appgate

SECURING THE HYBRID ENTERPRISE
Zero Trust Network Access to anything from anywhere by anyone

Hybrid enterprises, characterized by globally distributed workforces and a combination of legacy, on-premises and multi-cloud workloads, must overcome a number of security hurdles:

- **Traditional cybersecurity systems** were built for high-trust, perimeter-centric environments, making them ill-equipped to protect an expansive, ever-changing attack surface created by work-from-anywhere policies and dispersed IT environments

- **Legacy workloads** on midrange and mainframe equipment are difficult to secure and expensive to refactor but must still be accessible

- **Compromised devices** serve as unwitting attack vectors and may lack strict controls (e.g., BYOD)

- **Cloud environments** are notoriously complex to manage, leading many IT teams to default to permissive policies

ZERO TRUST NETWORK ACCESS (ZTNA)

Zero Trust Network 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, which takes a "default deny" approach to digital resources.

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 safeguards access across your entire ecosystem of users, use cases and workloads. And, it will readily adapt to your "now and next" business initiatives and unforeseen external forces of change.

"By 2024, at least 40% of all remote access usage will be served predominantly by Zero Trust Network Access, up from less than 5% at the end of 2020."

— Gartner, *Gartner forecasts 51% of global knowledge workers will be remote by the end of 2021*

APPGATE SDP FEATURES AND BENEFITS

Appgate SDP is a highly scalable, enterprise-grade ZTNA platform that:

- Delivers concurrent secure access for all users, devices and workloads wherever they reside

- Eliminates attack surfaces by making resources invisible until users are authenticated

- Allows customization through a rich feature set, including APIs, which aligns with 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 multidimensional identity profile for each user and device enables conditional access built on contextual entitlements that adjust in real time to changing conditions and risks.

Appgate SDP also:

- Reduces administrative burdens by providing a single framework and consistent configuration to unify access

- Keeps policies in synchronization with dynamic infrastructure

- Features micro-segmentation to deliver 1:1 secure access for users, devices, networks and resources

2021 AND BEYOND: THE HYBRID ENTERPRISE
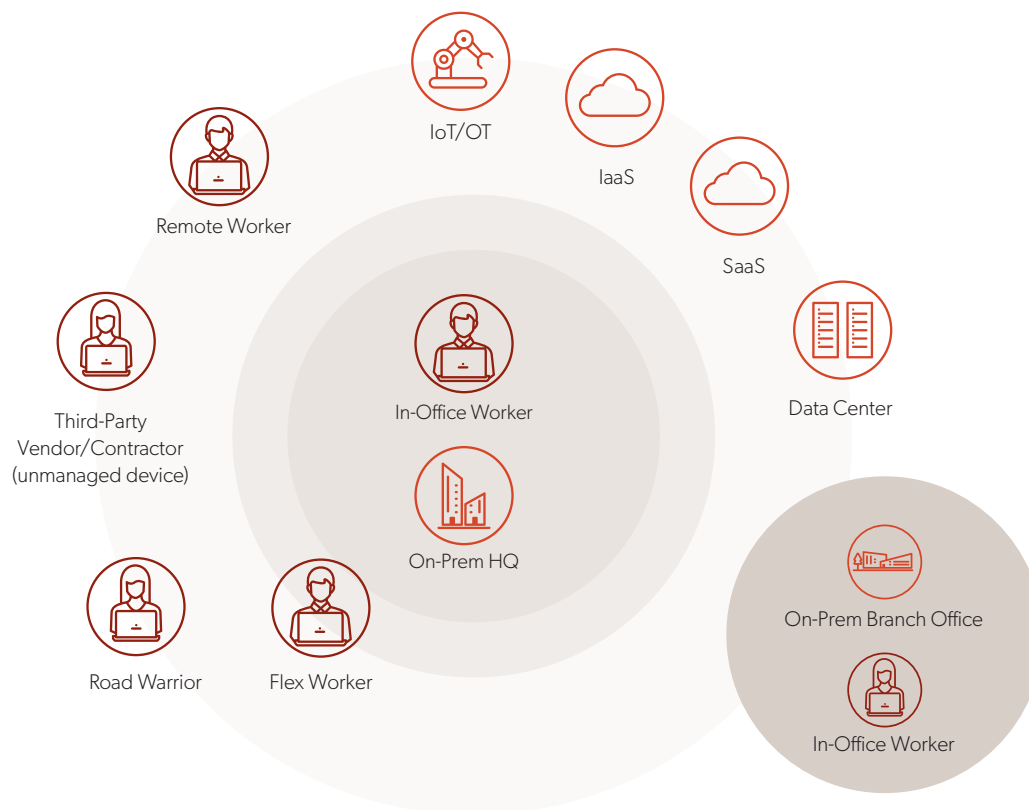
TRENDING STATS:

- 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.[1]

- 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.[2]

- 51% of organizations have experienced one or more data breaches caused by a third party.[3]

- 92% of enterprises have a multi-cloud strategy; 82% have a hybrid cloud strategy.[4]

- 37% of workloads are on-premises.[5]

- 72% of organizations are planning upgrades to their mainframe in the next three years.[6]

- The number of internet of things (IoT) connected devices worldwide will be 38.6 billion by 2025.[7]

- 64% of respondents say that VPNs don't meet the demands of today's security requirements.[8]

- 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).[1]

- 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.[1]

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

[2]Help Net Security, *Organizations ill-equipped to deal with growing BYOD security threats,* 2021

[3]SecureLink, *A crisis in third-party remote access security,* 2021

[4]Flexera, *Cloud Computing Trends: 2021 State of the Cloud Report,* 2021

[5]Statista, *Expectations around cloud and non-cloud workload distribution in the United States in 2017 and 2020,* 2021

[6]Deloitte, *Hello mainframe, our old friend,* 2020

[7]Statista, *Number of internet of things (IoT) connected devices worldwide in 2018, 2025, and 2030,* 2021

[8]451 Research, *VotE: Information Security, Organizational Dynamics,* 2020

SAFEGUARD YOUR HYBRID ENTERPRISE WITH APPGATE SDP

Appgate SDP delivers industry-leading ZTNA to anything from anywhere by anyone. It 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 permitting least privilege access to enterprise resources (to prevent unsanctioned lateral movement).

Acting as a network overlay and integrating with existing IAM and security systems, Appgate SDP delivers a single policy decision point that controls access across an enterprise's entire IT ecosystem to secure hybrid workforces and workloads.

SECURING HYBRID WORKFORCES

In addition to cloaking assets until users are authenticated and entitlements granted, Appgate SDP simplifies and strengthens access controls for all your users, devices and workloads via features such as:

- Identity and context awareness built on multidimensional user profiles that combines role and user data
- Dynamic least privilege approach ensures access by users to only what is needed, nothing more
- Concurrent access allows multiple simultaneous and direct connections through mTLS tunnel
- Device posture checking minimizes risk by incorporating contextual data from endpoint protection solutions
- Single packet authorization (SPA) keeps infrastructure hidden until pre-specified and encrypted packet received
- Unified policy engine defines granular policies for all users, devices and workloads in any location
- Flexible user access options accommodate different architectural styles to cover entire user population
- Seamless, consistent user experience from wherever they work (e.g., remote or in-office)

"We are likely to continue at better than 95% [of employees working from home] … Appgate enables connections to workloads wherever, securely."

- Senior technology strategist, high-tech company

SECURING HYBRID WORKLOADS

Public cloud, privately hosted and legacy workloads have various levels of risk and security requirements. Appgate SDP is a single secure access solution that improves usability and minimizes administrative burdens via features such as:

- Centralized policy engine for all workloads
- All resources rendered invisible and unscannable until trust is verified to greatly reduce attack surface
- MFA and least privilege access can be introduced to non-standard operating systems and legacy infrastructure
- Fine-grained micro-segmentation limits unsanctioned lateral movement across all workloads
- Metadata can be used for dynamic, just-in-time policy and auto-scaling—ideal for DevOps and the cloud
- Software-defined architecture allows for smooth, cost-effective scalability as workloads grow
- Principles of Zero Trust applied to service-to-service connections (east-west traffic) halt unsanctioned lateral movement and spread of malware between workloads

"It's easy to control who gets access to which resources no matter where they are running or what else is running on the same system."

-- Director of information security engineering, government not-for-profit

---

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

LEARN MORE

ABOUT APPGATE

Appgate is the secure access company that provides cybersecurity solutions for people, devices and systems based on the principles of Zero Trust security. Appgate protects more than 700 organizations across government and business. Learn more at appgate.com