Ebook

4 Reasons Firewalls and VPNs Are Exposing Organizations to Breaches

Yesterday’s Solutions Are Today’s Problems

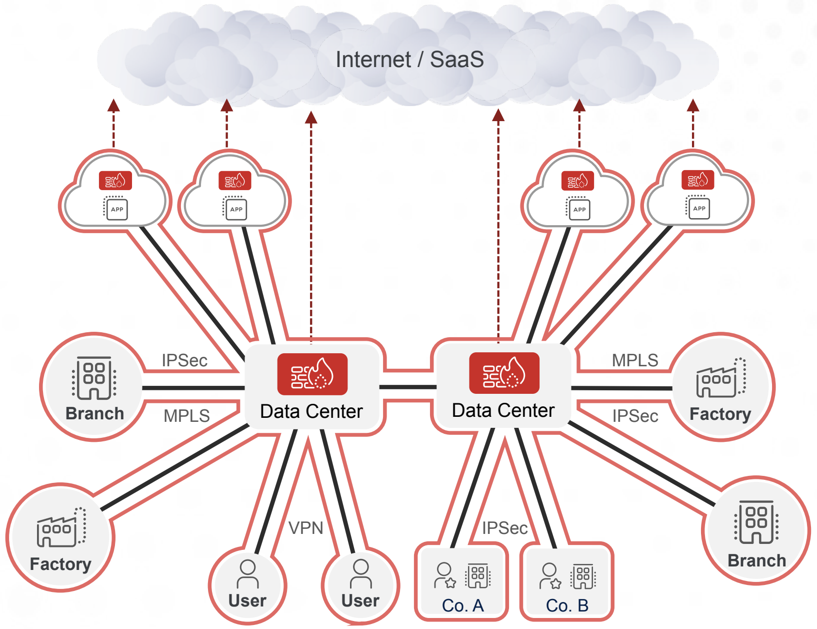
Firewalls and VPNs are exposing organizations to breaches. It may seem counterintuitive due to the fact that the two have been go-to security tools for decades—but therein lies the problem. They were designed for a time when work was done much differently than it is today. In the era of yesterday, users and apps resided on premises (whether at the main office or at a branch site), and security efforts focused on establishing a perimeter around the network that connected them. In other words, a hub-and-spoke network was defended by a castle-and-moat security model.

This approach goes by multiple names, including perimeter-based architecture, network-centric architecture, and traditional or legacy architecture. Regardless of what it is called, it inherently involves the use of tools like firewalls and VPNs, which are deployed in an attempt to protect the network; specifically, by keeping the bad things out and the good things in.

Organizations evolved rapidly in recent years, in large part due to the COVID-19 pandemic. To remain productive in 2020, they had to accelerate their digital transformation timelines, making cloud apps and remote work the new norm. However, this evolution was incompatible with firewalls, VPNs, and the perimeter-based architectures that the tools presupposed. That’s because it is infeasible to build a security perimeter around a network that is endlessly extended to more and more off-premises users, devices, apps, and clouds.

For organizations that press forward with legacy architecture amid digital transformation, it creates numerous challenges around complexity, rigidity, cost, and productivity. Additionally, and most importantly, it increases cyber risk and exposes organizations to breaches in four key ways that are explained throughout the following pages.

Firewall- and VPN-Centric Architecture



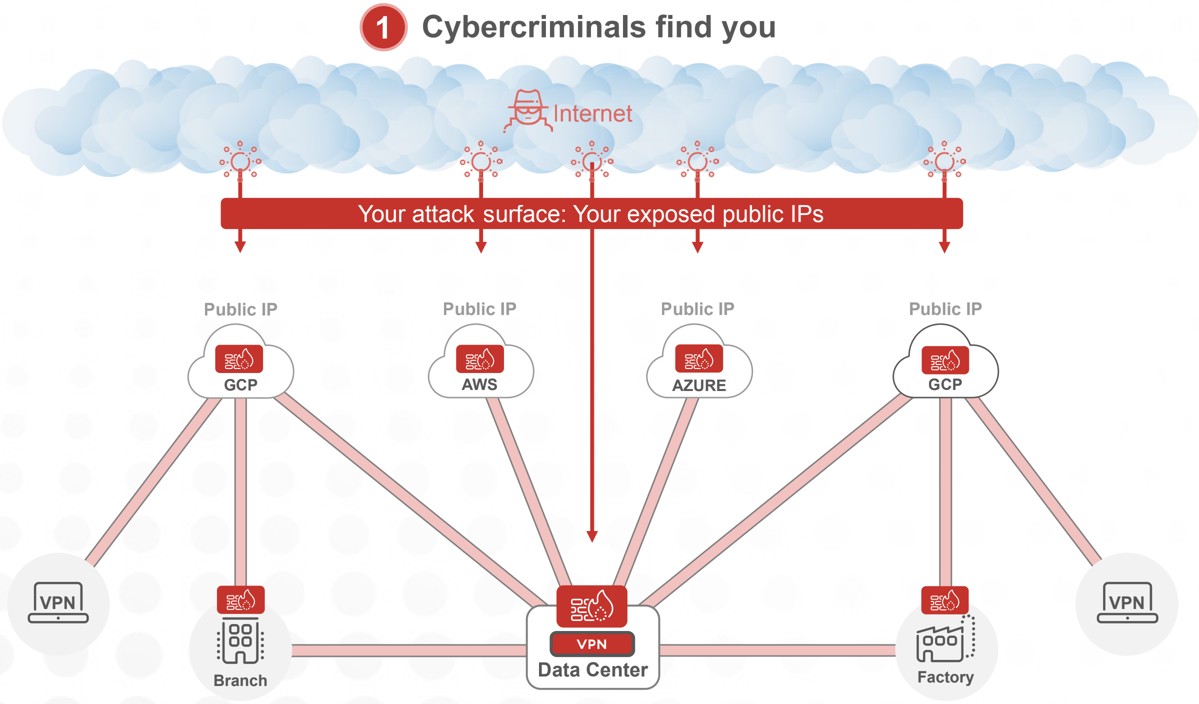
A trusted network connects users, sites, and apps.
Threat and data protection are focused on securing the network.

#1 Firewalls and VPNs Expand the Attack Surface

Cybercriminals are constantly looking for targets they can attack in order to penetrate organizations' defenses and execute their ill–intended designs. Unfortunately, with the way that work gets done today, perimeter–based architectures expand the attack surface and inadvertently assist malicious actors in their efforts to identify attractive targets.

As mentioned previously, continuing to use a hub–and–spoke network in the modern world involves continuously extending that network to more and more remote users, devices, cloud–based resources, branch sites, and more. This effectively means that a sprawling flat network is a ballooning treasure trove of interconnected resources, and that there are many avenues (cloud apps, remote users, etc.) for cybercriminals to exploit as entry points into said network. Stated simply, an ever–expanding network means an ever–expanding attack surface.

How Firewall– and VPN–Centric Architecture Increases Risk



Unfortunately, the attack surface problems of perimeter-based architectures go well beyond the above, and that is because of firewalls and VPNs. These tools are the means by which castle-and-moat security models are supposed to defend hub-and-spoke networks, but using them has unintended consequences.

Firewalls and VPNs have public IP addresses that can be found on the public internet. This is by design so that legitimate, authorized users can access the network via the web, interact with the connected resources therein, and do their jobs. However, these public IP addresses can also be found by malicious actors who are searching for targets that they can attack in order to gain access to the network.

In other words, firewalls and VPNs give cybercriminals more attack vectors by expanding the organization’s attack surface. Ironically, this means that the standard strategy of deploying additional firewalls and VPNs to scale and improve security actually exacerbates the attack surface problem further.

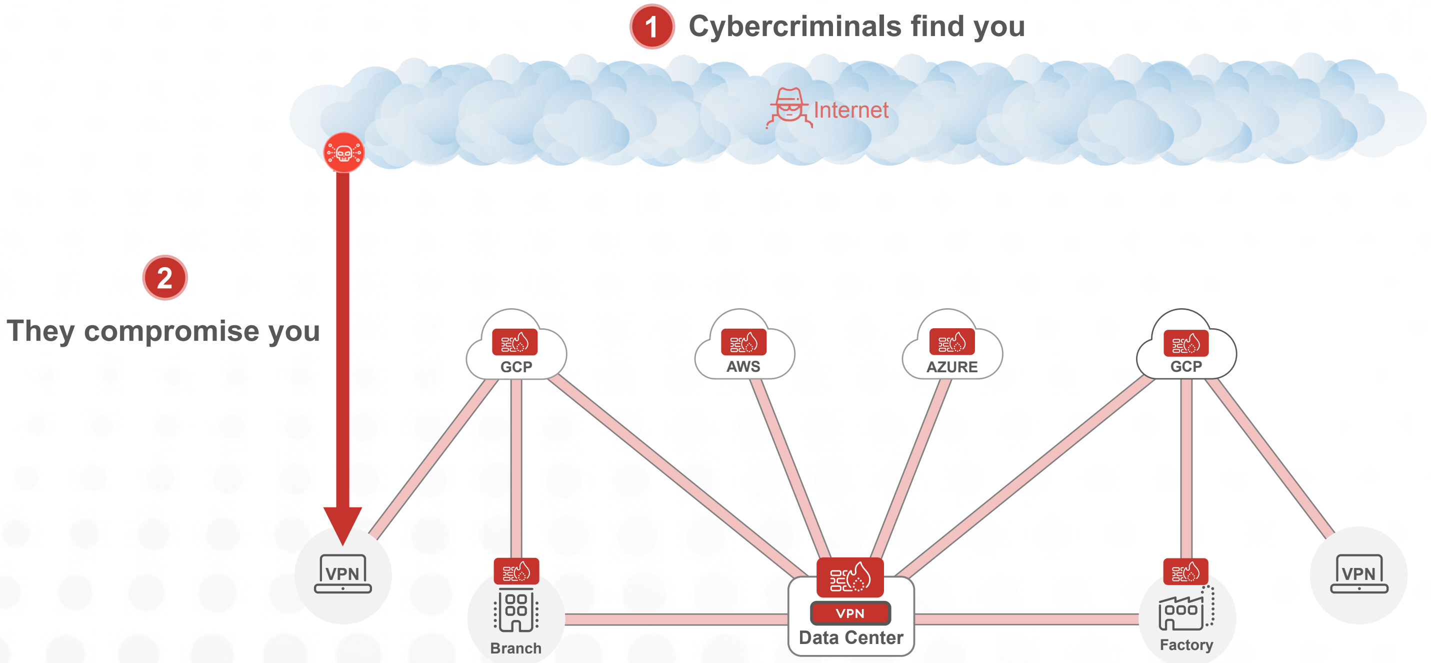
#2 Firewalls and VPNs Fail to Prevent Compromise

Once cybercriminals have successfully identified an attractive target, they unleash their cyberattacks in an attempt to penetrate the organization's defenses. Unfortunately, once again, traditional tools like firewalls and VPNs are a poor fit for securing this stage of the attack chain.

Preventing compromise requires the use of inline security policies that stop threats in real time, before they are able to enter an organization's environment and start doing damage.

This, in turn, means that organizations must be able to inspect all of the traffic across their operations so that they can identify any potential threats. To achieve this, the ability to inspect encrypted traffic is incredibly important, and that is because the vast majority of web traffic today is encrypted—upwards of 95%. But this is where another key weakness of firewall– and VPN–based architecture makes itself known.

How Firewall– and VPN–Centric Architecture Increases Risk



Inspecting encrypted traffic is a resource–intensive process, meaning that it takes an extensive amount of computing power in order to decrypt, scrutinize, and re–encrypt the traffic. Unfortunately, security appliances like firewalls struggle to perform as needed to accomplish this—whether they are deployed as hardware appliances on premises or virtual appliances in a cloud instance.

This is because appliances have fixed capacities to provide a certain level of service. They cannot indefinitely scale up to meet an organization's ever–growing requirements for real–time traffic inspection—particularly when it comes to encrypted traffic. As a result, organizations relying on traditional tools and architectures are left with incomplete inspection of encrypted traffic at best, and no encrypted traffic inspection at worst.

Failing to inspect encrypted traffic at scale means that threats are able to pass through defenses without being detected, allowing attackers to carry out their schemes. Regrettably, it seems that cybercriminals have become aware of this fact, and have begun using encrypted traffic as the preferred means of executing their attacks. Today, approximately 86% of cyberattacks now occur via encrypted traffic. So, if an organization fails to inspect its encrypted traffic, then it fails to stop the vast majority of threats trying to breach its defenses. To put all of this simply, firewall and VPN architectures fail to prevent compromise.

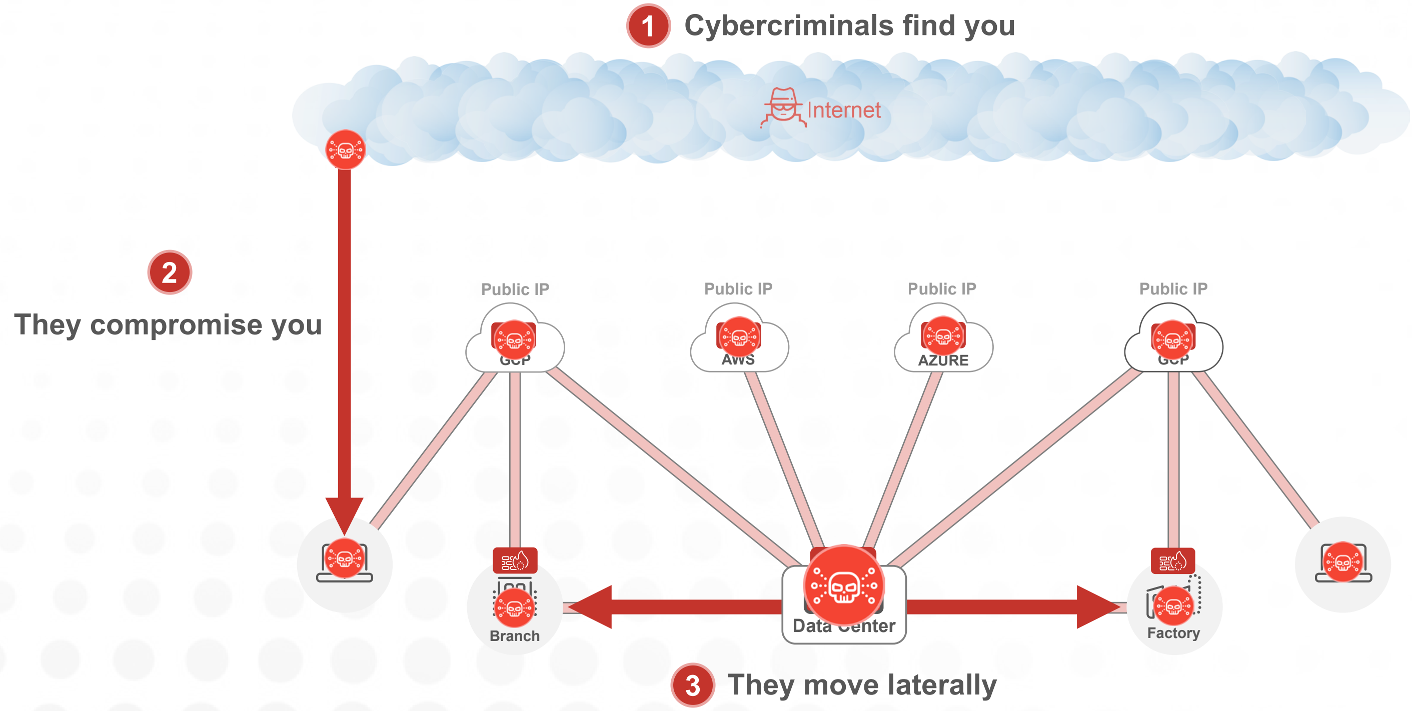
#3 Firewalls and VPNs Enable Lateral Threat Movement

Once compromise has occurred and a cyberthreat has made its way past an organization's defenses, the weaknesses of firewalls and VPNs are put on full display. Lateral threat movement, also known as lateral propagation, refers to the way that threats on the network can access the organization's various resources—whether they are on-premises applications, workloads in private clouds, or SaaS application instances. Rarely is it only a single application that is compromised when a threat breaches an organization's perimeter.

To understand how lateral threat movement is able to occur, one only needs to consider the analogy contained in the phrase "castle-and-moat security."

A moat is used to defend a castle; specifically, by preventing attackers from gaining access to the castle. This is done in order to protect the crown jewels and the people within the stronghold. However, if attackers were to make it past the moat, then a castle's primary defense mechanism would be rendered useless.

How Firewall- and VPN-Centric Architecture Increases Risk



In that case, there would be little remaining protection to keep enemies from ransacking the entirety of the castle.

The above weakness of castles and moats is also present when using firewalls and VPNs. This is because of the highly interconnected nature of the hub-and-spoke networks that some organizations still choose to rely upon, as well as the way that castle-and-moat security models focus threat protection efforts on defending access to the network as a whole.

Simply imagine firewalls as the “moat,” VPNs as the “drawbridge,” and the network itself as the “castle.” Once a cyberthreat prevails over the “moat” and enters into the “castle,” the malicious actor can easily move from one connected resource to another, accessing the various “rooms” in the “castle.”

To state all of this explicitly, firewalls and VPNs allow lateral threat movement and enable cybercriminals to expand the reaches of their breaches across the network, causing massive damage, disruption, and cost. Compromise anywhere effectively means compromise everywhere. While network segmentation is often presented as the solution to this problem, the tactic inevitably amounts to purchasing more and more firewalls, which fails to address the underlying architectural problems inherent in yesterday’s perimeter-based tools.

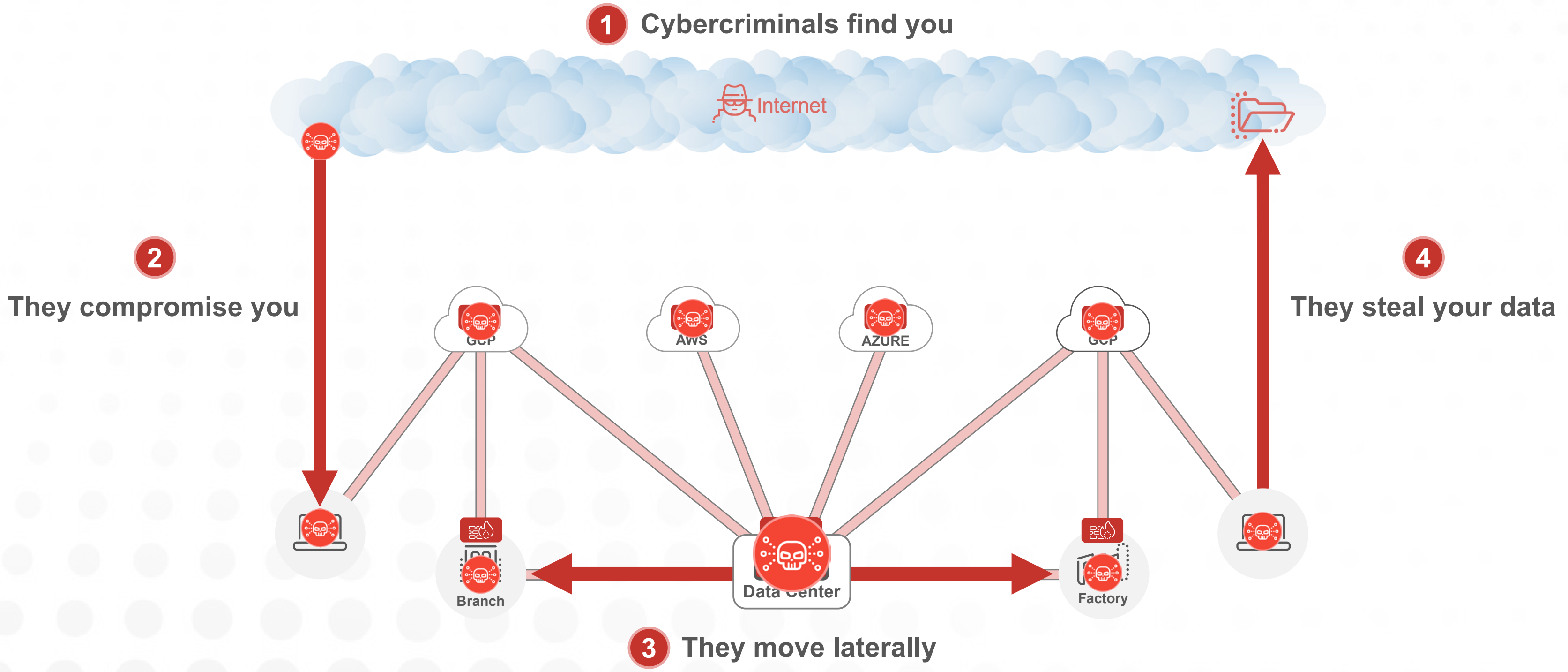
#4 Firewalls and VPNs Allow Data Loss

In the vast majority of cyberattacks, malicious actors are not looking to breach organizations merely for the thrill of it. Rather, they have a specific objective in mind, and that objective is to steal sensitive information. That's because stolen data can be sold on the dark web for a significant profit, or used as leverage in a double–extortion ransomware scheme to pressure an organization into paying a ransom. Either way, the repercussions can be catastrophic for any organization.

So, once cybercriminals have found an attack surface, compromised defenses, and begun lateral movement (all three of which are facilitated by firewalls and VPNs), they will hunt for as much data as possible across the network—prioritizing particularly sensitive or regulated information. Naturally, this is then followed by data exfiltration.

Relying upon traditional tools to stop this final link in the attack chain yields risky results once again, and enables data loss.

How Firewall– and VPN–Centric Architecture Increases Risk



1 Cybercriminals find you

2 They compromise you

3 They move laterally

4 They steal your data

As mentioned previously, over 95% of web traffic today is encrypted, inspecting encrypted traffic requires extensive computing power, and static appliances are unable to scale as needed to process the massive volumes of encrypted traffic generated by growing organizations. This challenge (for hardware and virtual appliances alike) is relevant not just for compromise, but for data loss. Cybercriminals are aware that organizations are more likely to have blind spots where traffic is encrypted, and are using this traffic as a preferred avenue for data exfiltration.

But it is not just because of scalability challenges that tools like firewalls are unable to stop data exfiltration. Yesterday's technologies were designed for yesterday's world, for a time before cloud apps and remote workers. As a result, they cannot secure modern data leakage paths; for example, the sharing functionality built into SaaS applications like Google Drive, Box, Microsoft OneDrive, and others. Similarly, misconfigured cloud resources, like AWS S3 buckets mistakenly set to "public," expose data but cannot be remediated with firewalls, VPNs, or even conventional data loss prevention (DLP) tools.

External attackers are eager to use these and other modern means to steal sensitive information; however, it is critical to note that they are not the only threat to data. Organizations must grapple with the reality that malicious and careless insiders may also leak sensitive information in the above fashions. Regardless of the perpetrator, security must evolve if data is to be kept safe.

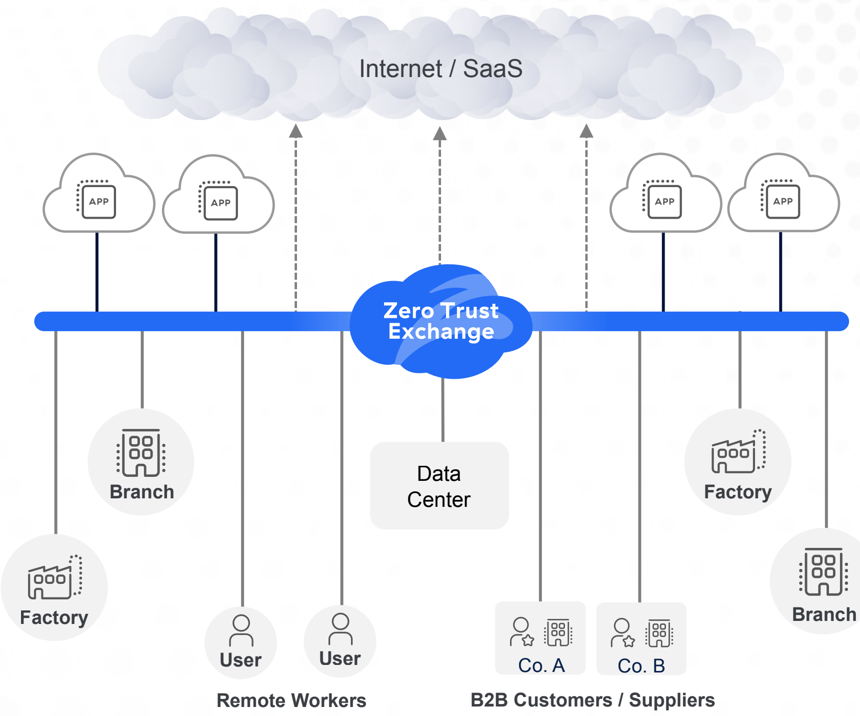
How Zero Trust Architecture Solves These Problems

Zero trust is not just another tool to add to the existing, network–centric status quo. It is not something that merely lessens the pains of perimeter–based architectures without actually solving their underlying causes. Rather, zero trust is a distinct architecture that is based on the principle of least–privileged access; it is inherently different from a standard firewall– and vpn–based architecture.

When zero trust architecture is in place, organizations benefit from a global security cloud that acts as an intelligent switchboard, securely connecting users, workloads, IoT/OT devices, and B2B partners—without extending the network to anyone or anything. At the same time, the zero trust cloud should offer comprehensive suites of solutions (like cyberthreat and data protection) that are delivered as a service at the edge, from as close to the end user as possible.

With zero trust, security and connectivity are successfully decoupled from the network, and perimeter–based architectures become things of the past.

Zero Trust Architecture



Business policies determine who can access what over any network; the network is just transport.

With this modern architecture, organizations can put an end to the four ways that firewalls and VPNs expose them to breaches:

- **Minimize the attack surface:** Leverage zero trust to stop endless network expansion, eliminate firewalls, VPNs, and their public IPs, prevent inbound connections, and hide apps behind a zero trust cloud.
- **Stop compromise:** Inspect all traffic, including encrypted traffic at scale, through a high-performance zero trust cloud that identifies threats and enforces security policies in real time.
- **Prevent lateral threat movement:** Connect users, workloads, and devices directly to apps instead of to the network as a whole, upholding the principle of least-privileged access.
- **Block data loss:** Stop data loss in encrypted traffic and across all other data leakage paths, including data at rest in the cloud and data in use on employees' endpoint devices.

In addition to reducing the risk of breaches, a zero trust architecture reduces complexity, increases user productivity, saves money, and enhances organizational dynamism, solving a variety of problems that plague firewall- and VPN-based architectures.

Wrap-Up

For those in need of a zero trust architecture, the AI-powered Zscaler Zero Trust Exchange is the platform of choice. As the world's largest and most widely deployed inline security cloud, its scale and success speak for themselves:

150+
Global data centers

360B+
Transactions secured daily

500T+
Daily telemetry signals

70+
Net Promoter Score

40%
Of the Fortune 500 are customers

Leader
In the Gartner MQ for SSE

To learn more, register for our monthly webinar, "Start Here: An Introduction to Zero Trust." In the webinar, we discuss zero trust architecture from an entry-level perspective (as well as share more information about Zscaler) so that anyone can begin a zero trust journey with confidence.

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**.

CS

contact@cybersherpa.ch
+41 21 561 36 48
Rue de Genève 100, 1004 Lausanne, Switzerland
www.cybersherpa.com