



Definitive Guide to Software-Defined Perimeter

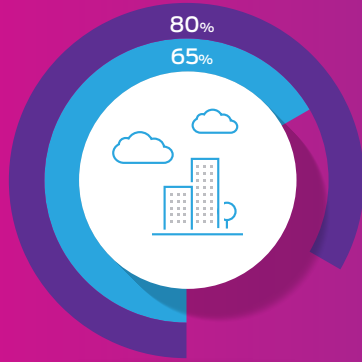
Guide Contents

- 03 Today's Network Security Reality
- 05 The Problem with Traditional Network Security
- 06 Time for an Identity-Centric Approach – Software-Defined Perimeter
- 08 Technical Architecture
- 14 AppGate SDP
- 19 Use Case – Secure AWS Resources
- 20 Use Case – Dramatically Reduce the Attack Surface
- 21 Conclusion
- 21 About Cyxtera

This Definitive Guide to Software-Defined Perimeter is intended for a CIO, head of IT and network security professional.

Today's Network Security Reality

IT has never been more diverse and distributed. Enterprise IT has entered a period of hybridization and diversification – IT is running in more locations, on more platforms and with more diversity of models than ever before.



By the end of 2018, over **65% of all IT assets** will be offsite.

IDC, FutureScape: Worldwide Cloud 2016 Predictions — Mastering the Raw Material of Digital Transformation

Yesterday's security technologies have not kept pace with today's evolved security challenges. Twenty years ago, organizations had centralized IT with a physical perimeter. Today, it is almost impossible to secure corporate infrastructure using technologies that have not fundamentally improved for over two decades.

Historically organizations built hardened perimeters with firewalls, VPNs and NACs to protect their internal networks. However these antiquated tools (firewalls, VPNs and NACs) are complex and expensive to operate.

Firewall rules are binary and static. They simply ask, "Should this IP block have access to this network (Y/N)?" And that's not enough.



Today's IT showcases a disparity between users and network resources. Applications are in globally-distributed public clouds, running on third-party managed hosting platforms, collocated in data centers, and corporate data centers. Yet users are mobile and distributed, connecting to business systems from home offices and airport lounges on personal and corporate devices. And these users aren't just our employees.

We live in a connected, hybrid world, where our systems and users need simple – and secure – methods of connecting and interacting with customers, partners and vendors.

The perimeter doesn't exist. It's gone. Perimeter security must begin elsewhere, namely with users.



“ Legacy, perimeter-based security models are ineffective against attacks. **Security and risk pros must make security ubiquitous throughout the ecosystem.** ”

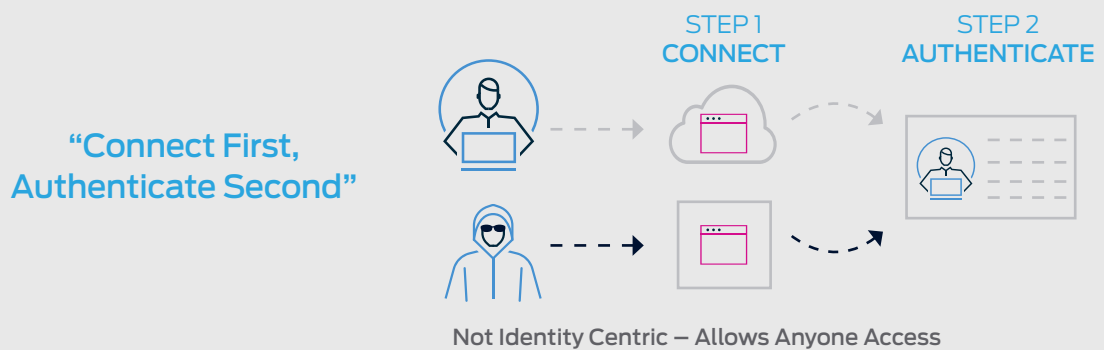
Forrester

The Problem with Traditional Network Security

Traditional network security approaches are failing to adequately protect organizations today. Trust is presumed and misplaced. It's an outdated model predicated on obsolete isolation of users and networks.

The fundamental reason is that TCP/IP – which was designed in a safer and more open world – is based on implicit trust, with a “connect first, authenticate second” approach. In today's hyper-connected and highly adversarial threat landscape, this approach puts organizations at risk, and has enabled far too many successful breaches.

Traditional TCP/IP – based on “implicit trust”



The TCP/IP approach results in:

- Servers exposed to reconnaissance scans
- Unauthenticated users able to exploit servers
- DDoS attack vulnerabilities
- Unauthorized users consuming unauthorized server resources
- Inherent over-entitlement
- Broad lateral attack surface

TCP/IP implicit trust is akin to someone knocking on the **front door of a house**, letting the person through the front door, and only **after** they are in asking who they are and what **they** need.

Time for an Identity-Centric Approach – Software-Defined Perimeter

Today's IT reality requires flexible and adaptive security, one centered on a user's identity instead of the various networks that they consume. This approach is called a Software-Defined Perimeter.

A Software-Defined Perimeter dynamically creates one-to-one network connections between users and the data they access. It addresses the perimeter-less enterprise.

A Software-Defined Perimeter is built on three core principles:



1. Identity-centric

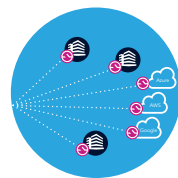
It is designed around the user, addressing the perimeter-less enterprise. Users are authenticated BEFORE they are allowed to connect to a network.



2. Zero-Trust

It enforces the “zero-trust model” so that anyone attempting to access a resource must authenticate first. All unauthorized resources are invisible. This applies the principle of least privilege to the network and completely reduces the attack surface.

By default, users are not allowed to connect to anything – opposite of traditional corporate networks, where once a user is given an IP address, they have access to everything it has access to. Instead, zero trust ensures that once proper access criteria is met, a dynamic one-to-one connection is generated from the user's machine to the specific resource needed. Everything else is completely invisible.



3. Built like cloud, for cloud

The Software-Defined Perimeter is built for the cloud, and like the cloud. It has no centralized network chokepoint. It's completely distributed and as scalable as the internet itself. A Software-Defined Perimeter is engineered to operate natively in cloud networks. It's not simply a modified perimeter-based device that's been placed into a virtual machine. Plus, it's completely compatible with existing corporate networks.

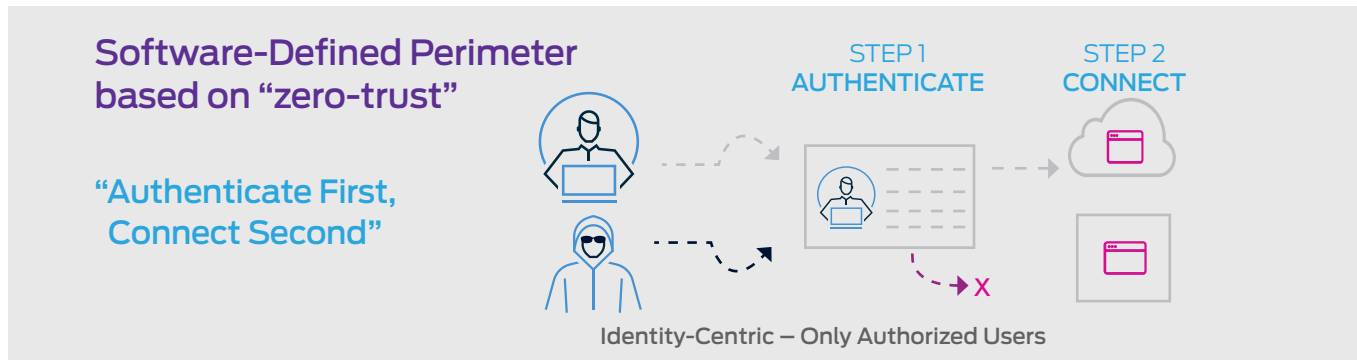


By 2021, **60% of enterprises will phase out network VPNs** for digital business communications in favor of software-defined perimeters.

Gartner, [It's Time to Isolate Your Services from the Internet Cesspool](#)

"Authenticate-First, Connect Second"

The basic premises of a Software-Defined Perimeter is built on an "authenticate first, connect second" approach. Unlike a traditional network that connects various roles or groups to a network segment and then relies on application level permissions for authorization, a Software-Defined Perimeter creates individualized perimeters for each user, allowing for much more fine grained access control.



As a user's situation changes, the individualized security perimeter changes. Software-Defined Perimeters control access to network resources that are across hybrid environments – in a corporate datacenter or in the cloud – meaning that consistent access policies can be enforced.

This "authenticate first, connect second" approach, ensures that only authorized users can connect to network resources. This reduces the attack surface and significantly improves security:

- All resources are invisible to potentially dangerous reconnaissance
- Only authenticated users can connect
- DDoS attacks are ineffective
- Unauthorized users cannot impact servers

Using the front door example, the Software-Defined Perimeter zero-trust approach takes the person that is knocking at the front door, confirms who the person is and what it is that they want/need, and then opens the door to let them inside of the house. Once inside the house, they can only access those rooms that they need, and nothing else.

History of a Software-Defined Perimeter

The principles behind Software-Defined Perimeters are not entirely new. Multiple organizations within the Department of Defense (DoD) and Intelligence Communities (IC) have implemented a similar network architecture based on authentication and authorization prior to network access.

Typically used in classified or high-side networks (as defined by the DoD), every server is hidden behind a remote access gateway appliance to which a user must authenticate before visibility of authorized services is available and access is provided.

A Software-Defined Perimeter leverages the logical model used in classified networks and incorporates that model into standard workflow. Software-Defined Perimeter's maintain the benefits of the "need-to-know" model, but eliminates the disadvantages of requiring a remote access gateway appliance. Further, Software-Defined Perimeters require endpoints to authenticate and be authorized first before obtaining network access to protected servers. Then, encrypted connections are created in real time between requesting systems and application infrastructure.

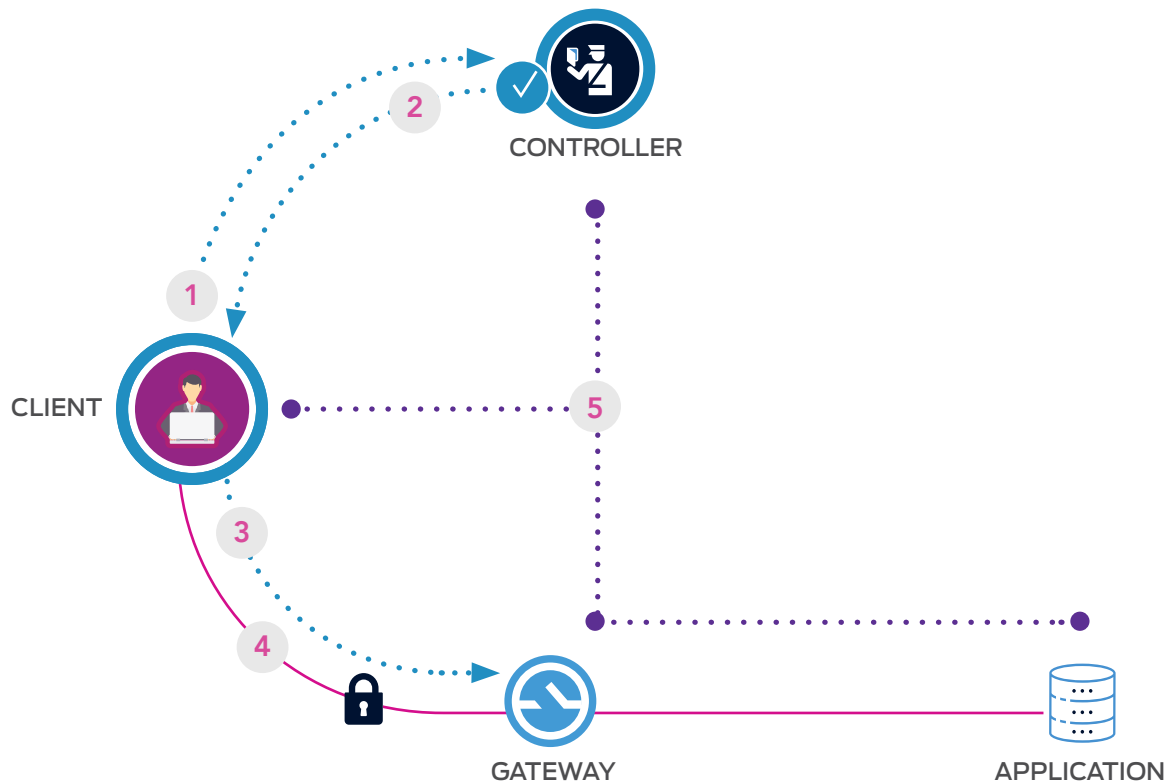
Technical Architecture

Core Components of a Software-Defined Perimeter

A Software-Defined Perimeter (SDP) architecture is made up of three main components:

- A Client – runs on each user's device
- A Controller – where users authenticate, policy is applied, and users are evaluated. The Controller issues tokens granting each user their individualized network entitlements
- A set of Gateways – brokers access to protected resources

How the Architecture Works



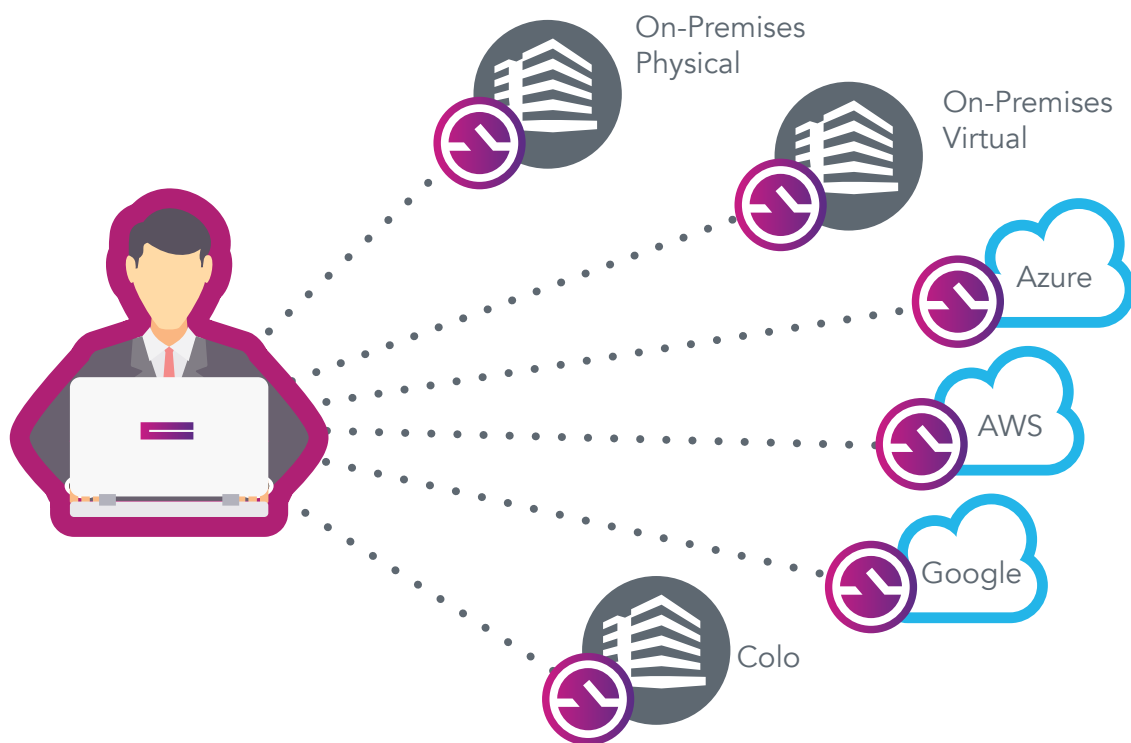
- 1. Using Single-Packet Authorization, client makes access request to controller.** Client devices authenticate to the Controller, which evaluates credentials, and applies access policies (based on the person, environment and infrastructure).
- 2. Controller checks context, passes Live Entitlement to client.** The Controller returns a cryptographically signed token back to the Client, which contains the authorized set of network resources.
- 3. Using SPA, client uploads Live Entitlement, which gateway uses to discover applications matching the user's context.** When the user attempts to access a resource – for example by opening a web page on a protected server – the network driver forwards the token to the appropriate cloaked Gateway, which then applies additional policies in real time – for example, to control access based on network location, device attributes, or time of day. The Gateway may permit access, deny access, or require an additional action from the user, such as prompting for a one-time password.
- 4. Dynamic Segment of One network is built for this session.** Once granted, all access to the resource travels from the Client across a secure, encrypted network tunnel, and through the Gateway to the server. Access is logged through the LogServer, ensuring that there's a permanent, auditable record of user access.
- 5. Continuously monitors for any context changes, adapts Segment of One accordingly.**


Software-Defined Perimeter in the Cloud

Securing access to public cloud workloads isn't easy. Static IP-based firewalls aren't working. They don't provide granular access control to cloud resources. Access control with static IP addresses and port mapping simply doesn't scale.

SDP provides consistent security across hybrid and multi-cloud environments. On-premises, colocation and public cloud instances can all have the same consistent identity-centric security policies and processes reducing complexity and ensuring adherence to all of the security controls for the enterprise. SDP is much more advanced than using direct connect which enables an entire internal IP range to access cloud network which extend vulnerabilities that exist on current internal networks.

SDP is better equipped to deal with an elastic environment by dynamically adjusting to new cloud server instances. CSA says that "SDP is the right way for enterprises to meet their security goals in today's complex environments."





“ Most organizations will have a complex and heterogeneous IT environment for the foreseeable future. Rather than looking at this as a problem to be eliminated, security teams need to **embrace this richness – and its associated complexity – as a part of doing business.** ”

CSA, Software Defined Perimeter for Infrastructure as a Service

Why Select SDP as a Security Solution

Businesses are constantly evaluating their security vision and strategy, based on numerous factors. Companies should consider a Software-Defined Perimeter solution as part of their overall security strategy to address some of the following reasons.

✓ Compliance Considerations

A Software-Defined Perimeter solution will address many of the common controls enterprises are trying to address. Software-Defined Perimeters are ideal for reducing the scope of an audit by limiting the visibility of systems on networks outside of the protected network. Reducing the scope of an audit will often decrease the overall cost and complexity of the engagement as there are fewer systems to evaluate. SDP also provides for a set of unified security policies and controls across the various on-premises and public environments. This decreases the management workload and decreases the audit variables that need to be tested and evaluated.

✓ Zero-Trust Security Model

Many enterprises are revising their corporate security strategy to reflect the zero-trust model. A Software-Defined Perimeter solution implements the key concepts of zero-trust in a single solution. According to Forrester, there are three fundamental concepts of our Zero Trust Model:

- Ensure all resources are accessed securely regardless of location
- Adopt a least privilege strategy and strictly enforce access control
- Inspect and log all traffic

A Software-Defined Perimeter solution can address these concepts by securing access to all workloads, providing granular access based on identity-centric policies, and logging all access and traffic on protected networks.

✓ Migration to the Cloud

For enterprises looking to migrate workloads to a cloud environment, a Software-Defined Perimeter solution provides a controlled path to migration. Enterprises are not forced to choose between an “all-or-nothing” approach, as Software-Defined Perimeters allow the organization to cherry pick which workloads to migrate and which ones to keep internally. After an evaluation period, moving high value or protected workloads becomes very easy and is seamless to the end user. All the while, the security administrators are able to maintain a single set of security policies – before, during and after the migration – ensuring those workloads maintain their security.

✓ **Augment Existing Security Solutions**

One of the key capabilities with the Software-Defined Perimeter specification is the ability to integrate and enhance the existing processes and tools used by the enterprise for networking and security. Many solutions are all-or-nothing, often defined as “replace,” requiring the enterprise to uproot existing installations in favor of the new solution. SDP is different – the specification calls for the ability to integrate with most types of enterprise class security and networking APIs. It can also consume calls and logs from existing solutions to increase security processes and functions.

✓ **Identity / User-Based Security Strategy**

The Software-Defined Perimeter security model is based on the individual user, instead of the more traditional IP addresses and devices. SDP can be used at the foundation of shifting an enterprise’s security strategy to an identity-centric model, replacing antiquated models that center primarily on device security or IP source – destinations. SDP can also align processes – many of which are user / employee based – with the company’s security infrastructure. This can lead to increased business agility and growth without compromising the company’s security.

✓ **Simplifying Security Operations**

Today’s every changing cloud environments require a security solution that is flexible to address constant change while maintaining a consistent level of security. A Software-Defined Perimeter solution can dynamically adjust as the enterprise environment changes, while maintaining constant, user-based security and access. SDP solutions also can automate many of the changes that are required with a changing environment without security administrator intervention. Simplifying security operations with SDP can allow for the rapid changes that come with business transformation without sacrificing security and compliance goals.



“ An SDP deployment can be a catalyst for changing how network security is accomplished across the entire enterprise – **both on-premises and cloud.**”

Cloud Security Alliance (CSA)

AppGate SDP

Cyxtera's Software-Defined Perimeter solution is AppGate SDP. It is the most comprehensive SDP solution providing an adaptive, identity-centric full network platform built for the hybrid enterprise. AppGate SDP is cloud agnostic and hybrid native, deeply integrates with business systems, resilient and massively scalable. Its *segment of one* is designed to reduce the attack surface and audit scope. The benefit is improved security that aligns access controls with your business and substantially reduces cost and complexity.

Meet Jim

Should Jim have access to the production SAP database server?

A Software-Defined Perimeter uses Live Entitlements to evaluate a user's situation before granting access:

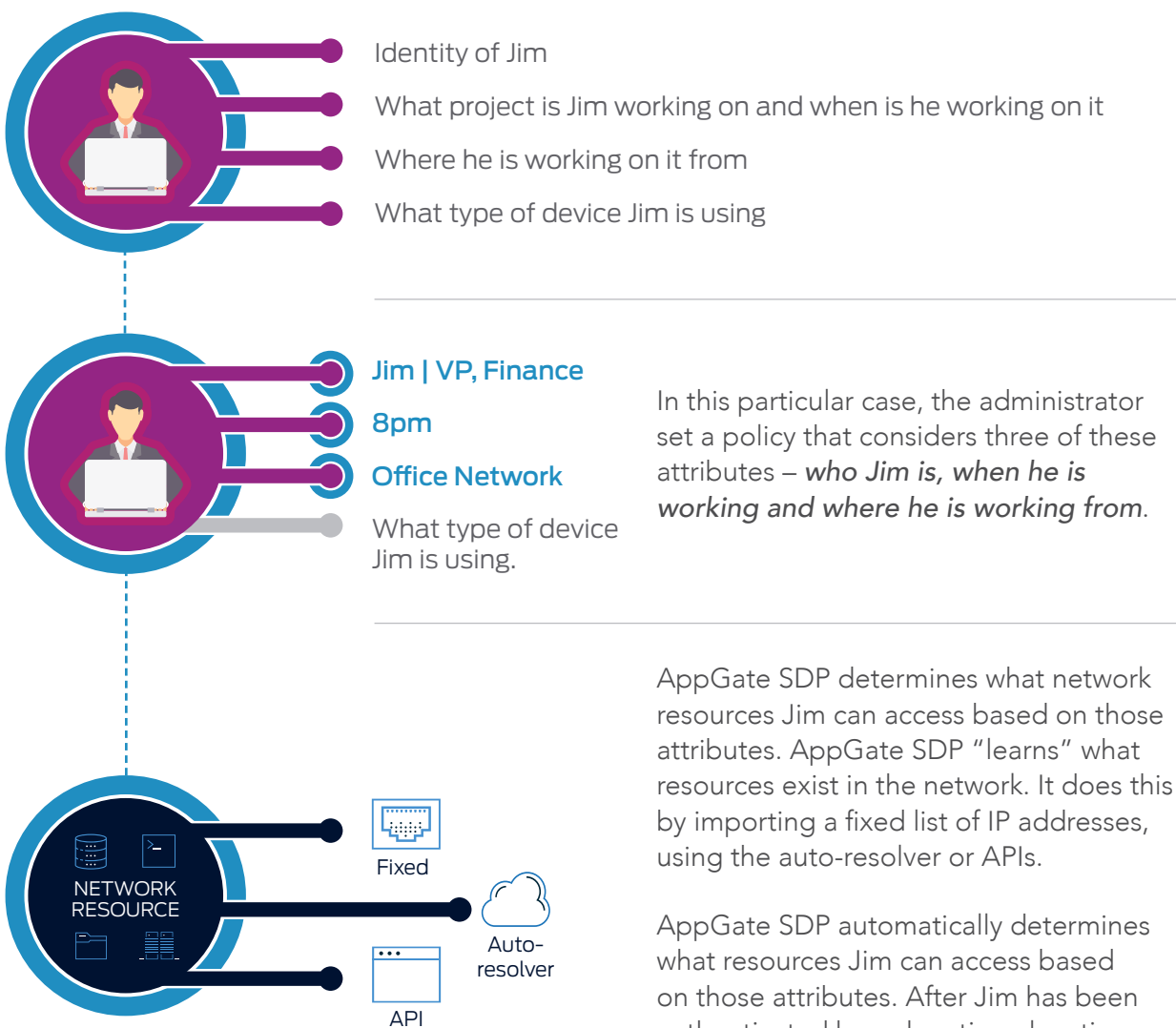


- Is Jim's machine patched?
- What's the current security posture?
- Where is he?
- What time is it?
- What project is Jim working on?
- What are his SAP credentials?

Live Entitlements

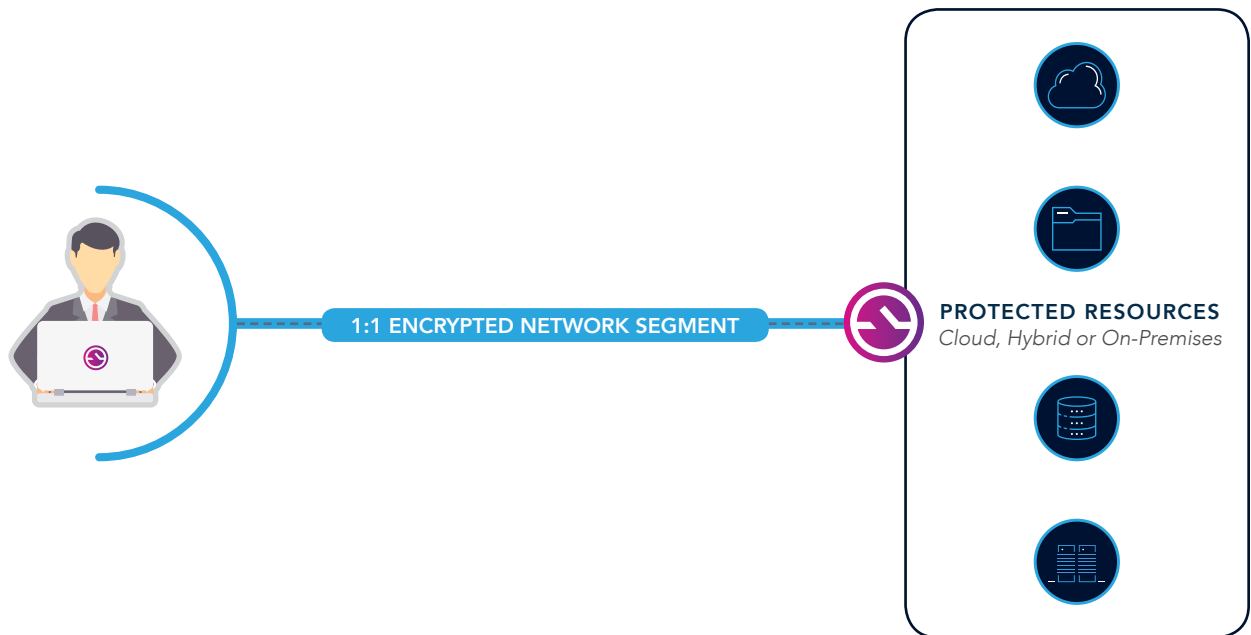
AppGate SDP replaces static access rules with Live Entitlements. Live Entitlements are dynamic, context-aware security attributes that confirm user identity while providing the flexibility necessary to adjust to changing variables, such as environmental / infrastructure changes, user location, time of day, and workload sensitivity. Live entitlements maintain security without manual interactions, often needed when modifying traditional static firewall rules. In AppGate SDP, Live Entitlements automatically update based on monitoring changes to the user context (such as an opened service ticket) or changes associated with the dynamic nature of a public or hybrid cloud environment. Further, Live Entitlements are extensible and scriptable. As hybrid IT environments change, this feature helps to remove human error.

Live Entitlements evaluate whether Jim can access the production SAP server database based on a variety of criteria, such as:



Segment of One

Unlike a traditional network that connects various roles or groups to a network segment and then relies on application level permissions for authorization, AppGate SDP creates individualized perimeters for each user, allowing for much more fine-grained access control and giving individual users access to only what they need to do their jobs. AppGate SDP provides this access control with a real-time understanding of policy.



AppGate SDP ensures that all endpoints attempting to access a given infrastructure are authenticated and authorized prior to being able to access any resources. Once the user initiates a session with an authorized resource, AppGate SDP creates an encrypted tunnel, allowing traffic to flow only from the user device to the protected resource. This creates a *segment of one* and makes the rest of the network completely invisible to the user - including the system itself. All resources, including AppGate SDP, are completely dark to all unauthorized users. Gateways and controllers are completely cloaked so they cannot be probed, scanned, or attacked. So, a port scan of the system would show NO open ports, reducing the network attack surface by preventing network reconnaissance and limiting lateral movement on the network.

Even while the session is open, Live Entitlements can detect changes in the posture of the user, his or her environment and infrastructure, including changes in the cloud, and automatically adjust access privileges. AppGate SDP may then force a step-up authentication or terminate the session completely based on this newly detected change in posture or context.

Ringfence – Single-Packet Authorization

AppGate SDP ringfences the user's device. This ringfence isolates and protects the user device from all inbound connections. It's useful for deploying devices onto trusted networks. Access to internal resources can be granted without concern about malicious users on the local network. Local outbound traffic (DNS, etc) is untouched.



AppGate SDP itself is safe from prying eyes. Single-Packet Authorization cloaks infrastructure so that only verified users can communicate with the system. It's invisible to port scans and cryptographically hashed as further defense.



How SPA Works

Clients create an HMAC-based One Time Password based on a shared secret (seed), and submit this to the SDP Controller and Gateway as the first network packet sent during connection setup. (It's also used for Gateway-Controller connection setup.) Because the SDP Controller and Gateway reject invalid packets (presumably from an unauthorized user), they can prevent the establishment of TCP connections from unauthorized users or devices. Because invalid clients can be distinguished by analyzing a single packet, the computational load incurred by the SDP controller and gateway are minimal.

AppGate SDP Overcomes Traditional Network Security Challenges

AppGate SDP overcomes the problems many traditional network security solutions face including firewalls, VPNs, NAC for example.



Firewalls are static and inflexible.

Firewalls are configured and forgotten because once set up, IT administrators do not want to change the firewall because it's usually a significant change ticket. They also look at port and addresses, not users. They're not designed to address specific users, which is why admins are always adding exceptions and holes for access. AppGate SDP is identity-centric adapting to the context of the user – where they are, what device they are on, etc. – so it overcomes the static and inflexible nature of firewalls.



VPNs extend vulnerabilities across hybrid environments.

VPNs authenticate to everything, are perimeter based security, static and unintelligent and provide over-entitled access. Companies often attempt to control access by having remote employees VPN into the office network, and then access hybrid resources. However, this approach effectively extends all of the vulnerabilities across hybrid environments allowing malicious users to move laterally on-premises or in the cloud, causing damage all along the way.

Further, in the past, credential theft of enterprise VPN access has led to data loss at many organizations. Since VPNs typically grant users broad access to an entire network, it is one of the weakest points of failure with respect to weak credential management.

In contrast, AppGate SDP does not allow broad network access and limits the access to only those hosts explicitly allowed. This limits the threat in the event of credential theft, making the security architecture much more resilient towards weak identity, credential and access management.



NAC solutions do not provide fine-grained access control over specific resources and don't extend to the cloud.

Network access control (NAC) is a method of bolstering network security by restricting the availability of network resources to endpoint devices. But NAC was designed to work inside the perimeter – build a perimeter around the internal network, verify users, and once in the door users gain full access to the network or at least a large portion of the network.

AppGate SDP offers an individualized, dynamically adjusted network segments for each user and user session – a *segment of one* to secure enterprise networks with fine-grained control and extend over hybrid environments.

AppGate SDP Addresses Cyber Attacks, Compliance and Migration to Cloud

SDP also overcomes challenges around specific types of cyber attacks, compliance and scope reduction.



Data breaches

AppGate SDP helps by reducing the attack surface of publically exposed hosts by adding a layer of pre-authentication and pre-authorization. This ensures a “least privileged access” model of security for servers and network and thereby reduces many attack vectors of data breaches.



Third party credential theft

OneLogin was a recent example where hackers obtained a set of AWS keys to gain access to AWS APIs. Hackers then created several instances for additional reconnaissance and gained access to databases containing user information, including user keys. AppGate SDP uses dynamic and contextual condition checking for multifactor authentication and integrates with existing enterprise SIEM solutions to provide immediate security when changes occur – user location, time of day, device hygiene. It therefore can prevent data breaches resulting from third party credential theft.



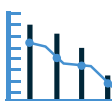
Malicious insiders

AppGate SDP will limit the ability of a malicious insider to cause damage. A properly configured SDP system will have access policies that limit users to only those resources required to perform their business function. Therefore, all other resources will be hidden.



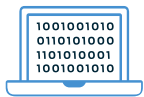
Compliance

AppGate SDP offers auditable, uniform policy enforcement across hybrid systems and dramatically reduces audit-preparation time: no need to correlate IP addresses to users.



Scope reduction

Compliance costs continue to rise, and one of the simplest ways to reduce the cost of compliance is by reducing the number of systems and instances that are considered in the scope of an audit. AppGate SDP can dramatically reduce audit scope by removing entire networks – and the systems connected to them - from being seen by audit analysis tools. When those systems are removed from the scope of the audit, the level of effort significantly decreases, and generally the cost of the audit evaluation will decrease.



DDoS attacks

DDoS attacks are one of the most common forms of cyber attack, with the number of global DDoS attacks increasing. AppGate SDP eliminates DDoS attacks by making network resources invisible, preventing bad actors from seeing anything to attack.



Micro-segmentation

AppGate SDP provides for micro-segmentation through assigning fine grained security policies to individualized users or groups that are authorized to gain access to the workload or protected resource. Micro-segmented networks are becoming a common regulatory compliance requirement, and implementing the network security design created by using AppGate SDP satisfies and exceeds most of these requirements.



Cloud migration and integration

AppGate SDP creates a controlled migration path for organizations migrating their protected workloads to a cloud environment. AppGate SDP applies consistent security policies across the organizations various environments – from on-premises to cloud-based workloads and infrastructure.

Software-Defined Perimeter Use Cases

Use Case – Secure AWS Resources

This financial services regulatory agency analyses massive volumes of financial data across multiple markets to detect potential fraud, overseeing up to 75 billion market transactions every day.

The organization, which performs its massive Big Data analysis on AWS, needed to ensure secure access and compliance to these resources. It required a solution that automated DevOps user access to AWS instance deployment without breaking compliance, reduced compliance data collection and report preparation and isolated production QA and development.

The organization built an automated framework with a user-facing portal – connected with their Identity Management system – which the DevOps team used to instantiate new AWS EC2 instances. From a security and compliance perspective, they required that the portal generate a unique SSH key for each instance. They also required that each user's network access be restricted to just those resources for which they had valid credentials – a challenge that traditional network security solutions were unable to meet.

AppGate SDP enabled the organizations to adopt a Software-Defined Perimeter that delivered:

Identity-centric, highly granular access control

Using AppGate SDP, the organization gained an identity-centric, highly granular access control solution. Every user obtains a dynamically adjusted network perimeter that's individualized based on their specific requirements and entitlements. This ensures that the context of the user and the device is evaluated in real-time before AppGate SDP provides network access to the user-authenticated instances and services in the AWS environment.

Real-time access changes

With simple policies in place, network access automatically adapts in real-time to changing conditions on the client side as well as on the cloud infrastructure side. Every new instance that is added or removed is automatically traced and added or removed from the user's access entitlements, without needing to change policies. AppGate SDP was easily integrated with their portal, automatically adjusting each user's network access when new instances were created. This simplifies and enhances security, while ensuring development teams can be highly productive.

With AppGate SDP, their network system was automated, driven by simple rules, and logged from compliance and audit purposes.

Full audit trail for compliance

AppGate SDP also overcame the organization's compliance challenges. It applies policy enforcement to all instances when deployed, solving their SSH key management issue. Policies are automatically adjusted based on user attributes. AppGate SDP provides detailed logging of user access and activities to efficiently feed audit request data needs and reduces audit scope.

Use Case – Dramatically Reduce the Attack Surface

AppGate SDP can have a dramatic and immediate effect on an organization's security posture.

A NYC based hedge fund had its IT environment spread across its own data center and a managed hosting provider. As many companies do, its network security was based on traditional, perimeter based technologies like firewalls and VPNs. The new CISO wanted an outside baseline assessment to determine the firm's vulnerabilities.

A security consultant was given a single VPN credential, allowing them to connect to the corporate network. From there they were able to do a simple port scan, and what was visible to them would be a cause for concern for any CISO. Based on scanning the network while connected as an everyday VPN user, the consultant was able to see an astounding 4,300 network services across their internal and Wi-Fi networks. They were also able to see network services – both theirs and other customers – inside the hosting provider's network. This massive attack surface quickly became the number one priority for the CISO to correct. And while not as urgent, the CISO wanted to report on what users accessed what systems – a challenge with future audits.

To quickly address the security risk, the firm implemented AppGate SDP. AppGate SDP integrates into and leverages existing identity stores, and leverages simple, common logic policies allowing the hedge fund to fully deploy AppGate SDP in less than 3 weeks. Once implemented, the consultants ran the same port scans as an individual user – and were now only able to see a single network service.

AppGate SDP dynamically created a secure *segment of one* to reduce visibility inside the network. In this case, it was able to reduce the network attack surface from 4300 to 1! Based on AppGate SDP's user centric approach and enforced logging capabilities, the firm was able to eliminate their audit shortcomings as well.

Conclusion

It's time to move away from traditional security solutions and look to a Software-Defined Perimeter. By implementing it throughout hybrid environments, organizations will have an identity-centric, zero-trust, hybrid cloud solution.

This definitive guide outlines the benefits of a Software-Defined Perimeter alongside details into the market leading solution, Cyxtera AppGate SDP, an identity-centric, security solution built for today's hybrid enterprise. AppGate SDP protects critical data from internal and external threats, while significantly lowering costs.

About Cyxtera

Cyxtera Technologies combines a worldwide footprint of best-in-class data centers with a portfolio of modern, cloud – and hybrid-ready security and analytics offerings – providing more than 3,500 enterprises, government agencies and service providers an integrated, secure and resilient infrastructure platform for critical applications and systems. For more information, visit www.cyxtera.com.



© 2017 Cyxtera Technologies, Inc. All Rights Reserved.
The Cyxtera mark and name are the property of Cyxtera.

Contact Us

+1.855.699.8372

+1.305.537.9500

sales@cyxtera.com

www.cyxtera.com