Zero Trust for Cloud

BEYOND SECURITY:

How Zero Trust helps modern enterprises pursue and profit from cloud transformation

appgate

TABLE OF CONTENTS

Beyond Security: Zero Trust and Cloud Transformation

INTRODUCTION

For every industry, cloud and cloud-native adoption ushers in workload scale, performance, and agility. According to the Ponemon Institute's *Global Study on Zero Trust Security for the Cloud* — which surveyed nearly 1,500 IT decision makers and security professionals in the U.S., Europe and the Middle East (EMEA) and Latin America (LATAM) — the top five reasons why organizations use cloud resources are to:

1. Increase efficiency
2. Reduce cost
3. Improve security
4. Shorten deployment times
5. Enable flexibility and choice

However, while motivations behind cloud adoption and the exact makeup of the environment itself will vary from organization to organization, there is a universal truth: the cloud introduces new complexities around securing workloads and managing access to them.

Unfortunately, traditional perimeter-oriented solutions and access provisioning are incapable of meeting these new security requirements, forcing enterprises to seek alternatives.

This eBook addresses how the principles of Zero Trust security, applied via Zero Trust Network Access (ZTNA), harden cloud security, remove complexity and improve your ability to achieve the business objectives driving your cloud transformation.

ZERO TRUST 101

The Zero Trust security paradigm is gaining widespread adoption throughout the technology world. In fact, the U.S. federal government has endorsed Zero Trust and issued an executive order mandating that federal agencies implement a Zero Trust architecture.

But what exactly does it mean? The terminology gets used often and not always in the right way. Depending on the context, the words "Zero Trust" could describe a methodology, a strategy to implement the principles of that methodology, or a security tool.

Let's get on the same page with a quick overview of Zero Trust security and how to apply it.

WHAT IS ZERO TRUST?

At its core, Zero Trust is a paradigm that creates a new way of thinking about cybersecurity. It challenges the conventional idea of "trust but verify" and changes the rules for how an organization grants access to resources.

Zero Trust focuses on five attack surfaces to protect an organization: people, workloads, networks, devices and data. To keep those attack surfaces safe, according to *Zero Trust Security: An Enterprise Guide*, Zero Trust applies three core principles: [1]

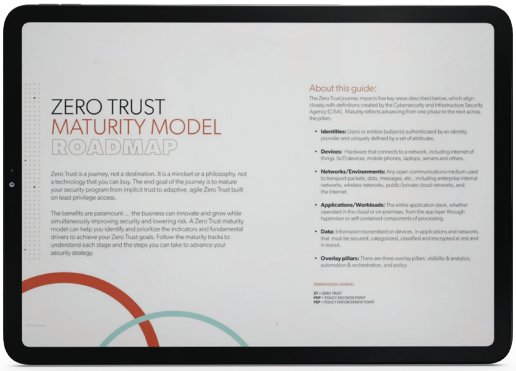
1. **Ensure all resources are accessed securely, regardless of location:** No exceptions are made for resources that may have been previously regarded as inherently secure. It requires a holistic approach for organizations that eliminates the silos and barriers that have historically existed between security tools and teams. Another requirement is to disregard whether a resource is on-premises or cloud hosted. Every asset is subject to an enforced policy model that sees no geographic perimeters.
2. **Adopt a least privilege access strategy and strictly enforce access control:** If users are not authorized to access a given service, they must not have the ability even to connect to that service. There are far too many known and critical vulnerabilities that don't require authentication to bypass something like a login page and can be remotely exploited. The ability to send network packets to a system is a privilege and must be managed as such. Least privilege access in its simplest form means you can only see and connect to resources you're entitled to and nothing else.
3. **Inspect and log all traffic:** Networks are how distributed components connect and communicate with one another and this final core principle requires the inspection and logging of network traffic. Zero Trust systems should broadly examine and log network traffic metadata but be more judicious in the inspection of network traffic content due to processing and storage costs. That traffic content should be enriched by the Zero Trust system with identity and device context to enhance an organization's ability to detect, alert, respond and support incident response.

[1] Co-authored by Jason Garbis, Chief Product Officer at Appgate, and Jerry W. Chapman, Engineering Fellow, Identity Management at Optiv Security, *Zero Trust Security: An Enterprise Guide* covers the breadth of enterprise security and IT architectures providing substantive architectural guidance and technical analysis with the goal of accelerating your organization's journey to Zero Trust.

PLANNING YOUR JOURNEY

Zero Trust is a journey, not a destination —a mindset or a philosophy, not a technology that can simply be bought. The end goal of the journey is to mature your security program from implicit trust to adaptive, agile Zero Trust built on least privilege access.

We help you navigate this journey in the *Zero Trust Maturity Model Roadmap.*



[Download the roadmap]

WHAT IS ZERO TRUST NETWORK ACCESS?

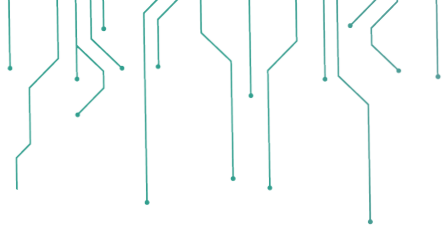
Zero Trust Network Access (ZTNA), often used interchangeably with the term software-defined perimeter (SDP), applies Zero Trust principles to network security. ZTNA is rapidly becoming the enterprise standard of choice for secure access control as the cloud, hybrid IT and hybrid workforces turn the security perimeter inside out and outdated legacy access solutions like NAC and VPNs create more risk with their static and outdated "connect first, authenticate second" approach.

With ZTNA, a user is denied access to networks and digital assets by default. Identity is subject to an extensive authentication process that considers the user, device and context. Dynamic policies and entitlements are then granted to the multi-dimensional identity, provisioning limited access to authorized resources. These surgical entitlements are conditional and based on context and risk tolerance defined by each organization.

This Zero Trust approach starts from a default deny posture and then extends limited, earned trust, which is continuously assessed. From this basis, ZTNA enables a range of business benefits—including a strengthened defensive posture, reduced complexity, improved end-user experience and streamlined automation—with fewer trade-offs between security, convenience and agility.

Now that we have a shared understanding of Zero Trust, let's take a closer look at the enterprise cloud to see what challenges exist and how ZTNA applies.

ENTERPRISE CLOUD **SECURITY CHALLENGES**



Data breaches, ransomware attacks, resource hijacking and other threats all apply to the cloud and all have the potential to cause serious short-term disruption and long-term damage to the victimized organization.

Fortunately, these risks can be lessened by strictly and surgically controlling access to cloud resources.

But before we look at how Zero Trust principles can be applied to help secure the cloud, we first need to examine what the modern enterprise cloud looks like and what obstacles render traditional approaches unsuitable.

WHAT DOES AN ENTERPRISE CLOUD LOOK LIKE?

The Ponemon Institute report cited in the introduction of this eBook reveals that there is enormous diversity in cloud environments.

The large majority of organizations represented in the study are using some form of public cloud. A third are using public cloud from a single provider, 28% use all public cloud from multiple providers (multi-cloud), and 26% use a mixture of public and private (hybrid cloud). Only 13% of respondents say their organizations use a private cloud exclusively. On average, those with some form of a public cloud infrastructure estimate that 46 percent of their applications run in the public cloud.

Those employing a multi-cloud architecture or strategy reported an average of four different clouds, while the average for those with a hybrid cloud environment is three different clouds.

More than half of respondents whose organizations don't have a multi-cloud environment in place today have plans to adopt this architecture, with a preference for the near term. Presuming that those organizations already using a multi-cloud architecture maintain this approach, these findings indicate that three years from now 67% of organizations will have a multi-cloud environment.

Looking a bit more deeply into how these clouds are used, the survey also reveals that:

- 61% of the survey respondents report that their organizations are using containers for microservices architectures and another 32% say they will use containers for microservices architecture within the next two to three years
- More than 80% expect to be using serverless architectures within the next few years
- The vast majority of organizations rely on SaaS applications: on average, respondents indicated that 43 percent of their organization's applications use SaaS, spread out across 17 separate applications; in fact, only seven percent of respondents indicated that their organization does not use SaaS today

Returning to the question that opened this section—"What does an enterprise cloud look like?"—we see the answer varies considerably from organization to organization.

THE SECURITY CONSEQUENCES OF CLOUD TRANSFORMATION

Cloud transformation is not without its challenges. In fact, while improving security is a major motivation, most respondents to the Ponemon survey reported concerns that cloud adoption has actually introduced new security risks.

Additional attack vectors and difficulty monitoring the expansive threat surface are considered by the experts polled by the Ponemon Institute to be two of the most significant concerns associated with cloud transformations.

Practically every aspect of the cloud brings with it such trade-offs. For example, microservices architectures enable developers to accelerate application delivery, but microservices-based applications are more complicated and more open than their monolithic counterparts. They also rely on APIs to facilitate communication between different microservices. This combination of complexity, openness and APIs creates a greatly expanded attack surface when compared to traditional workloads.

Unfortunately, organizations report a number of obstacles that prevent them from achieving their cloud security objectives, including:

- **Outdated network security tools:** Perimeter-based VPNs, next-gen firewalls and NACs are difficult to administer and can't secure distributed, hybrid infrastructure due to their "default allow" access approach that weakens overall security posture.
- **Fragmented security architectures:** Maintaining and scaling policies with traditional access solutions across hybrid infrastructures is cumbersome and prone to errors without a centralized console that can seamlessly apply rules across all endpoints, users and workloads.
- **DevOps and DevSecOps vulnerabilities:** The potential to introduce vulnerabilities and cyber risk goes up as development teams are pressured to quicken the pace of software releases.
- **Limited visibility and control:** A lack of a single-pane-of-glass policy view across users, endpoints and workloads makes it difficult for IT and security teams to discern a true security posture.
- **A shortage of specialized expertise:** Cloud security expertise exists at the intersection of two domains for which knowledge is already in high demand and short supply.

Any solution that purports to secure the cloud must therefore account for the enormous diversity within cloud architectures and must be able to address and overcome these challenges. Fortunately, ZTNA has proven itself up to the task.

USING ZERO TRUST NETWORK ACCESS TO **SECURE CLOUD ACCESS**

While most Zero Trust discussions focus on user access, in the cloud it's necessary to look at things differently by distinguishing between human users and other agents. In practice, securing cloud access means:

- **Securing user-to-resource access:** enabling authorized employees and third parties to access resources (e.g., workloads, applications, etc.) securely and conveniently, while preventing unauthorized users from doing so.
- **Securing resource-to-resource access:** enabling authorized resources—including microservices—running in public or private cloud environments to access other resources securely, while preventing unauthorized resources from doing so.

ACHIEVING THESE RESULTS IS ONLY POSSIBLE THROUGH A COMBINATION OF ZTNA FEATURES AND CAPABILITIES WORKING IN TANDEM.

ZTNA FEATURE SUMMARY	WHY IT'S NEEDED
Reducing the attack surface by cloaking servers, workloads and data so they remain invisible and inaccessible to a user or resource until authorization is granted	Exposed or otherwise discoverable resources provide threat actors with opportunities to gain initial access into the IT environment and to spread laterally to extend the attack
Enforcing least privilege access for all user-to-resource and resource-to-resource connections, and automatically applying least-privilege policies to new cloud environments	Preventing unauthorized access of applications, workloads, microservices, etc. is essential for containing intrusions by limiting lateral movement
Continually evaluating identity, device posture and contextual risk as authentication criteria in combination with dynamic policies that adjust in real time as risk posture or context changes	Risks can emerge and threats can escalate very quickly in the digital world, and attackers are adept at exploiting any amount of trust, making it imperative to re-assess access on a continuous basis
Integrating security tooling with the existing IT ecosystem for greater telemetry and automation capabilities, and to extract maximum value from the existing security stack	Existing tooling can provide important context needed to evaluate access requests, while automation is essential for achieving the speed and scale required in cloud environments
Providing a consistent and single view of all network traffic across hybrid IT environments	Directly addresses one of the most common and significant pain points associated with cloud transformation and equips security teams and tooling with vital intelligence
Equipping organizations with a unified policy framework for consistent policy and enforcement regardless of the cloud provider, workload or hosting model	Enables efficient policy management that extends across the entire cloud environment, reducing both the operational burden and the risk of gaps in security posture
Empowering human users with a single access solution that connects to all hybrid workloads or services concurrently	Enables secure user-to-resource least privilege access without impeding the productivity of employees and third parties
Integrating with cloud platforms and technologies both to leverage their security capabilities and to enable implementation-specific deployment models (e.g., as a Kubernetes sidecar)	Strengthens the security posture and enables functionality that is not possible without hooking into cloud APIs

BENEFITS AND USE CASES

Organizations that have applied Zero Trust principles to protect their cloud environments experience benefits that extend well beyond an improved cybersecurity posture. In fact, not only does Zero Trust directly support the major motivators for cloud adoption—increasing efficiency, reducing cost and improving security—but it also addresses specific challenges like a lack of visibility into environments and difficulty segmenting resources.

In practice, these benefits are gained through a number of use cases, some of which are outlined below.

BAKING SECURITY INTO CLOUD MIGRATIONS

Moving workloads into a cloud environment can be a major undertaking, and at enterprise scale it's simply impractical to move everything at once.

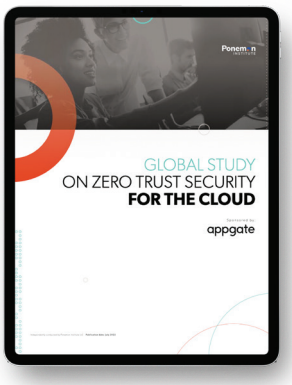
ZTNA enables an incremental migration by protecting the workloads that are part of the initial migration, and then easily scaling to accommodate the seamless addition of different waves of workloads.

All the while, administrators maintain a single set of security policies—before, during and after the migration—which significantly reduces the operational burden associated with the digital transformation.

Learn more about how ZTNA helps before during, and after cloud migrations

The top six benefits of Zero Trust for cloud, per Ponemon Institute's Global Study on Zero Trust Security for the Cloud, are:

1. Increased productivity of the IT security team
2. Stronger authentication using identity and risk posture
3. Greater network visibility and automation capabilities
4. Increased productivity of the DevOps team
5. Improved user experience
6. Prevention of unsanctioned lateral movement



Want a copy of the study? Read it now

PROTECTING TRADITIONAL CLOUD WORKLOADS

Current architectures—while agile from a development perspective—greatly increase security risks by broadening the attack surface and introducing management complexity.

ZTNA enables organizations to architect and efficiently manage a wide range of legacy workload solutions by dynamically granting, limiting, or restricting access on a precise user-to-server or server-to-server basis, informed by continual contextual assessments.

PROTECTING CLOUD-NATIVE WORKLOADS

As organizations focus on developing cloud-native applications, they need a means to easily and effectively secure containerized workloads. Unfortunately, current network security concepts don't work well in the cloud, especially when it comes to Kubernetes security best practices.

Implementing Zero Trust to overcome Kubernetes' trusting defaults requires leveraging hooks that control authentication, authorization, admission control, plus logging and auditing to control access between clusters and traditional resources that live outside Kubernetes (e.g., database server). By doing so, an enterprise can increase Kubernetes security by applying Zero Trust principles to precisely control user-to-service access and service-to-service access.

Learn more about Kubernetes security best practices and Zero Trust

SIMPLIFYING MULTI-CLOUD USER ACCESS

In the modern enterprise, many users—including employees and third parties—must access many clouds. Manually managing this many-to-many relationship with precision imposes enormous operational overhead that consumes valuable IT resources, introduces delays that impede productivity and frequently causes mistakes that introduce risk.

ZTNA offers a convenient and secure solution by enforcing dynamic, identity-centric micro-segmentation policies and permissions that are managed in a highly automated and unified manner.

ENABLING DEVOPS AND DEVSECOPS

Developers, operators, administrators and other users—including third parties such as partners and contractors—need secure and convenient access to multiple cloud environments, which may themselves be spread across a number of providers. Importantly, though, the specific access needs—in terms of who needs access to what services, which development environments and with what privileges—vary from role to role, and even from user to user.

The complexity and dynamism inherent to DevOps renders traditional tools and manual administration completely impractical, but ZTNA supports modern CI/CD pipelines by providing secure, seamless and direct access to multiple cloud accounts simultaneously—improving the speed and productivity of developer teams. In fact, the largest ZTNA deployments have been proven to work with over 100,000 users while achieving ultralow latency and linear scalable bandwidths, driven by things like autoscaling and stateless architectures.

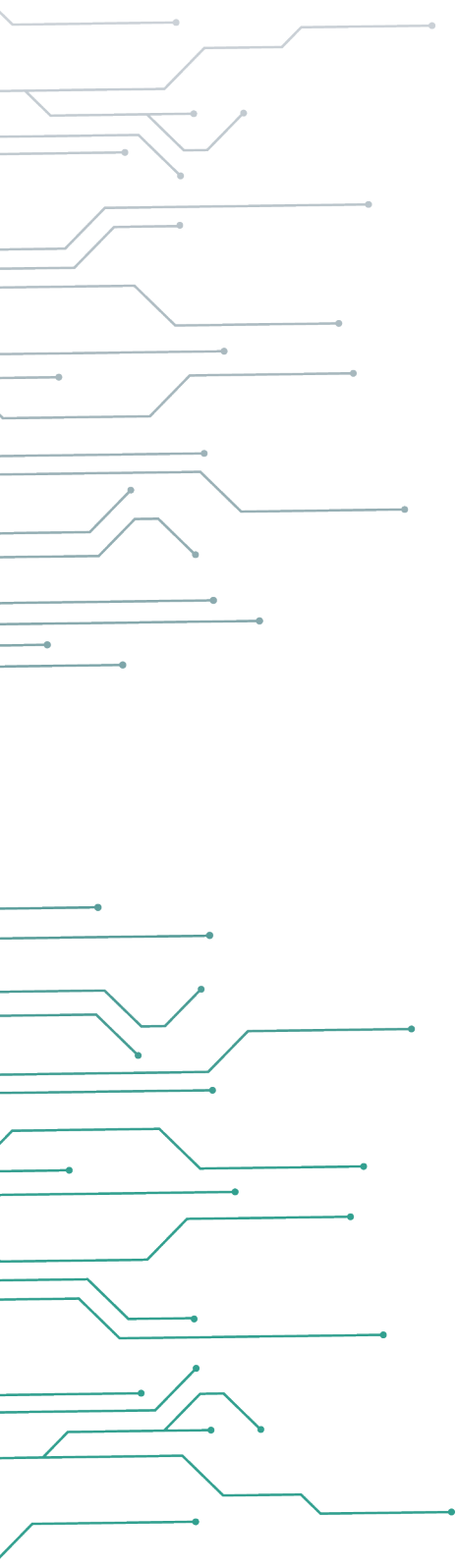
Learn more about how Zero Trust security will revolutionize DevSecOps

IMPLEMENTING SECURE ACCESS AS CODE

Within DevSecOps, the ability to run and configure security as code is a key requirement, as it defines security at the start of a project and ensures secure practices are applied consistently throughout the development cycle to deny bad actors the opportunity to infiltrate.

However, traditional solutions are ill-equipped to keep pace with the programmatic and dynamic nature of such cloud-driven security requirements.

In contrast, ZTNA solutions offer the rich integration and automation capabilities needed to dynamically create or update policy in support of just-in-time least privilege access and other requirements of security-as-code and mature development practices.



CONCLUSION

Zero Trust access is based on the fundamental principle that no user, human or machine should be automatically granted access to anything. It is the ultimate extension of the principle of least privilege approach to security.

Zero Trust Network Access has become the standard for securing enterprise access control, as it offers a proven solution that applies across the entire IT landscape—including multi- and hybrid-cloud environments—of modern enterprises large and small and that overcomes the shortcomings of traditional solutions.

ZTNA starts with a "default deny" approach to access using identity and risk factors to establish trust, which limits the privileges of users, devices and resources even after they're authenticated. It involves implementing a Zero Trust network architecture that uses dynamic, context-sensitive policies for stronger access controls while improving agility and experience.

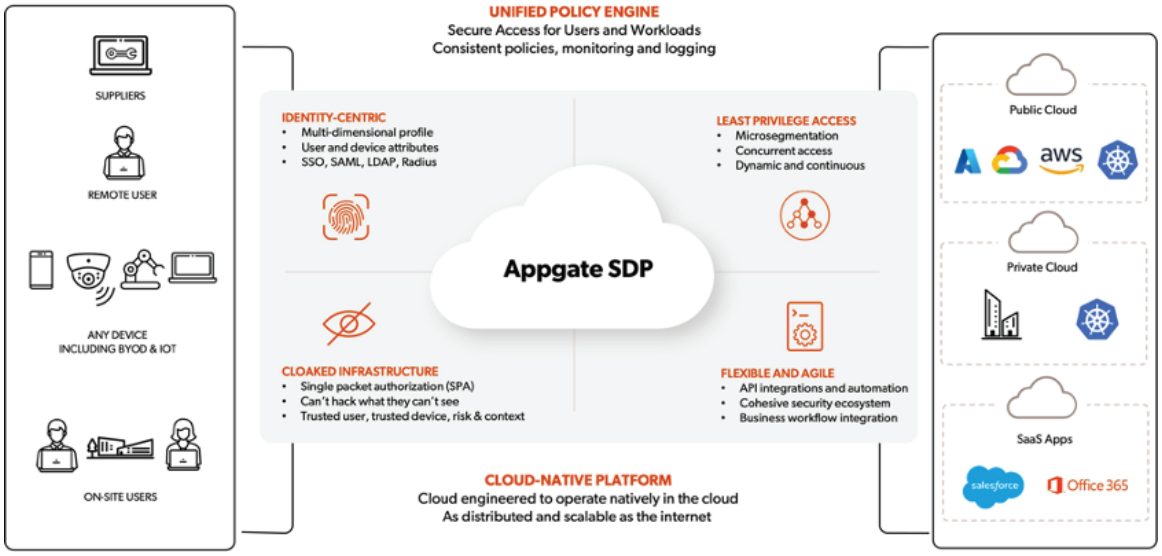
While ZTNA is an effective means of protecting valuable data and mission-critical services within cloud environments, organizations that have deployed ZTNA report a range of benefits beyond security, including added efficiency and productivity gains.

These results suggest that ZTNA shouldn't be regarded as a security layer that gets added on after a cloud migration or transformation—but instead as a vital enabler and accelerant of those cloud adoption initiatives.

ABOUT APPGATE SDP

Cloud deployments are about speed and agility, so complicated security controls that impede users and developers are antithetical to cloud benefits. Organizations with a robust cloud strategy need a Zero Trust secure access platform with a single policy framework to dynamically protect people and workloads, while keeping pace with cloud agility.

Appgate SDP, an industry-leading ZTNA solution, streamlines secure user-to-workload and workload-to-workload access within a single system and unified policy model.



UNIFIED PLATFORM

Build a Zero Trust café-style network and apply least privilege access to, from, and between users, devices, workloads and microservices. Acting as a network overlay and integrating with existing identity tools, security and business systems, Appgate SDP architecture supports a heterogeneous network and delivers a unified policy model across your entire IT ecosystem.

ANY CLOUD

Appgate SDP is proven to provide secure dynamic Zero Trust access to solve complex hybrid enterprise security problems. It secures all types of cloud workloads, as well as cloud-native microservices by enforcing granular, secure access to and from Kubernetes environments and building security into CI/CD pipelines.

VISIBILITY

Appgate SDP collects a rich set of detailed logs that provides the who, what, when and where behind every access request and session. This data can be presented using Kibana and a built-in ELK stack or be fed to an enterprise SIEM to enrich SOC and incident response and investigation. These logs also support compliance efforts and reduce audit scope.

FLEXIBLE AND AGILE

The API-first, extensible and programmable capabilities of Appgate SDP integrate with existing technology stacks so you can build security directly into business processes and workflows. It also has built-in scripting to extend functionality and adapt to future or unforeseen security challenges. This powerful combination supports secure access-as-code deployments and matures DevSecOps practices.

For more information, visit www.appgate.com/ztna.

appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Learn more at appgate.com.