SOLUTION BRIEF

FortiADC Delivers Unmatched Web Protection for SAP

FortiADC integrates with SAP using an innovative connector for web security, application acceleration, and load balancing.

Executive Summary

Business leaders must stay on top of emerging trends and modern technology to remain relevant in the digital world. Organizations turn to SAP for accessing real-time data across business units to make data-driven decisions, improve business outcomes, and drive innovation. With SAP, businesses can integrate customer information, supply chains, and vendors to transform business processes with intelligent automation.

A focused SAP security practice is necessary to protect all the data generated by SAP, and Fortinet utilizes a holistic approach to secure the entire SAP landscape. The Fortinet Application Delivery Controller (FortiADC) includes an SAP connector designed for advanced protection against cyberattacks by securing SAP applications with a full-featured web application firewall. It not only protects SAP APIs, but as an application delivery controller, it optimizes SAP application performance. With FortiADC, IT teams can forge ahead with their SAP projects with the confidence they can keep their systems protected against potential cyberattacks.

The SAP threat landscape is shifting

SAP systems contain data from finance, human resources, and proprietary information. Security of this highly sensitive data is paramount, especially as cloud, mobile, and hyper-scale technologies come into play, exposing more services to the Internet and increasing the attack surface area. The threat landscape for SAP software is shifting as many organizations embrace hyperscalers to upgrade their SAP system or move to SAP S/4HANA. The key factors listed below are responsible for the shifting SAP threat matrix.

Fiori, SAP's new user web interface, opens the door for web-based threats. Modern SAP systems use Fiori technology to provide a state-of-the-art user interface. SAP Fiori is replacing the traditional, old-fashioned UI technology such as SAP GUI or SAP Web Dynpro. Now, SAP users are using web browsers to access SAP applications via HTML5 which opens the door for many new web-based threats. Even users from the Internet access SAP systems via HTTP(s).

More SAP landscapes run on cloud and hybrid solutions. Customers are deploying more and more SAP systems in hybrid or multi-cloud solutions, and most S/4HANA systems are moving to the cloud. Adding point products to extend to the perimeter of the attack surface creates silos and added complexity.

Protecting SAP is top of mind

- Cybercrime To Cost The World $10.5 Trillion Annually By 2025[1]
- SAP systems are targets of threat actors
- SAP security updates do not provide sufficient protection

SAP Security risks exist

- SAP does not provide guidance on infrastructure security
- SAP does not provide any rules on how SAP systems can prevent security attacks
- SAP users connect to SAP using browsers (HTTPs) opening up new threats

Cloud deployments of SAP

- The attack surface shifts
- Protecting SAP APIs becomes a new requirement
- SAP systems' uptime requirements create a burden to SAP Basis teams

FortiADC provides advanced services for SAP

- SAP application delivery is integrated into Fortinet Security Fabric
- Adds Web Application Firewall, Intrusion Prevention, load balancing, and user authentication
- Simplified setup by leveraging SAP Internet Communication Manager (ICM) and SAP Message Server

SAP APIs are at risk. SAP is providing a variety of different APIs like OData for SAP Fiori or SOAP for SAP IDoc. These APIs enable sharing of digital assets between enterprise systems but going digital increases the risk of API attacks. The rise of B2B and C2C communication via APIs creates another security exposure for SAP landscapes.

Smart Devices connect to SAP applications. With the advent of Industry 4.0, customers and enterprises are using smart devices (e.g., industrial smart sensors, industrial machinery, and smart meters.) These devices provide information directly to SAP systems to enable fast business processes and decisions, however the SAP systems collecting data over the Internet increase the risk of security threats.

How Fortinet provides higher security for SAP

The modern SAP system, and its migration to the cloud, enable ever more interfaces and connections to other SAP and non-SAP systems that are internal and external to an organization. Defending a business's most vital application is as complex as it is critical. An SAP deployment may involve multiple landscapes spread across hybrid premises and cloud footprint running on a variety of software-defined networks (SDNs). Frontends, application servers, and databases must be segmented against lateral infection and unauthorized access. With user connections and data largely encrypted by SSL, high-performing, inline deep packet inspection is a necessity. At the same time, security must have no perceptible impact on the user experience and system performance.

With so many vectors to protect against, visibility can be a challenge across such a broad and diverse infrastructure as SAP. **Fortinet's Security Fabric** platform specifically addresses SAP's most common and emerging threats by providing a unified security context that is simultaneously integrated with and independent of the underlying infrastructure. Fortinet uniquely provides the high-performing network and content protection that an SAP deployment demands.

The role of the SAP Web Dispatcher

The SAP Web Dispatcher is an SAP software component located between the Web client (browser) and the SAP system running the Web application. The SAP Web Dispatcher connects SAP users to SAP Application Servers and balances load between SAP AppServers. It provides basic capabilities but is not intended to provide security functionality like a web application firewall (WAF).

Limited security functionality leads to risk for cybersecurity attacks

Cybercrime is on the rise, and cybercriminals are becoming smarter and more dangerous, using scripted attacks that improve their speed and scale. Many organizations use Fortinet's FortiADC and configure the SAP Connector to provide their business-critical applications with advanced protection, 24×7 availability, and optimization.

- Security-Driven Networking
- Adaptive Cloud Security
- Fabric Management Center - Security Operations
- Zero Trust Network Access
- Open Ecosystem

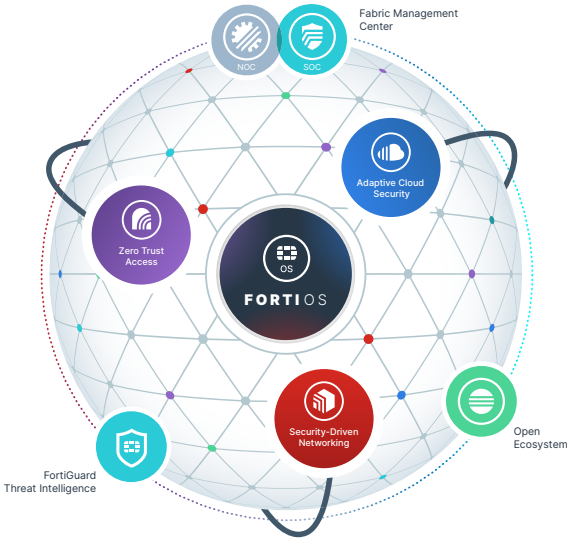

FIGURE 1: FORTINET SECURITY FABRIC DIAGRAM

Security Functionality	FortiADC	SAP Web Dispatcher
Protection from the OWASP Top 10 application attacks	Yes	No
SSL termination, URL rewrite and URL filter	Yes	Yes
High-capacity decryption and encryption with hardware-based SSL ASIC	Yes	No
SAP API protection	Yes	No
Real-time actions based on SAP metrics	Yes	Limited
Application optimization	Yes	No
24×7 application availability	Yes	No
Advanced application load balancing	Yes	No
Supports large SAP deployments	Yes	Limited
Content delivery optimization for web pages	Yes	No

How FortiADC provides advanced services for SAP

FortiADC is an advanced application delivery controller that enhances SAP applications' security, scalability, and performance. FortiADC provides WAF, intrusion prevention system (IPS), SSLi, link load balancing, and user authentication in one solution, whether SAP applications are hosted on-premises or in the cloud. Deploy FortiADC as either a physical or virtual machine (VM) or a cloud solution.

Dynamic SAP integration

FortiADC secures SAP both with Dynamic SAP integration and by integrating application delivery into the Fortinet Security Fabric. The SAP connector gets changes from the SAP Message Server. All SAP web traffic to the SAP Application Servers is protected with end-to-end encryption using the FortiADC.

Simplify setup and management

An intuitive user interface streamlines the configuration of CLI and APIs. Automated configuration gathers information from the SAP ICM configuration (HTTP/HTTPs Ports, virtual hosts, etc.) and additional application server instances. The SAP connector provides a topology view of the SAP landscape within the network for easier management and unified visibility for multi-cloud or on-premises SAP deployments.

Full-featured WAF and more

- Detect a zero day attack
- Protect from OWASP top-10 and many other threats
- Enterprise-class layer 4-7 ADC
- Disaster recovery and multi-site availability using FortiGSLB Cloud
- DDoS application and web filtering
- IPS, Geo-IP and IP reputation
- Support multiple deployment mode

Use real-time threat intelligence

Each day Fortinet FortiGuard Labs uses one of the most effective and proven artificial intelligence (AI) and machine learning (ML) systems in the industry to process and analyze more than 10 billion events, sending actionable real-time threat intelligence to customers. The FortiADC Fabric Connectors enables the SAP connector to use the threat intelligence of FortiLabs. With deep integration to the Fortinet Security Fabric, FortiADC integrates to additional Fortinet products such as FortiSandbox that decrypts, scans, and re-encrypts files before reaching the end-user, detecting both known and unknown threats

Optimize maintenance

The SAP connector automatically adds or removes the SAP Application Server. For example, if an SAP Application Server goes offline, the FortiADC will remove it from the pool, and likewise, if a new server is deployed, it will be automatically added.

Enterprise protection for SAP

Fortinet protects all SAP data generated by edge devices, endpoint systems, users, AI, applications, databases, 3rd party systems in multi-cloud environments and on-premises. By replacing the SAP Web Dispatcher with FortiADC, organizations not only improve security visibility and traffic but gain advanced functionality for their SAP systems.

Secure your SAP system with Fortinet

As the world evolves, businesses turn to SAP to remain resilient, agile, and innovative. SAP is a business's most critical business application, and protecting its sensitive data is vital. Fortinet's holistic coverage ensures SAP systems are protected and that security policy and visibility remain unified across the hybrid and multi-cloud footprints. While SAP's web dispatcher provides basic security, many organizations use FortiADC to reduce their security risk and leverage additional functionality.

FortiADC is part of Fortinet's Security Fabric, which provides a broad, integrated, and automated cybersecurity framework. It weaves together all operational and technical security facets, creating a consistent structure to the SAP security landscape's needs.

Web Application Firewall

Multiple levels of protection to defend against attacks that target your SAP applications with native WAF integration.

API protection

Protection for SAP APIs (JSON, SOAP & XML) against security threats and attacks.

Antivirus and IPS

FortiADC has built-in IPS capabilities to provide an additional layer of security.

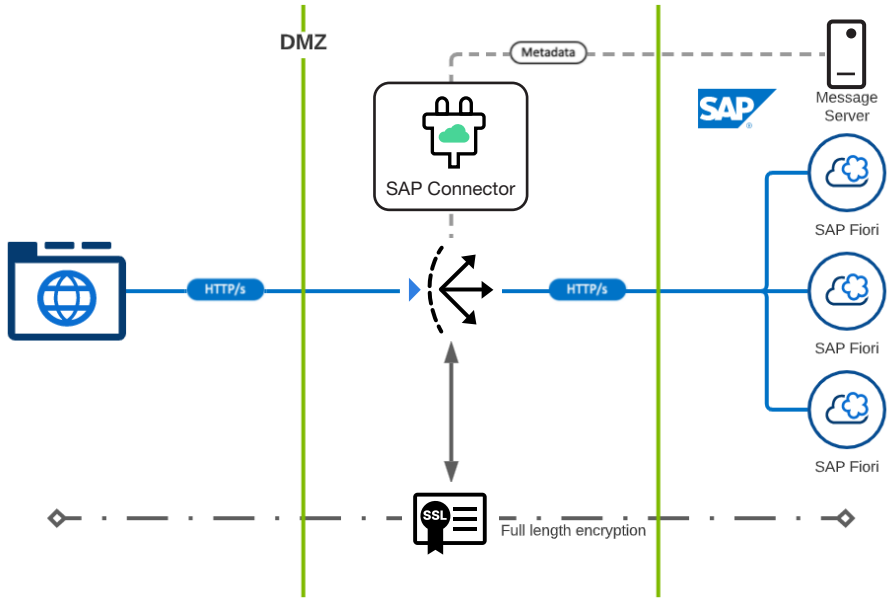

FIGURE 2: FORTIADC SAP CONNECTOR

[1]"Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybercrime Magazine, November 13, 2020.

www.fortinet.com