Cryptzone™

DATASHEET

AppGate for SAP

Why AppGate is Needed

You run your business on SAP or SAP HANA, and like most organizations any downtime would be both disruptive and expensive. Your business needs to strike a balance between keeping business users productive and ensuring the security of your SAP system.

This is a difficult challenge, especially given the requirement to keep SAP up to date with all the latest security patches. And, as recently patched SAP and SAP HANA vulnerabilities show, there are real risks if these systems are exposed to unauthorized users on the network and internet. According to a 2016 Ponemon Institute survey[1], two out of three SAP platforms were likely breached between 2014 and 2015. That's because traditional perimeter-based security approaches do not provide real-time context-based protection for on-premises, hybrid or cloud-based SAP environments from modern cyber-threats.

WHAT INDUSTRY EXPERTS ARE SAYING ABOUT SDP

Gartner

"SDP enables organizations to provide people-centric, manageable, secure and agile access to networked systems. **It is easier and less costly to deploy** than Firewalls, VPN concentrators and other bolt-in technologies."

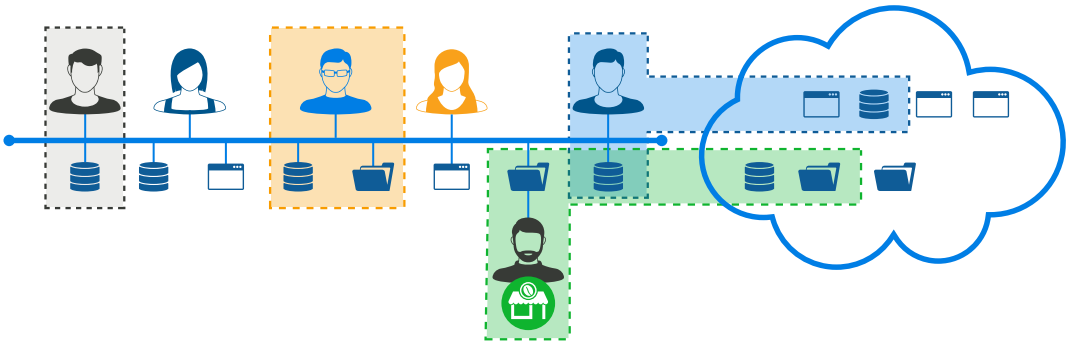
FORRESTER

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

It is more important than ever to know who is connecting from where and how to enforce the correct security criteria before granting network access, the point being if they can ping it they can hack it.

What can you do? Gartner and Forrester advocate customers investigate a new security paradigm called a Software-Defined Perimeter (SDP). This new security architecture provides strong network access control with real-time dynamic user-centric access policies. With this approach, you can define simple policies which distinguish and control business, developer, and admin access to the SAP application and infrastructure, without impeding user productivity. And, because access is controlled at the network level, it completely cloaks the whole SAP environment from all unauthorized users – significantly reducing the attack surface.

What Does an SDP Look Like?



AppGate

With AppGate, every organization can cloak and ultimately protect on-premises, hybrid and cloud-based SAP applications and infrastructure. AppGate, a Software-Defined Perimeter solution, is a distributed, real-time dynamic secure access platform for simplified fine-grained user-based access control. It draws in many claims, from device posture queries and API queries to user context which are then used to dynamically create a network *segment of one* that's tailored for each unique user session. The security platform hides all network resources – servers, services and applications – except those that the user is authorized to see and prevents pivoting between different systems. AppGate is an enterprise-ready solution with platform maturity enabling production-ready deployment in front of the SAP environment, whether on-premises, hybrid or cloud.

BENEFITS

- Makes SAP assets invisible to any unauthorized users.
- Single, centralized logging of all authorized SAP network traffic, per user and per device which can also be pushed into SAP's Enterprise Threat Detection software for deeper analysis.
- Proactively Secure SAP and HANA systems from malicious insiders, over-privileged users, and compromised 3rd-party access
- Drives consistent access policies and user control across on-premises, hybrid and cloud-based SAP landscapes.
- Integrates with existing SAP single sign-on, identity and threat solutions such as SAP GRC and Enterprise Threat Detection.
- Non-authorized services and resources are invisible, reducing attack surfaces by as much as 98%
- Reduces cost, complexity and effort for configuring user access to on-premises, hybrid and cloud hosted SAP HANA instances

Direct integration with SIEM and IDS systems like SAP Enterprise Threat Detection builds bridges among the security stack. The result is a security platform able react to real-time threats and remove user access to secured assets by a simple API call. What makes AppGate different is its distributed, scalable architecture designed for on-premises, hybrid and dynamic cloud environments. Its distributed architecture features three services:

- Controller – the central authentication and token-issuing service. It applies policies and determines access rights for clients
- Gateway – a distributed, dynamic firewall through which network traffic flows. It consumes tokens and enforces access policies
- LogServer – provides secure logging services

How it Works

Client devices, such as laptops, desktops, or mobile devices, use the AppGate network driver to authenticate to the Controller, which evaluates credentials, and applies access policies. The Controller returns a cryptographically signed token back to the client, which contains the set of network resources – at a server and service level – that the user is authorized to access, subject to further conditions.

When the user attempts to access a resource – for example by opening up a web page on a protected server, the network driver forwards the token to the appropriate Gateway, which applies policies in real-time – for example, to control access based on network location, device attributes, or time of day. The Gateway sets routes from a fully-rendered firewall ruleset based on the user's entitlement list for each Gateway and may permit access, deny access, or require an additional action from the user, such as prompting for multi-factor authorization.

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. AppGate can also immediately block malicious traffic and feed alerts into SAP's Enterprise Threat Detection (ETD) or IDS for analysis and response.

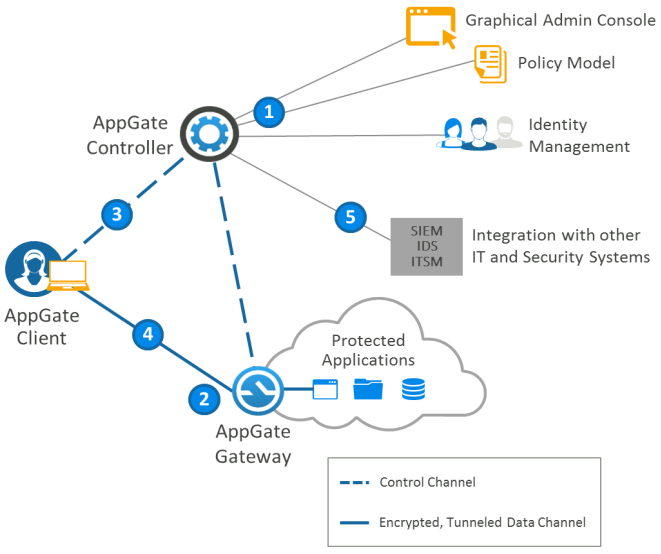
Scenarios

AppGate is used today in these SAP environments:

- To secure the SAP application
- To secure the SAP infrastructure
- To secure SAP HANA and cloud instances

SDP in Action

1. Controller uses existing Identity Management systems. Controller is an authentication point and policy store System administered via graphical admin console.
2. Gateways protect cloud and network resources. Application network traffic passes through Gateway.
3. Clients securely onboarded, authenticate to Controller, communicate with mutual TLS.
4. Clients access resources via Gateway
   - Mutual TLS tunnels for data
   - Real-time policy enforcement by Gateway
5. Controller can enhance SIEM and IDS with detailed user activity logs.
   Controller can query ITSM and other systems for context and attributes to be used in Policies.



Cryptzone™

Americas +1 888 272 2484 | EMEA & APAC +44 118 900 1236 | www.cryptzone.com | sales@cryptzone.com

[1]Uncovering the Risk of SAP Cyber Breaches by Ponemon Institute LLC