native security capabilities that public cloud vendors offer. This approach typically adds to the staffing burden of staffing. Plus, implementing a purpose-built security infrastructure for each individual cloud service provider (CSP) is cost prohibitive.

Cloud-native, legacy-based, and multi-vendor strategies all have sharp limitations. They offer inconsistent threat and data protection, with high complexity and operational costs. With these approaches, it's near impossible to prevent lateral movement, let alone block it early in the attack lifecycle.

There's a better way: by implementing a modern zero trust architecture, enterprises can radically simplify hybrid workload security while achieving consistent, comprehensive threat and data protection. The Zscaler Zero Trust Exchange, the world's largest inline cloud security platform, delivers comprehensive zero trust protection for all workload-to-workload and workload-to-internet communications.

The Zscaler platform inspects all traffic inline to block cyberthreats and data loss. It's able to establish the identity and context of all access requests before granting access, and to apply all appropriate policies before allowing connectivity to the internet, SaaS apps, or workloads in public or private clouds. Cloud-scale TLS inspection makes it possible to prevent zero-day attacks, while inline data protection and DNS inspection stop data leaks. Strict controls stop workloads and servers from communicating with known-risky and unknown destinations.

Zscaler's approach also makes enterprise resources undiscoverable, eliminating the attack surface, and effectively preventing lateral movement. At the same time, it makes it simpler to apply least-privilege access, since workloads can easily be segmented by IP, domain name, virtual private cloud (VPC), VNet, or user-defined tags.

With the Zscaler Zero Trust Exchange, it's possible to take an all-in-one approach, replacing costly combinations of point products with a single, comprehensive cloud platform. Not only does this reduce operational overhead, but it also limits real-world ransomware and data breach risks. This increases the productivity of IT and security teams while safeguarding the business against far-reaching damage from today's most prevalent threats.

In this white paper, we'll examine the costs and benefits associated with deploying Zscaler Workload Communications. We will focus in particular on:

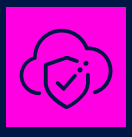
- **Ransomware risks.** How ready is your organization to face this significant risk? With the average global ransom payment having increased 500% over the past year,[1] what steps are you taking to reduce your potential cost burden? How effectively can you prevent attackers from moving laterally across your environment to spread damaging malware?
- **Data breach risks.** Can your organization stop threat actors before they exfiltrate valuable intellectual property, customer records, or financial data? By how much can an effective solution enable you to buy down real-world cyber risks?
- **Tool and implementation costs.** Which vendor-provided solutions are most expensive? Which deliver the most risk-reduction per dollar spent on them?
- **Operational expenditures.** How many hours per year are your organization's IT and security teams currently devoting to the management of complex, unwieldy tooling? How much time are they spending configuring and updating firewall rules or troubleshooting virtual private network (VPN) issues?

Summary of Benefits of Zscaler Workload Communications[2]

Total Cost Savings

$2.3M
saved per year

30%
decrease in cost



Cyber Risk Reduction

50%
decrease in ransomware risk

40%
reduction in data breach risk

Operations Improved

$1.6M
saved on annual labor costs

65%
decrease in operational expenditures

[1] Source: Sophos State of Ransomware 2024 Report, April 2024.
[2] For an organization running approximately 10,000 cloud workloads, as compared to operating a third-party firewall equivalent to the Palo Alto Networks virtual firewall.

Cyber Risk's Impact on the Business: Understanding the Costs

It may be illicit, but cybercrime is among the world's most profitable activities. The National Institute of Standards and Technologies (NIST) estimates that cyberattacks cost U.S. businesses as much as four percent of the nation's GDP annually.[3] Described as "the greatest transfer of economic wealth in history," these losses are estimated to have totaled $8.15 trillion on a global basis in 2023, and are predicted to exceed $13 trillion per year by 2028.[4] If cybercrime were a country, it would have the world's third-largest economy (after the U.S. and China).[5]

Given the enormous size of these numbers, it's no surprise that the direct costs to individual victims are huge. According to IBM Security, the average cost of a data breach in the U.S. reached an all-time high of $4.45 million in 2023, marking a 2.3% increase over the past year, and a 15.3% increase since 2020. Ransomware attacks made up approximately one quarter (24%) of these breaches, and cost their victims an average of $5.13 million each.[6]

These giant figures still don't capture the full extent of the damages that victims of cybercrime suffer. Soft costs such as damage to brand reputation or loss of employee confidence are difficult to quantify, as are downstream effects such as needing to shift business strategy or adjust the enterprise's operating model.

Like all business risks, those associated with cybercrime are impossible to avoid entirely. However, it is possible to mitigate them effectively. As in any other type of risk management, stakeholders can buy down cybersecurity risks by implementing protective measures that demonstrably reduce the chances that an attack will succeed.

To calculate the value you'd gain from mitigating cyber risks, you'll need to model the financial losses that a successful cyberattack would cause, as well as its probability. Then you can determine how to balance those risks against what you'd need to spend to reduce them.

Let's take a closer look at what these calculations look like.

Ransomware Risks

Ransomware risks differ across industries and geographies, with some verticals (such as manufacturing, healthcare, and retail/e-commerce) experiencing significantly higher incident and breach rates than average.[7] Some risk factors counterbalance each other. On the one hand, organizations with very mature cybersecurity programs will experience fewer successful ransomware attacks than those that have implemented fewer protective measures. On the other, larger companies—brands that are household names—are targeted far more often.

Many ransomware attacks succeed by targeting vulnerabilities in infrastructure like virtual private networks (VPNs) and then moving laterally to find crown jewels. Recent threat research shows that as many as 56% of organizations have been targeted in cyberattacks exploiting VPN security vulnerabilities over the past year.[8]

[3] Source: NIST, Update: "Evidence suggests that the U.S. loses hundreds of billions to cybercrime, possibly as much as 1% to 4% of GDP annually," May 2020.
[4] Source: Statista, Estimated Cost of Cybercrime Worldwide 2018–2029, June 2024.
[5] Source: International Monetary Fund, World Economic Outlook, April 2024.
[6] Source: IBM Security, Cost of a Data Breach Report 2023.
[7] Source: Verizon, 2024 Verizon Data Breach Investigations Report.
[8] Source: Zscaler, 2024 VPN Risk Report.

Firewall Vulnerabilities Create Major Risks

These are some examples of Common Vulnerabilities and Exposures (CVEs) recently disclosed by vendors of widely used firewalls.

- **Palo Alto Networks (CVE-2023-6790):** This cross-site scripting (XSS) vulnerability in the Palo Alto Networks operating system (PAN-OS) enables a remote attacker to execute a JavaScript payload as if they're logged into a browser with administrative privileges.
- **Palo Alto Networks (CVE-2024-3400):** Unauthenticated users can exploit this vulnerability within PAN-OS to infiltrate the networks that its solutions are supposed to be protecting. Threat researchers have observed a large number of exploits targeting this vulnerability,[9] which received the maximum CVE severity score of 10.
- **Ivanti (CVE-2023-46805 and CVE-2024-21887):** By exploiting this vulnerability, remote attackers have been able to perform authentication bypass and remote command injection attacks. The severity of these vulnerabilities led the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to immediately sever connections with devices connected through affected VPNs.
- **Fortinet (CVE-2024-2172 and CVE-2024-23323):** These critical vulnerabilities in FortiOS, the operating system running on all Fortinet firewalls, allow threat actors to execute code remotely on affected systems. When Fortinet released a security update addressing these vulnerabilities, it reported that they were likely being exploited in the wild.[10]
- **Check Point (CVE-2024-24919):** This vulnerability in Check Point Security Gateway software makes it possible for threat actors to access information passing through Check Point Security Gateways when remote access VPNs or Mobile Access Software is enabled.

We assume, in accordance with data published in the most recent IBM Cost of a Data Breach Report, that the average successful ransomware attack in a hybrid or multi-cloud environment will cost its victim $5.11 million.[11] Smaller organizations running fewer cloud workloads can be expected to experience lower costs than this cross-industry average.

Based on this assumption, an organization with a 15% chance of being victimized by ransomware each year will incur, on average, $1,022,000 worth of ransomware-related expenses annually. (In reality, these expenses will not be encountered every year, but instead the organization will have to pay $5.11 million every five years (on average) in a large lump sum when a major attack is successful.)

[9] Source: Palo Alto Networks, Announcement, "More on the PAN-OS CVE-2024-3400," April 2024.
[10] Source: CISA, Cybersecurity Advisory, "Fortinet Releases Security Advisories for FortiOS," February 2024.
[11] Source: IBM Security, Cost of a Data Breach Report 2023.

By the same logic, an organization with a 20% chance of falling victim to a ransomware attack will incur an average of $2,555,000 in ransomware-related expenses annually, while one with a 25% chance of being victimized annually will incur $5,110,000 in average expenses. Based on our threat researchers' observations, larger organizations not only have a higher risk of encountering ransomware, but these incidents come with higher costs, since a larger computing infrastructure is involved.[12]

Organizations operating a major security vendor's firewall solution, firewall capabilities delivered as-a-Service or a public cloud vendor's native firewall can expect that some ransomware attacks will eventually succeed, since none of these solutions is capable of blocking 100% of lateral threat movement.

By contrast, an enterprise that adopts a zero trust approach in its architecture design will, by definition, be able to block all lateral threat movement.

In actuality, real-world customers who have implemented the Zscaler Zero Trust Exchange to secure their workload communications see, on average, a 40% reduction in ransomware risk across the board, though larger organizations with more complex IT environments will experience an even greater reduction in ransomware risk.

This translates to the following risk-associated annual costs for enterprises with 15, 20, and 25% chances of encountering ransomware annually—these are smaller, medium-sized, and larger enterprises, respectively.[13] The costs are identical for each of these types of security solutions, since none can block all lateral movement.

SECURITY POSTURE – RANSOMWARE			
	Small	**Medium**	**Large**
Annual Risk of Experiencing a VPN-Related Ransomware Attack	15%	20%	25%
Average Cost of a Ransomware Attack	$1,022,000	$2,555,000	$5,110,000
% Reduction in Risk of Ransomware with Zscaler	40%	50%	60%
Reduction in Annual Ransomware Risk Cost with Zscaler	**$61,320**	**$255,500**	**$766,500**

[12] Source: Zscaler, 2024 VPN Risk Report.

[13] Throughout this analysis, we group enterprises into three categories, corresponding to the size and/or maturity of their cloud environment. Those in the "small" group are running approximately 1,000 workloads in the cloud, storing 5TB of data each month, and operating across 5 regions. Enterprises in the "medium" group are running 10,000 cloud workloads, storing 30TB of data per month, and operating across 25 regions. Those in the "large" group are running 20,000 workloads, storing 100TB of data per month, and operating across 50 regions.

Data Breach Risks

Based on data gathered by the Cyentia Institute, the average enterprise across industries has a 14% chance of suffering a data breach each year.[14] Expenses associated with these events include investigation costs, costs associated with business disruption, including lost revenues and customers, as well as costs associated with network repair and recovery, forensics, notifications, and regulatory fines and penalties.

No firewall or cloud vendor's native data protection solution is foolproof. Within the past year, we've seen CVEs impact several prominent cybersecurity vendors' firewall solutions, including the previously-mentioned CVE-2024-3400, which has been exploited in a number of zero day attacks documented by threat researchers.[15] Cisco also recently disclosed critical vulnerabilities impacting its firewall solutions, including CVE-2024-20553 and CVE-2024-20358 (affecting the Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) software).[16] Back in 2022, a major vulnerability in Fortinet's FortiOS software allowed attackers to bypass authentication mechanisms and gain access to networks that were supposedly protected by Fortinet firewalls.[17]

A small organization operating third-party firewall solutions, -aaS solutions, and cloud vendors' native capabilities can expect to see $798,000, $950,000, and $914,000 in annual data breach costs, respectively. These cost differences are due to the fact that different types of firewalls are typically deployed in different environments. For instance, the use of an on-premises firewall usually indicates that significant amounts of data are stored on-premises, whereas the use of a public cloud vendor's native solution usually signals that most data is stored in the public cloud, where average breach costs are higher.[18]

Those adopting a zero trust-based approach like the Zscaler Zero Trust Exchange will experience, on average, a 40% reduction in these risks.

SECURITY POSTURE – DATA BREACH			
	Small	**Medium**	**Large**
% Risk of data breach (over 12 months)	14%	14%	14%
Average Cost of a Data Breach: Third-Party Firewall	$798,000	$1,995,000	$3,990,000
Average Cost of a Data Breach: Third-Party Cloud Firewall	$950,000	$2,375,000	$4,750,000
Average Cost of a Data Breach: Public Cloud Native Firewall	$914,000	$2,285,000	$4,570,000
% Reduction in Data Breach Risk with Zscaler	40%	40%	40%
Decrease in Annual Data Cost Associated with Data Breach Risks: Zscaler vs. 3rd Party Firewall	**$44,688**	**$111,720**	**$223,440**
Decrease in Annual Cost Associated with Data Breach Risks: Zscaler vs. aaS Solution	**$53,200**	**$133,000**	**$266,000**
Decrease in Annual Cost Associated with Data Breach Risks: Zscaler vs. Cloud-Native Firewall	**$51,184**	**$127,960**	**$255,920**

[14] Source: Cyentia Institute, Information Risk Insights Study, 2022.
[15] Source: Cybersecurity Dive, "Palo Alto Networks fixes maximum security, exploited CVE in firewalls," April 2024.
[16] Source: National Cyber Security Centre, UK, "Exploitation of vulnerabilities affecting Cisco firewall platforms," April 2024.
[17] Source: Avertium, "Flash Notice: Critical Fortinet Zero-Day Vulnerability Exploited in the Wild," December 2022.
[18] Source: IBM Security, Cost of a Data Breach Report 2023.

Deployment and Operational Expenditures

Powered by the Zscaler Zero Trust Exchange, Zscaler Workload Communications radically simplifies hybrid workload security. Because this approach is simpler, it's easier and less expensive to implement and maintain.

Designed to protect workload–to–internet and workload–to–workload egress traffic across public cloud and on–premises data center workloads, the solution ensures that there's consistent threat and data protection everywhere. Zscaler Workload Communications makes it easy to standardize security policies for users and applications across diverse technology environments. And it leverages extensive automation, including infrastructure as code (IaC) templates, to simplify deployment.

Streamlining Connectivity, Cutting Costs

For nearly all enterprises, there are a significant number of expenses that can be greatly reduced or entirely eliminated by switching to an inline cloud security platform like the Zero Trust Exchange. These include costs associated with:

- **Cloud/virtual firewalls:** Subscription costs are per user, per year. To secure their cloud workloads, organizations deploy virtual firewalls such as the PAN Virtual Firewall, the PAN Cloud Firewall, the AWS Network Firewall, the Microsoft Azure Firewall, or one of many others. This approach is scalable, supporting bursts of increased traffic (including seasonal increases) with no need to deploy additional physical appliances. It also eliminates the need for centralized firewall management tooling

  Zscaler customers have no need to deploy dedicated firewalls to protect their cloud workloads, eliminating this expense.

- **Backhauling traffic:** Many enterprises still backhaul traffic from the public cloud to their corporate data center in order to inspect and secure workload egress traffic. Achieving this typically requires the creation of a dedicated network between AWS, Azure, and/or GCP and the organization's data center. This requires building DX/ExpressRoutes, as well as investing in the on–premises hardware and infrastructure required to secure cloud egress traffic.

  Zscaler customers no longer need to route traffic back to their data centers for inspection, so they bear none of the associated costs.

- **Multi–cloud support:** Most enterprises work with multiple cloud service providers (CSPs) such as AWS, Microsoft Azure and GCP. Because these environments are different, security teams typically implement CSP–specific security tools, develop CSP–specific skills, and replicate their security policies, one by one, across each cloud. It also takes time and resources to establish overlapping IP addresses across multiple clouds.

  Zscaler customers can leverage a single cloud–delivered security platform to protect workloads running on multiple clouds, eliminating the need for CSP–specific tools and resources.

- **VPN connections:** To enable secure connectivity between workloads across VPCs, regions, and public clouds, enterprises often install VPN connections.

  Zscaler eliminates the need for—and all expenses associated with—VPN connections.

- **TLS inspection:** Enterprises often deploy specialized inspection tools like Squid or Blue Coat proxies or cloud firewalls. Not only can these appliances be expensive, but they can have a negative impact on performance by increasing latency and reducing throughput.

  Zscaler includes TLS inspection capabilities, so there's no need to pay for additional appliances or solutions. Most importantly, performance does not suffer when you turn on inspection.

- **Data protection:** Deploying DLP tools or services is a common strategy for protecting sensitive data as mission-critical applications move to the cloud.

  Zscaler includes built-in DLP capabilities that can safeguard workloads in the public cloud or elsewhere.

In the rest of this white paper, we'll take a closer look at how Zscaler's simpler approach impacts technology costs and operational expenditures. Adding these cost savings together with those associated with cyber risk reduction will allow us to calculate the overall financial value of Zscaler Workload Communications.

Cost Optimization: Software and Appliances

The Zscaler Zero Trust Exchange offers a new, modern approach to workload security that eliminates the attack surface, provides for full inline content inspection and DLP, and enables direct connectivity to make lateral threat movement impossible. Because all of this is achieved with an inline cloud platform, there's no need for costly appliances, software licenses, or MPLS connections.

Depending on the size of your enterprise, this can eliminate annual expenditures of up to $3 million or more.[19] Some of the tools, solutions, and subscriptions you may be able to remove:

- MPLS circuits (you may also eliminate expenses associated with network termination)
- Cloud-native firewalls (from providers like AWS, Microsoft Azure, and GCP)
- as-a-Service firewall subscription costs (including features such as SSL inspection)
- Traditional firewall costs
- Network address translation (NAT) gateways
- Data protection/data loss prevention (DLP) solutions
- Cloud-native virtual private network (VPN) solutions
- TLS inspection solutions

[19] Costs calculated from multiple sources, including: CarrierBid Communications, MPLS vs. internet price comparison tool, 2024; Amazon Web Services, AWS pricing calculator; Microsoft Azure Marketplace; Google Cloud, Cloud Next Generation Firewall pricing; and Palo Alto Networks, Cloud NGFW Pricing Estimator.

Cost Optimization: Operational Expenses and Labor

The skills gap in cybersecurity remains a pressing issue across verticals and geographies, with an estimated four million workers needed around the world to fill open positions in information security.[20] Practitioners with experience working in AWS, Azure, and GCP environments are in especially short supply. Hence, we estimate that labor costs are approximately $200 per hour for these professionals. We estimate that a smaller organization would require three full-time employees, a midsized one six, and a larger organization eight.

On average, Zscaler enables a 60–65% reduction in labor hours needed for operational support, compared to all the cloud software solutions described above.

OPERATIONAL SUPPORT (LABOR)			
	Small	**Medium**	**Large**
Assumed Resources	3	6	8
Assumed Hourly Rate	$200	$200	$200
Assumed Annual Hours	2,080	2,080	2,080
Total Annual Labor Cost	$1,248,000	$2,496,000	$3,328,000
Reduction with Zscaler	60%	65%	65%
Cost Savings with Zscaler	**$748,800**	**$1,622,400**	**$2,163,200**

[20] Source: World Economic Forum, Strategic Cybersecurity Talent Framework, April 2024.

Putting It All Together: The Business Value of the Zscaler Zero Trust Exchange for Securing Workload Communications

Let's take a more in-depth look at how these savings add up in real-world customer environments. We'll start with a third-party virtual firewall, comparing the three organization sizes we've been considering throughout this analysis, small, medium, and large.

ORGANIZATION SIZE ASSUMPTIONS:		
	Approximate number of cloud workloads	Deployment size
Small	1,000	Across 2 CSPs
Medium	10,000	Across 3 CSPs and few Availability Zones
Large	20,000	Across 3 CSPs and multiple Availability Zones

THIRD-PARTY FIREWALL[21]			
	Small	Medium	Large
Third-party firewall annual licensing and appliance cost	$209,394	$1,046,970	$2,093,940
Operational cost	$1,248,000	$2,496,000	$3,328,000
Cost of Ransomware	$1,022,000	$2,555,000	$5,110,000
Cost of Data Breach	$798,000	$1,995,000	$3,990,000
Total annual cost of 3rd party firewall (PAN virtual firewall)	**$3,277,394**	**$8,092,970**	**$14,521,940**
Cost savings with Zscaler	**$944,202**	**$2,316,590**	**$2,847,080**
Decrease	**28.8%**	**28.6%**	**19.6%**

THIRD-PARTY -AAS FIREWALL[22]			
	Small	Medium	Large
Annual cost for 3rd party aaS	$159,492	$832,464	$1,676,820
Operational cost	0	0	0
Cost of Ransomware	$1,022,000	$2,555,000	$5,110,000
Cost of Data Breach	$950,000	$2,375,000	$4,750,000
Total annual cost of 3rd party firewall (PAN aaS firewall)[23]	**$2,131,492**	**$5,762,464**	**$11,536,820**
Cost savings with Zscaler	**$154,012**	**$500,964**	**$309,320**
Decrease	**7.2%**	**8.7%**	**2.7%**

[21] Palo Alto Networks Virtual Firewall used as example here.
[22] Palo Alto Networks Cloud Firewall used as example here.
[23] This includes licensing costs for the Palo Alto Networks aaS Firewall (including SSL), NAT Gateway and Cloud-Native VPN Connectivity.

PUBLIC CLOUD PROVIDER NATIVE FIREWALL[24]			
	Small	**Medium**	**Large**
Cost for Native firewall (AWS)	$163,434	$758,964	$1,840,080
Operational cost	0	0	0
Cost of Ransomware	$1,022,000	$2,555,000	$5,110,000
Cost of Data Breach	$914,000	$2,285,000	$4,570,000
Annual cost for Native firewall (AWS)[25]	**$2,099,434**	**$5,598,964**	**$11,520,080**
Cost savings with Zscaler	**$257,434**	**$422,424**	**$462,500**
Decrease	**11.7%**	**7.5%**	**4.0%**

We cannot account for these kinds of damages in our calculations. And we do not measure the impact of improved performance upon employee productivity or business agility, though these non-quantitative factors are also worthy of attention. Decision-makers are typically aware of the cost benefits of consolidating multiple point solutions into a single platform like the Zero Trust Exchange. But they may not be thinking of all the ways that a solution that can eliminate lateral movement, simplify security operations teams' jobs, and deliver consistent, comprehensive threat and data protection can bring value to the business.

Growing numbers of businesses are adopting cloud infrastructures for a plethora of reasons, but the move to the cloud demands new ways of thinking about securing workloads. A modern zero trust architecture radically simplified the process of mitigating some of the biggest risks that today's enterprises face. This is what leading organizations need to reduce operational overhead and administrative burden, all while overcoming the biggest cloud workload security challenges.

[24] AWS Firewall used as example here.
[25] This includes licensing costs for a Cloud-Native Firewall (AWS/Azure/GCP) and Cloud-Native VPN Connectivity.