appgate

ZERO TRUST NETWORK ACCESS **SOLUTION BRIEF**

# APPGATE SDP SOLUTION OVERVIEW

## Maximize security, maintain control, cut complexity and cost with industry-leading, direct-routed universal Zero Trust Network Access

Network security is hard. Infrastructures are complex. Applications and requirements constantly change. Attack surfaces grow overnight. Organizations of all sizes are turning to universal Zero Trust Network Access (ZTNA) to address today's security and operational challenges that include:

- More attack vectors like unmanaged devices, cloud workloads, IoT/OT devices, zero-day exploits, remote workers and third parties
- Flat network topologies exploited by threat actors seeking unsanctioned lateral movement
- Perimeter-based security solutions and disparate controls not built for hybrid workforces and distributed infrastructure
- Obsolete connect, then verify access models that introduce needless risk
- Overprivileged employees and third-party users with access to more data and systems than required to do their job
- Tedious, manual and error-prone user and device access provisioning for heterogeneous legacy solutions like VPNs, NACs and WANs

To compete globally, organizations continue to escalate digital transformation via the cloud, DevOps, CI/CD, IoT, AI, automation and SaaS initiatives. Security must stop inhibiting and start enabling enterprise agility as well. Universal ZTNA drives proven ROI for the business and overcomes the operational deficiencies and inherent risk of legacy security solutions. For these reasons and more, ZTNA is the fastest-growing global network security segment forecasted to grow 31% in 2023, according to Gartner.

### Appgate SDP: Industry-leading Universal ZTNA Designed Differently for a Reason

But not all Zero Trust access solutions are created equal. The vast majority are cloud-routed built on a proxy-based architecture often called identity-aware proxy (IAP) that runs all traffic through a vendor cloud. These cloud-routed ZTNA solutions are good enough to secure remote connections to web apps but weren't designed for complex hybrid infrastructure nor can they accommodate all use cases.

That's why Appgate SDP, the industry's most comprehensive universal ZTNA solution, is designed differently. It is purpose-built on a direct-routed software-defined perimeter model adhering to stringent Cloud Security Alliance (CSA) Zero Trust guidelines. And it can secure all user-to-resource and resource-to-resource connections across every enterprise use case including remote, on-premises, multi-cloud, cloud native, legacy applications and infrastructure, IoT and OT.

Additionally, the unique Appgate SDP architecture ensures that sophisticated organizations get the flexibility, control and extensibility required to secure their whole environment, harden defenses, transform their network, and drive measurable ROI and value for the business.

### APPGATE SDP ZTNA BENEFITS

#### HANDLES COMPLEX ENVIRONMENTS, HIGH SECURITY REQUIREMENTS AND INTRICATE NETWORK TOPOLOGIES

- Get flexibility to design architecture for unique network challenges and requirements
- Maintain control of how traffic and data flows without routing through vendor cloud
- Utilize extensibility to build unified, interoperable security ecosystem across full environment without vendor lock-in

#### HARDENS YOUR SECURITY POSTURE

- Cloak all resources making attack surfaces invisible
- Stop unsanctioned lateral movement with risk-informed Zero Trust least privilege access
- Gain full network visibility
- Build a strong Zero Trust journey foundation

#### REVOLUTIONIZES YOUR NETWORK

- Overlay secure universal access experience across entire topology
- Transform the network with secure café-style connectivity
- Reduce OpEx by eliminating connectivity costs and expensive private networks like WAN and MPLS

#### MINIMIZES IT AND SECURITY ADMIN TIME

- Decrease hands-on time to configure, manage and scale access with unified policy engine
- Automate access provisioning
- Minimize trouble tickets

#### IMPROVES USER EXPERIENCE

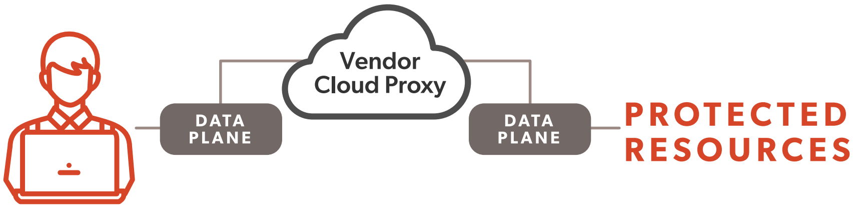
- Deliver consistent connectivity experience for any employee or authorized third party on any device (remote, in office, on campus)
- Deploy simultaneous direct connections via patented multi-tunneling technology

## Cloud-routed vs. Direct-routed ZTNA

Organizations on a Zero Trust journey shouldn't compromise when building their ideal Zero Trust architecture. When comparing architecture models, direct-routed ZTNA offers distinct operational and security advantages over cloud-routed ZTNA solutions.

### Cloud-routed ZTNA

Most Zero Trust Network Access solutions route your traffic through a cloud broker and are good enough to secure remote connections to web apps but can't handle complex network topologies and hybrid infrastructure.

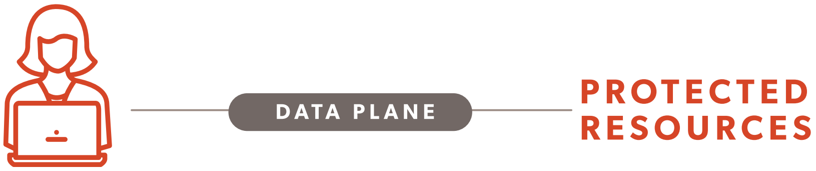


Cloud-routed disadvantages:

- Network traffic forced through vendor cloud
- Network protocol and on-prem resource constraints
- Throughput, scale, latency and hair-pinning limitations
- Implicit trust of vendor multi-tenant cloud
- Hidden or variable costs

### Direct-routed ZTNA

Direct-routed ZTNA avoids vendor cloud pitfalls, puts you in control of how data traverses your network and secures all user-to-resource and resource-to-resource connections from anywhere across hybrid infrastructure scattered everywhere.



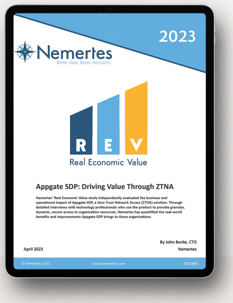
Direct-routed advantages:

- Full control over your network traffic
- Universal access control for all users, devices and workloads
- Low-latency, high availability direct access
- Flexible deployment options for true Zero Trust architecture
- Predictable pricing

### THE PROVEN ROI OF APPGATE SDP

Organizations are reaping real returns by deploying universal, direct-routed ZTNA. An independent 2023 Nemertes analyst study quantifies the operational and security improvements identified by commercial and federal Appgate SDP customers:

- 83% saw significant reduction in the number security incidents
- An overall 87% average decrease in time to modify access privileges
- An overall 32% average reduction in hands-on staff time to manage access
- An overall 55% average decrease in the number of security tools needed to manage on-prem access
- A 67% decrease in connectivity costs reported by global systems integrator
- A 6% decrease in gross IT spend reported by software and IT services company



2023

Nemertes
Better data. Better decisions.

R E V
Real Economic Value

Appgate SDP: Driving Value Through ZTNA

Nemertes' Real Economic Value study independently evaluated the business and operational impact of Appgate SDP, a Zero Trust Network Access (ZTNA) solution. Through detailed interviews with technology professionals who use the product to provide granular, dynamic, secure access to organization resources, Nemertes has quantified the real-world benefits and improvements Appgate SDP brings to these organizations.

April 2023

By John Burke, CTO
Nemertes

© Nemertes 2023 www.nemertes.com DN10842

Get full Nemertes report and industry-specific case studies on the operational and security benefits of Appgate SDP.

**DOWNLOAD NOW**

## Nemertes Report: Customers Highlight Appgate SDP Benefits

"Many of our legacy internal systems are unpatched and contain vulnerabilities that are difficult or impossible to remediate. Limiting exposure to these machines to only those with legitimate needs significantly reduced our attack surface."
*Associate Director, Security Operations, Major Internet Retailer*

"Many products focus on web only. Appgate was network-centric, which we were interested in. We couldn't allow third-party access before, as we had no tools to do this. Our level of security and granularity of access have improved."
*Principal Architect, Global IT Services Company*

"Deploying Appgate resulted in 6% reduction in gross IT spend, 5.7% in security spend."
*Principal Enterprise Architect, Software and IT Services Company*

## Covering All Strategic Use Cases

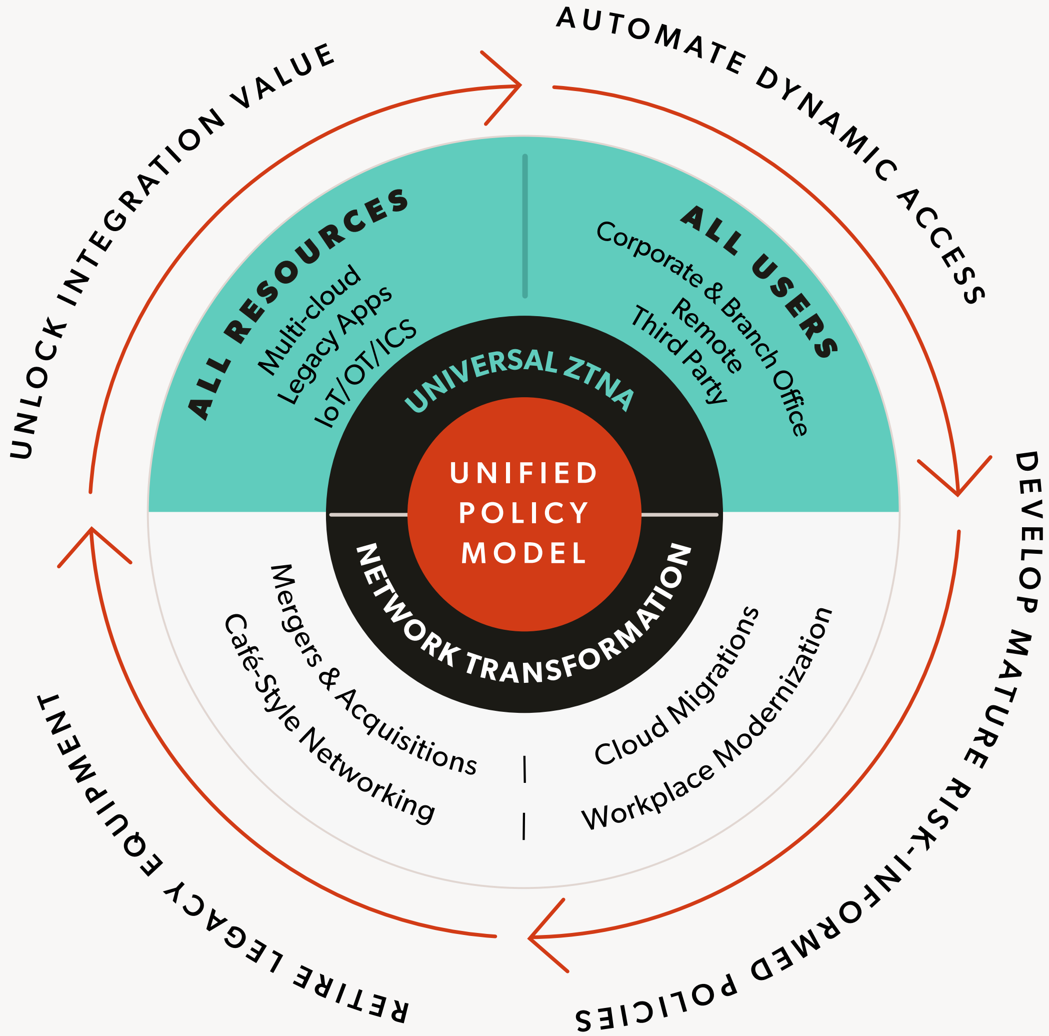
Many organizations deploy Zero Trust Network Access as the foundational start of their Zero Trust journey. The flexibility, extensibility and integration capabilities of Appgate SDP direct-routed ZTNA supports any organization's ideal Zero Trust architecture, puts IT and security teams in control of how data traverses the network, and can be applied across all enterprise use cases.

### THE JOURNEY TO ADAPTIVE ZERO TRUST SECURITY

**Think big**
Direct-routed Zero Trust access allows you to transform your network, retire legacy equipment and reach the ideal state of adaptive Zero Trust.

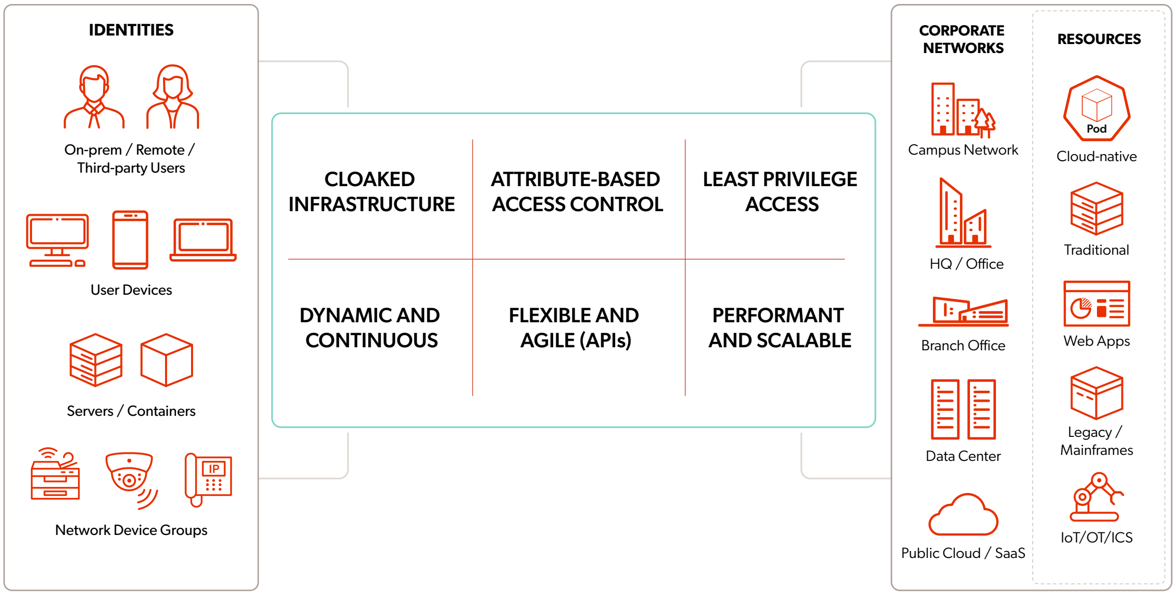
**Start small**
Your ideal state won't be built in a day. First tackle ZTNA use cases that will address immediate risk and prove value to the business.

**Scale fast**
Rapidly deploy universal ZTNA across your full environment to replace legacy tools and integrate with adjacent systems to continue to mature and automate access policies.



> **"IT people are understandably leery of new tools and bold claims, but the truth is Appgate SDP just works. The security, transparency and scalability are exactly what we need."** -- *Leslie Devlin, CISSP, Senior Security Manager, Reltio*

## Appgate SDP Unified Policy Model



Appgate SDP is built on six core design tenets:

- **Cloaked infrastructure:** A sophisticated form of single packet authorization (SPA) makes your network invisible where no ports are exposed because hackers can't attack what they can't see.
- **Attribute-based access control:** Identity-centric security that adapts access based on user, device, application and contextual risk, building a multi-dimensional identity profile before access is granted.
- **Least privilege access:** Builds "segments of one" just-in-time, session-based micro firewalls or perimeters using patented multi-tunneling technology to microsegment users, workloads and resources and limit lateral movement inside the network.
- **Dynamic and continuous:** Continuous is a core Zero Trust tenet but operational benefits are realized when adding dynamic live entitlements that automatically modify access in near-real time based on context and risk so security threats are automatically blocked.
- **Flexible and agile:** Extensible 100% API-first technology that enhances and integrates with your technology stack so you can build security directly into the fabric of your business processes and workflows.
- **Performant and scalable:** Stateless and distributed architecture allows for nearly limitless horizontal scale and performance.

The combination of these design principles is what makes industry-leading Appgate SDP the most comprehensive Zero Trust Network Access solution available on the market today … securing connections with a unified policy model that applies to:

### All Users

Not just remote but also on-premises, campus, branch office and hybrid workers

### All Resources

Not just cloud-native or web applications, but also legacy and custom applications

### All Locations

Not just cloud, but also hybrid, multi-cloud, headquarters, branch offices and data centers

> **"Appgate SDP saved time and hassle since it was easy and quick to roll out. The entitlements are very straightforward and make a lot of sense. Day to day, I don't have to touch it! And the end users are pleased with the experience."** -- *James Sharp, Senior Network Engineer, Convoso*

## How Appgate SDP Works

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

Appgate SDP consists of three major components:

- The **Controller** is the policy decision point—the brain of the system—and acts as a trust broker, evaluating context and granting entitlements.
- The **Gateway** is the policy enforcement point and is located wherever resources need to be protected.
- The **Client** connects users with their allowed access to protected resources.

Both the Controller and Gateway are cloaked using single packet authorization (SPA). When a user or identity needs access to a resource, they connect to the Controller via SPA; the Controller then authenticates the user (via OIDC, SAML, LDAP or Radius) and retrieves all configured user claims to determine access entitlements. Based on this multi-dimensional identity profile, the Controller generates a live entitlement token and sends it to the Client via a signed certificate.

Using SPA, the Client sends that live entitlement packet to the Gateway. Once the Gateway validates that the certificate has not been tampered with, it dynamically generates a microsegment that allows access only to specific resources granted by the controller.

Crucially, Appgate SDP continuously monitors the entire system for changes in context—adjusting or revoking access privileges in near real-time.

### Keeping Up With the Business

Unlike static entitlements used by traditional access control solutions, live entitlements are granted based on context and risk at the time of access and are reevaluated when those factors change.

### Reducing the Attack Surface

The Client can only connect to Gateways where a user is granted entitlements; Clients only have access to specific resources, while all others remain cloaked.

**Got 3 minutes?** Watch a short introductory demo on how Appgate SDP works.

WATCH NOW

### Zero Trust Access Demo Hub

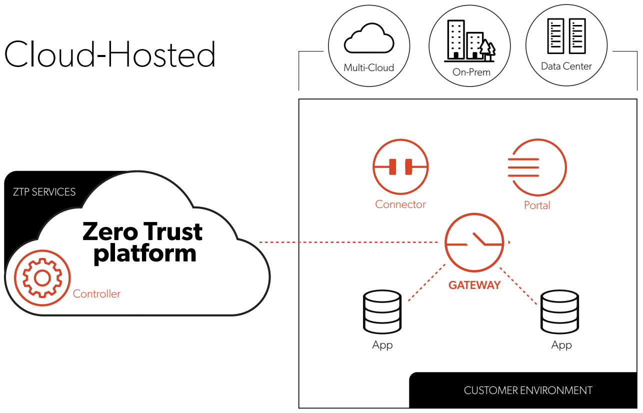
Watch demos on the robust features and functionality of Appgate SDP, platform services and integrations.

EXPLORE DEMO HUB NOW

## Appgate SDP Deployment Models

Zero Trust architectural requirements are unique for each organization. Appgate SDP offers flexibility with a choice of deployment models: cloud-hosted, self-hosted or isolated.

The result is a powerful, immensely flexible solution that can be configured to meet exact security and compliance requirements regardless of your network topology. And advanced automation and orchestration tools can be deployed to further streamline administration.



### AS A SERVICE DELIVERY AND ACCESS TO VALUE-ADDED PLATFORM SERVICES

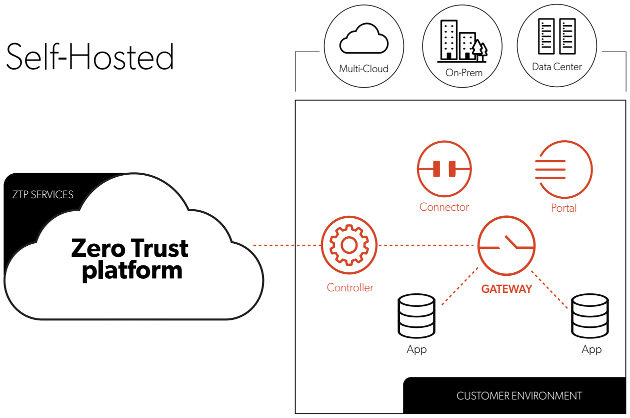
Not to be confused with cloud-routed architecture, your controller is hosted in our platform's cloud environment and other appliances remain in your controlled environment. This reduces admin burden and overhead by offloading monitoring, maintenance and upgrades to Appgate.

*Appgate SDP Deployment Models (cont.)*

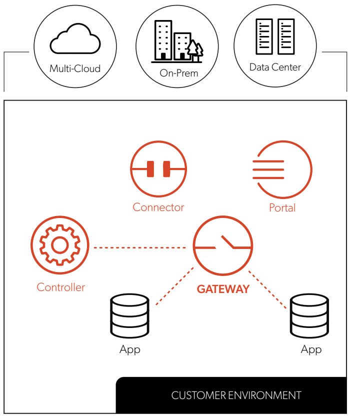
### SELF-HOSTED WITH ACCESS TO VALUE-ADDED PLATFORM SERVICES

Customer hosts controllers (or policy engine) themselves and connects their Appgate SDP deployment to Zero Trust platform services with a few simple clicks.

Self-Hosted



Isolated



### ISOLATED WITH NO ACCESS TO ZERO TRUST PLATFORM SERVICES

This is for those organizations that must maintain a completely isolated environment for internal or external policy compliance.

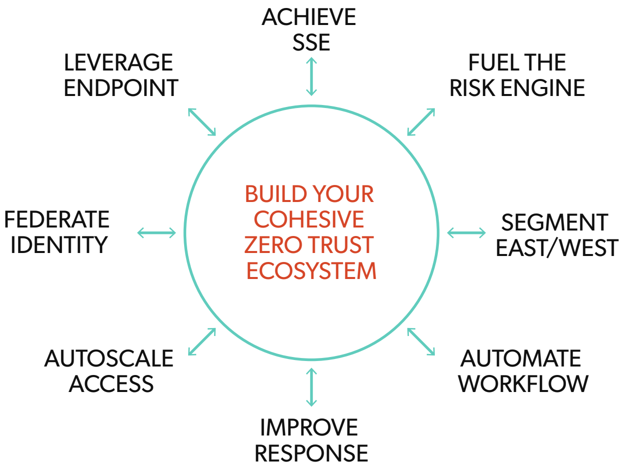
## Extensibility to Maximize Investments with Unparalleled Interoperability

Appgate SDP maximizes existing or future investments in other security and business technologies so organizations can create a cohesive ecosystem and dynamically build security into existing processes and business workflows. This comprehensive interoperability is enabled by extensible 100% API-first Zero Trust platform services and an API call-based GUI to reduce complexity for admins, engineers and operators.

Far-reaching interoperability benefits include:

- To and from context-enriched data flow to make processes more efficient between Appgate SDP and other security and business systems
- Integration into business workflows
- Ability to quickly react to issues and threats detected by other systems like IDS/IPS, EDR or NAV/EUB
- Deploy as code to programmatically establish new Controllers, Gateways or Connectors when required, new VPCs are established, or new accounts activated, etc.
- Configure as code to programmatically update or create policy, entitlements, conditions, sites, IdP, MFA, and much more to the SDP collective
- Built-in risk engine customizes risk rules with "no code" integrations to prominent IT, business and security systems

### Zero Trust Platform Services



Robust Bi-Directional APIs

Connected Cloud-Delivered Services

Customizable Built-in Risk Engine

Easy to Deploy Codeless Integrations

LEARN MORE ABOUT THE ZERO TRUST PLATFORM SERVICES

## Appgate SDP: Industry Validated, Government Approved, Enterprise Trusted

Appgate SDP, the industry-leading Zero Trust Network Access solution, has a long list of analyst accolades, federal agency working relationships and customers of all sizes that trust it to secure access across their complex hybrid environments, harden their cyber defenses, cut line-item expenditures and boost operational efficiencies.

FORRESTER®

Named a Leader in the latest Forrester New Wave, positioned highest for current offering

Gartner.

Peer Insights 4.8 out of 5 stars

Representative Vendor, ZTNA Market Guide

CSA cloud security alliance®

Aligned to Software-Defined Perimeter (SDP) Reference Architecture

NCCoE

National Cybersecurity Center of Excellence

NIST SP800-207 Collaborator Zero Trust Architecture Project

U.S. DEPT OF DEFENSE

DoD Authorized to Operate & CNAP

Aligned to DoD Reference Architecture

DXC TECHNOLOGY

Secureworks®

chewy

FINRA.

ManTech. Securing the Future

**Fortune 10** Oil & Gas Company

**Fortune 500** Bank

**Fortune 500** Health Insurance Company

**Fortune 500** Chemical Company

## About 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. Appgate helps organizations and government agencies worldwide start where they are, accelerate their Zero Trust journey and plan for their future. Learn more at appgate.com.

appgate

©2023 Appgate. All Rights Reserved. The Appgate logo and certain product names are the property of Appgate.
All other marks are the property of their respective owners.