appgate

SECURING THE HYBRID ENTERPRISE

Zero Trust Network Access to anything ... from anywhere ... by anyone

TABLE OF CONTENTS

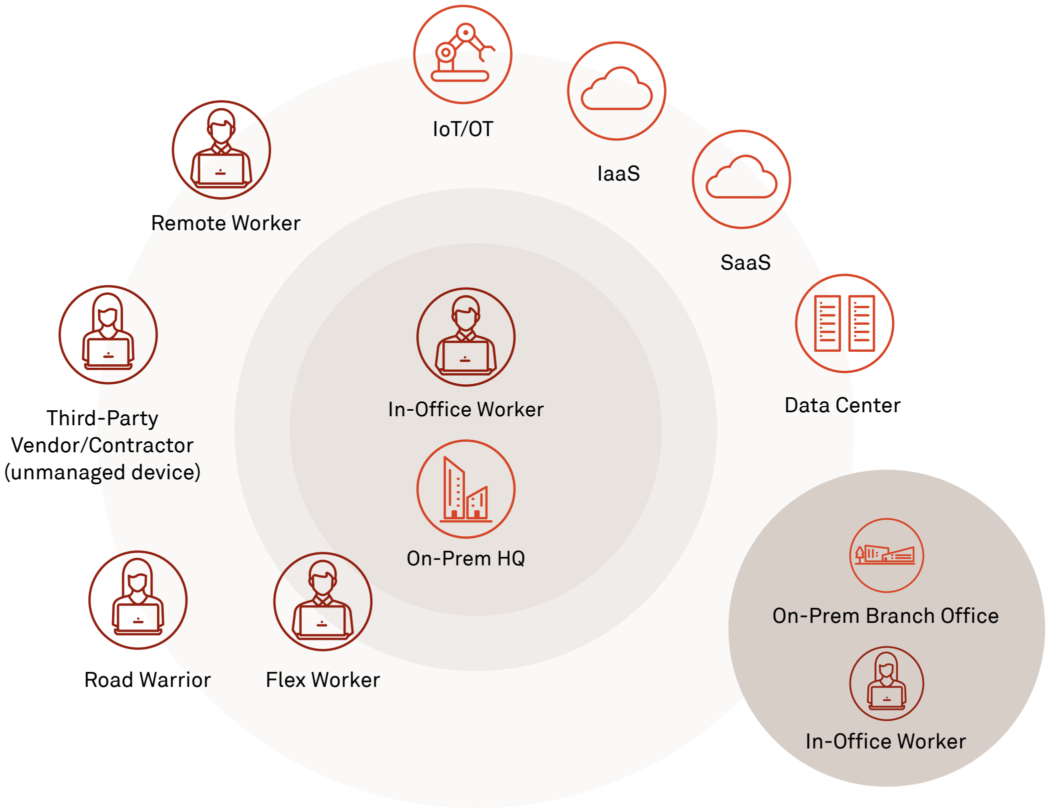
Introduction

The corporate world is witnessing a profound shift in the way people work and interact with digital assets. As conventional perimeter-centric operational models erode, the ensuing mobile workforce and diverse IT infrastructure sprawl creates a distributed juggernaut of people, devices and workloads.

The hybrid enterprise is not solely due to the pandemic that spiked remote work ... in various forms, it's been here for some time. It is a business steeped in digital transformation that's built on legacy, on-premises and multi-cloud workloads ... employing workers and third parties no longer confined to physical offices.

This paradigm shift from a fixed to nebulous ecosystem of humans, devices and systems requires a shift in how organizations approach secure access control. Legacy network security solutions can no longer protect an expansive, ever-changing attack surface created by "work from anywhere" and dispersed IT. Organizations looking to secure access for all users, devices and workloads need a comprehensive, future-proof Zero Trust Network Access (ZTNA) solution. Implementing robust ZTNA provides secure, unified and consistent access controls for all workers and workloads regardless of type or location.

2021 AND BEYOND: THE HYBRID ENTERPRISE



TRENDING STATS:

- Through 2024, organizations will be forced to bring forward digital transformation plans by at least five years as a survival plan to adapt to a post-COVID-19 world that involves permanently higher adoption of remote work and digital touchpoints.[1]
- By the end of 2021, 51% of all knowledge workers worldwide are expected to be working remotely, up from 27% of knowledge workers in 2019.[2]
- The shift to remote work amid the pandemic resulted in 47 percent of organizations reporting an increase of personal devices being used for work. As a result, a total of 82 percent of organizations said they now actively enable BYOD to some extent.[3]
- 51% of organizations have experienced one or more data breaches caused by a third party.[4]
- 92% of enterprises have a multi-cloud strategy; 82% have a hybrid cloud strategy.[5]
- 37% of workloads are on-premises.[6]
- 72% of organizations are planning upgrades to their mainframe in the next three years.[7]
- The number of internet of things (IoT) connected devices worldwide will be 38.6 billion by 2025.[8]
- 64% of respondents say that VPNs don't meet the demands of today's security requirements.[9]
- Zero Trust is one of the most-planned security projects in the next 24 months (49% either have zero trust pilots underway or plan to deploy within the next 6-24 months).[10]
- By 2024, at least 40% of all remote access usage will be served predominantly by zero trust network access (ZTNA), up from less than 5% at the end of 2020.[11]

[1] Gartner, *Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021*, 2021
[2] Ibid.
[3] Help Net Security, *Organizations ill-equipped to deal with growing BYOD security threats*, 2021
[4] SecureLink, *A crisis in third-party remote access security*, 2021
[5] Flexera, *Cloud Computing Trends: 2021 State of the Cloud Report*, 2021
[6] Statista, *Expectations around cloud and non-cloud workload distribution in the United States in 2017 and 2020*, 2021
[7] Deloitte, *Hello mainframe, our old friend*, 2020
[8] Statista, *Number of internet of things (IoT) connected devices worldwide in 2018, 2025, and 2030*, 2021
[9] 451 Research, *VotE: Information Security, Organizational Dynamics*, 2020
[10] Gartner, *Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021*, 2021
[11] Ibid.

Risks in the Hybrid Enterprise

OLD DEFENSES IN A NEW BATTLEGROUND

Fast-tracked digital transformation and the erosion of traditional perimeters have burdened IT teams with legacy cybersecurity that can't keep up. Network-centric protection like firewalls and VPNs are inadequate and their "default allow" policies make them vulnerable. Additionally, disparate access controls cause complexity, and flat networks intensify lateral movement risks. To keep pace with IT sprawl, organizations have deployed siloed access solutions that complicate policy management and enforcement. This is risky because it's much easier to provision wide-open network access than truly enforce the principle of least privilege.

LEGACY WORKLOADS

Organizations have upgraded infrastructure with public cloud and on-premises private clouds. However, they still maintain midrange or mainframes running legacy applications. These systems are often the heart of an enterprise, but modern security solutions like multi-factor authentication can't be easily applied to them. They are highly specialized environments running old operating systems and software, making migration to the cloud unlikely or very expensive to refactor. Regardless, they are critical enterprise IT mainstays that require access and security.

COMPROMISED DEVICES

Unmanaged devices, arising out of Bring Your Own Device (BYOD) policies, create vulnerabilities that are extremely problematic to manage and detect. Devices connected to the corporate network may lack on-boarding management, controls and security features making it hard—or even impossible—to secure them and their access to enterprise resources. As these compromised devices make their way inside the network, outdated "defend the perimeter" strategies are highly vulnerable to lateral movement and internal vector attacks.

THIRD-PARTY ACCESS

Partners, vendors and other third parties are essential to how business gets done. However, granting them access to critical systems introduces increased risk. Third parties may not have the same stringent enterprise security requirements and are an easy target for bad actors. Legacy secure access solutions such as VPNs expose organizations to overprivileged third-party access because these solutions treat all users the same way: as an IP address allowed to connect—or blocked from connecting—to the network. This all-or-nothing approach results in broad access for third-party users.

CLOUD ACCESS

The dynamic attributes of the cloud elevates risks because instances can easily be spun up by anyone, i.e., shadow IT. This is problematic due to a lack of knowledge about shared security models inherent with cloud providers, resulting in often unknown misconfigurations. A different cloud access risk relates to DevOps teams that—to achieve agility—provision environments with wide-open access. This speeds productivity by avoiding constant access permission updates but many developers lack a security mindset, thus creating additional exposure.

Enterprises require unified policies and dynamic one-to-one secure connections for all people, devices and workloads regardless of where they are located.

Zero Trust Network Access Solves Hybrid Enterprise Challenges

Today's cybersecurity requirements include new countermeasures created specifically to protect hybrid enterprises comprising scattered users, devices and workloads. As you harden your organization's overall security posture, many factors will be at play ... **but your top priority for this evolving hybrid world must be secure access.**

ZTNA is the most effective secure access method available. In contrast to the "default allow" mode of VPNs, network access control (NAC) solutions and firewalls, ZTNA is based on the principles of Zero Trust and takes a "default deny" approach to digital resources.

> ***"By the end of 2021, 51% of all knowledge workers worldwide are expected to be working remotely, up from 27% of knowledge workers in 2019."***[1]

ZTNA requires users to be fully authenticated across a range of identity-centric and context-based parameters such as role, time, date, location and device posture before access is permitted. ZTNA grants least privilege access with limited authorization to select hybrid workloads, which prevents unsanctioned lateral movement. And it acts as a network overlay and integrates with identity and other security systems to deliver a single policy decision point that controls access across your entire IT ecosystem.

BEWARE THE PRETENDERS:

SECURE REMOTE ACCESS

≠

ZERO TRUST NETWORK ACCESS

The need to enable millions of employees to work remotely under global pandemic health protocols resulted in rapid-fire deployments of quick fix—but unsustainable—secure access band aids.

As companies contemplate remote, in-office or work-from-anywhere models, now is the time to bolster and future proof *all* digital access control needs. This means uniform access from *any* location, **including the main office.**

Many secure access solutions claim ZTNA advantages but can only handle remote access and won't scale to meet hybrid enterprise requirements. For instance, they don't enforce the principles of Zero Trust when users are in-office and struggle to secure anything beyond web-app protocols.

A comprehensive, full-featured ZTNA solution goes beyond remote access to deliver secure access to anything from anywhere by anyone.

> ***"VPNs are antiquated, and while they may have some value for an immediate 'fix,' they need to go away. They are vulnerability aggregators and are a prime target for exploitation."***
> ***– Dr. Chase Cunningham , Dr. Zero Trust***

[1] Gartner, *Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021*, 2021

SECURING HYBRID WORKFORCES

The key to securing your hybrid workforce with ZTNA is to assume that everybody needs quick and easy secure access to private resources.

An identity-centric approach enables the operationalization of these objectives. No matter what category the user falls into, access privileges must be dictated by the user's *identity*, not their IP address. This means eliminating TCP/IP-based "connect first, authenticate second" VPNs with only username/password credentials. Whether your users are on-site, working from home, at a vendor's office or serving as a contractor, they can only gain access to resources based on authentication of identity and other critical contextual factors.

HOW ZTNA SECURES HYBRID WORKFORCES

A robust ZTNA solution leverages a software-defined perimeter (SDP) architecture to make assets "invisible" until users are authenticated and proper entitlements granted. It also simplifies and strengthens access controls for all your users, devices and workloads through these functionality and policy enforcement features:

- **Identity and context aware:** How trust is verified and users are authenticated goes well beyond the legacy TCP/IP approach. ZTNA builds a multi-dimensional user profile by combining role data with multiple identity systems and contextual user data such as date, time, location and device posture. This enables identity verification prior to provisioning access.
- **Principle of dynamic least privilege:** Users, devices and systems are permitted limited access as defined by entitlements, which adjust in real-time based on identity and context changes. This means you only have access to what you need and nothing more, which halts unsanctioned lateral movement, significantly reduces risk and makes compliance audits simpler.
- **Concurrent access:** Facilitates productivity by allowing concurrent access across heterogeneous environments through multi-tunneling capability. Users can have multiple simultaneous and direct connections through a Mutual Transport Layer Security (mTLS) tunnel. This type of access prevents latency and bottlenecks, as users no longer must wait to be authenticated multiple times when accessing more than one system.
- **Device posture checking:** Minimizes risks by conducting deep device posture analysis as criteria before granting access, which may include integration with endpoint protection software for enhanced risk evaluation.
- **Single packet authorization (SPA):** All infrastructure remains hidden until a single pre-specified and encrypted packet is received with the proper cryptographically pre-seeded data. Only then is a user be authenticated and a connection granted.
- **Default-deny:** By default, any user attempting to gain access is initially denied that privilege. By using pre-determined access criteria, a dynamic one-to-one connection is then established between the user's device and the requested resource.
- **Unified policy engine:** Reduces the burden on your security and IT teams by defining granular policies for all users, devices and workloads in any location from a centralized place—single pane of glass—to reduce complexity and enable efficient securing of workloads.
- **Flexible user access options:** Accommodates different architectural styles to cover your entire user population. Client-based systems rely on having a ZTNA client installed, but this is not practical for every use case. So, you also need the option of access via an agentless browser-based interface.
- **Seamless user experience:** Users are everywhere and highly mobile, requiring access from anywhere there is an Internet connection. Regardless of whether a user is remote or in-office, they use the same solution and have the same experience.

SECURING HYBRID WORKLOADS

Public cloud and privately hosted and legacy workloads require varying security approaches. This creates complex management headaches that can lead to risks and vulnerabilities. To securely utilize these environments, you need a single secure access solution that can handle them all—even the older mainframes and midrange servers that still support critical enterprise applications.

HOW ZTNA SECURES HYBRID WORKLOADS

All workloads are not created equal, nor do they carry the same level of risk. How they are architected, varying protocols and the surrounding ecosystem in which they reside must all be taken into account when considering how to protect them.

A robust ZTNA solution unifies secure access across all workloads, regardless of where they are hosted or what protocols they exercise. The benefits include:

- Admins leverage a centralized policy engine for all workloads, which simplifies policy management
- All resources are rendered invisible and unscannable until trust is verified and access permitted, greatly reducing your attack surface
- Seamless addition of MFA and least privilege access to non-standard operating systems and legacy infrastructure without refactoring
- Fine-grained micro-segmentation limits unsanctioned lateral movement across all workloads
- Metadata can be leveraged for dynamic, just-in-time policy and auto-scaling, which is particularly helpful for DevOps and the cloud
- The software-defined architecture of ZTNA solutions allows for simple and cost effective scalability as new workload requirements get defined
- The principles of Zero Trust get applied for service-to-service connections (east-west traffic flows), further halting unsanctioned lateral movement and the spread of malware between workloads

Data traverses between workloads to enable digital business and it's important to consider not only how users access workloads but also the service-to-service connections. Many systems require interconnectivity and access to other workloads in order to run the operation. The principles of Zero Trust and least privilege can and should be applied to machine-to-machine communication.

Choosing the Right ZTNA Solution

The enterprise has changed. People are working differently. Workloads are hosted anywhere. Physical perimeters no longer exist. As a result, traditional secure access controls are no longer effective for today's hybrid enterprise.

ZTNA is rapidly emerging as the secure network access solution of choice. It delivers individual micro-perimeters around every user and resource, cloaks every digital asset and permits only authenticated users to access only the precise assets they require to do their jobs.

However, not all ZTNA solutions are created equal … the most effective will address more than just secure remote access, which some providers claim is the only factor to consider. A future-proof ZTNA solution will safeguard access requirements across your entire ecosystem of users, use cases and workloads. And it will readily adapt to your "now and next" business initiatives as well as unforeseen external forces of change.

Ultimately, only full-featured, agile ZTNA solutions, like Appgate SDP, are built to meet the demands of a hybrid enterprise, its hybrid workloads and work-from-anywhere users.

The right ZTNA solution goes beyond solving today's hybrid enterprise security issues. It has the flexibility to adapt to tomorrow's unknown challenges.

WANT TO LEARN MORE?

Read *Zero Trust Network Access: Everything You Need to Know*

DOWNLOAD NOW

About Appgate SDP

Appgate SDP is a comprehensive, highly scalable, enterprise-grade ZTNA platform that delivers concurrent secure access for all users, devices and workloads wherever they reside. It effectively eliminates your attack surface by making resources invisible until users are authenticated. And its rich feature set, including APIs, allows customization that aligns with your central IT requirements and processes.

You can smoothly deploy Appgate SDP on-premises, in any cloud, in hybrid scenarios or as a service by using a client- or browser-based model ... or both. A multi-dimensional identity profile for each user and device enables conditional, contextual access built on dynamic entitlements that adjust in real-time to changing conditions and risks.

In addition, Appgate SDP reduces administrative burdens with consistent configuration across all environments to unify access and keep policies in sync with your dynamic infrastructure. It applies a single framework to all users, devices, networks and resources using micro-segmentation to deliver 1:1 secure access between users and authorized applications, regardless of location.

Appgate SDP enables digital transformation with a ZTNA approach that reduces risk, removes complexity and future-proofs your security posture.

Visit ***appgate.com/SDP*** *to learn more.*

Want to see for yourself how Appgate SDP delivers comprehensive ZTNA to anything ... from anywhere ... by anyone?

GET A DEMO