AKAMAI SOLUTION BRIEF

Securing SAP S/4HANA with Akamai Guardicore Segmentation

The enterprise infrastructure of clouds, networks, and the applications that power them are growing increasingly complex. Applications hosted on multiple forms of infrastructure can be more difficult to manage and secure. Leading enterprise resource planning (ERP) providers such as SAP recommend network zoning, or segmentation, to minimize or eliminate unauthorized traffic to and from the applications. Akamai Guardicore Segmentation offers a software-based approach to creating network zones, implementing and enforcing granular firewall controls, and managing your application security in the context of your overall environment. This platform can be leveraged to provide enterprises with security services to solve their SAP security requirements.

Background

Today's enterprises manage and operate an average of 1,061 applications (source: 2023 Connectivity Benchmark Report by MuleSoft in collaboration with Deloitte Digital). Leading enterprises depend on many of these applications provided by SAP to enable business operations, ERP, and more. SAP deployments can include dozens of applications, a core ERP platform, servers, and proprietary operating systems, making them complex in nature with many potential points of vulnerability. As the beating heart of many enterprises, the SAP infrastructure must be properly secured to protect sensitive data and ensure business continuity.

While SAP does offer a few standard security capabilities, these tools are only part of the equation when it comes to achieving holistic application security. Organizations have been historically frustrated when trying to use legacy firewalls to implement security use cases, such as environment separation, application ringfencing, and attack surface reduction. Faced with the technical limitations of legacy firewalls, many organizations are now seeking alternative solutions to solve their application visibility challenges, and to understand their associated network dependencies.

SAP solution compatibility

This solution brief applies to the following SAP products:

- **SAP trading platform integration**
- **SAP S/4HANA Cloud, public edition, system extension**
- **SAP S/4HANA for central finance**
- **SAP S/4HANA Cloud for group reporting**

- **SAP S/4HANA Cloud**
- **SAP CRM**
- **SAP S/4HANA Enterprise Management**

Following SAP's guidance

SAP's technical documentation offers insight into the types of visibility and security solutions that can help.

Specifically, network segmentation is embraced by SAP and recommended as a key solution set to fully secure their applications and infrastructure. The SAP HANA Security Guide for SAP HANA Platform shares the following guidance for improving network and communication security of SAP applications:

"We recommend that you operate the different components of the SAP HANA platform in separate network zones.

To prevent unauthorized access to the SAP HANA environment and the SAP HANA database through the network, use network firewall technology to create network zones for the different components and to restrictively filter the traffic between these zones implementing a 'minimum required communication' approach."

How network segmentation solves tough security challenges

Network segmentation is a core pillar of an enterprise Zero Trust security model and adheres to the Zero Trust principle of "never trust, always verify." Leading segmentation solutions provide a software-defined means of fulfilling SAP's recommendation to create network zones for different SAP HANA databases. This can be accomplished through a combination of environment separation, application ringfencing, and attack surface reduction use cases.

The table below presents some of these security challenges, and how a leading segmentation solution would solve for those challenges:

SAP security challenge	**Segmentation solution**
● Limited or no understanding of how SAP applications communicate across the network, to other applications, servers, clouds, endpoints, or user devices	● Quickly understand how your SAP deployments and other applications communicate with other points of the network ● Software-based approach with comprehensive coverage solves all

	blind spots with a comprehensive and contextual network map
● As new versions of SAP are released, securing the platform becomes more difficult due to their architectural and hosting complexities	● Experience a single pane of glass for all applications and network traffic, whether your SAP applications are running on-prem or in the cloud ● Control network traffic to and from any SAP application in the cloud or on-prem from the same UI
● Friction between SAP application owners and security teams	● Provide scoped application visibility maps to align the needs of application owners with the guidelines of security teams ● Enable granular network controls for impactful security improvements that don't disrupt business processes
● Protect against SAP data extraction	● Detect and halt unauthorized external connections ● Set a policy to limit who has access to which data, applications, servers, etc.

While there are a handful of solutions available that could fulfill these requirements for enterprises, one leading solution stands out from the rest, offering superior visibility, coverage, ease of use, and time to value.

What is Akamai Guardicore Segmentation?

Akamai Guardicore Segmentation provides the simplest, fastest, and most intuitive way to enforce the network segmentation needs of enterprises using SAP. It is designed to stop lateral movement and prevent security breaches by visualizing the SAP infrastructure, applications, and network flows, and allowing you to implement precise microsegmentation policies in the enterprise's network. Network segmentation helps reduce breach detection times and stop an evolving security attack before it causes significant damage.

SAP provides built-in security features such as data masking, data anonymization, data encryption, and more. These features are complemented by Akamai Guardicore Segmentation, which is focused on securing the network traffic to and from the SAP application. Additionally, the visibility maps, policy templates, and true security characteristics of the solution make it easy to complete security projects for expansive SAP deployments.

In addition to the SAP software solutions listed on the first page, Akamai Guardicore Segmentation is also able to secure many additional types of SAP solutions, regardless of their underlying infrastructure, due to our breadth of additional bare-metal server and VM coverage. You can read more about this in the SAP store.

Customer example

Guided by a clear leadership directive, a large European pharmaceutical company needed to ringfence five separate environments that hosted their crown jewel applications and associated servers, many of which were running SAP.

Akamai Guardicore Segmentation was able to map all SAP applications and servers — as well as legacy, on-prem, and cloud machines — in the same interface. The project began by rolling out monitoring and alert policies, and then moved to block mode once the implications were clearly understood by the security teams and application owners. Additionally, scoped application visibility maps were provided to SAP application owners for more granular visibility of the network traffic to and from their applications.

With adherence to Zero Trust principles, only permitted application network traffic was allowed, and everything else was blocked by default.

Summary

With Akamai Guardicore Segmentation, you can:

- Achieve a robust security posture for SAP deployments.
- Map and reveal your SAP environment with deep insight and network-wide context into dependencies.
- Go beyond application security by compartmentalizing your enterprise network through implementation and enforcement of granular security controls.
- Fulfill SAP’s recommendation to use firewall-based technology to segment SAP infrastructure, preventing unauthorized access or communication.

To learn more, visit akamai.com/guardicore or the SAP store.

Available on
SAP Store