FORTINET

WHITE PAPER

Fortinet Security Solutions for SAP S/4HANA

Securing the Intelligent Enterprise

October 2020

Authors
Ricardo Ferreira, Aidan Walden, Julian Petersohn, Joeri van Hoof, Matthias Czwikla

Table of Contents

1. Executive Summary

With today's challenges and economic climate, organizations leverage enterprise resource planning (ERP) to improve decision-making and integrate information from customers, supply chains, and vendors to gain competitive insights.

SAP is the world's largest enterprise application software provider, a leader on the Gartner Magic Quadrant helping organizations with their digital commerce platforms sales and operations planning systems, integrating, consolidating, and generating insights into its critical processes.

As these systems contain data from finance, human resources, and proprietary information, their security is paramount, especially as cloud, mobile, and hyperscale technologies come into play, exposing more services to the internet and increasing the attack surface area.

Fortinet secures the Intelligent Enterprise running SAP

Fortinet, a cybersecurity leader, helps organizations to create a holistic security posture across all their SAP landscapes to secure them from intrusions.

Fortinet leverages its extensive threat intelligence, a strong portfolio, and state-of-the-art artificial intelligence (AI) and machine learning (ML) security to provide a seamless security experience across your SAP landscapes. It automates security controls, making it easier to manage, respond, and automate the SecOps capabilities.

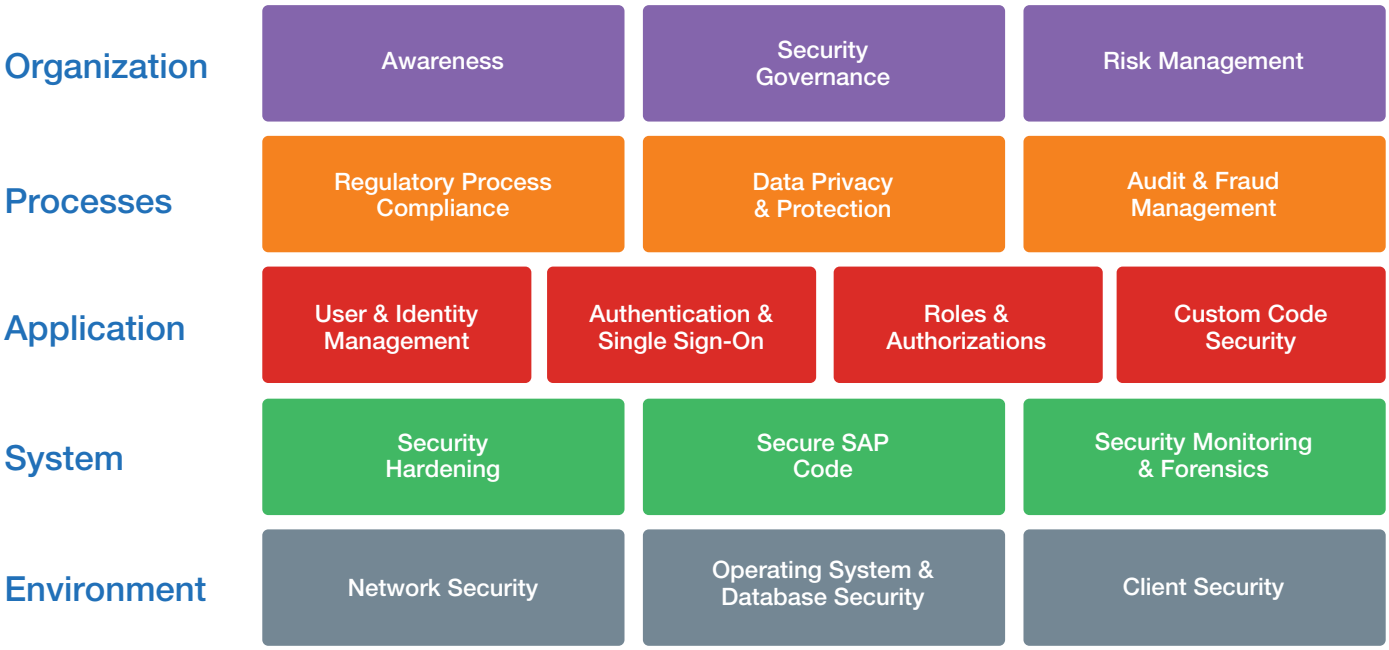


Figure 1 SAP Secure Operations Map

This white paper provides insights into how Fortinet aligns to the five layers of the SAP Secure Operations Map with several degrees of integration across the layers.

Fortinet provides advanced security for SAP, and with its network security pedigree, Fortinet has a focus on the environment layer, providing in-depth attention in network segregation, web dispatcher security, and client security.

In this paper, we also highlight SAP's most common attack vectors, and how Fortinet's portfolio can address those vectors by taking a preventative and detective role in SAP environments.

The recommendations and best practices contained herein are useful for stakeholders involved in the design, implementation, and security of SAP systems.

2. Audience

The intended audience of this document is:

- Executive and Management
  - Chief Information Security Officer (CISO)
  - Head of IT Infrastructure
  - Lines of Business Manager
  - SAP Program and Security Manager
- Technical and Operations
  - SAP Basis Consultant
  - SAP Security Architect or SAP Security Administrator
  - SAP Application Architect
  - Risk Management and Security Professionals
- And others who have responsibilities in the security of SAP landscape

The authors of the document assume that readers have some knowledge of SAP and the Fortinet portfolio, along with some security and networking expertise and agile application development.

Because of the massive nature of SAP technologies, readers are encouraged to take advantage of other resources, including those listed in this document's references for more detailed information.

3. Introduction

This document aims to present best practices and recommendations for implementing a secure SAP environment, including SAP S/4HANA, a future-ready enterprise resource planning (ERP) system with built-in intelligent technologies, including AI, ML, and advanced analytics. S/4HANA transforms business processes with intelligent automation and runs on SAP HANA—a market-leading in-memory database that offers real-time processing speeds and a dramatically simplified data model.[1]

Problem Statement 1 – Why should you care?

Today, new implementations of SAP systems, SAP upgrades, conversions to S/4HANA, etc., are not deployed by default in on-premises data centers. "Do more with less" has been the challenge for CIOs for many years, meaning to provide more IT services to the enterprise with a reduced or at best stable IT budget. By outsourcing IT to cloud providers, organizations can free budget and invest parts of that budget into more innovative tasks and projects.

However, by adding services from the cloud or by managing hybrid environments, enterprises shift their attack surface. As a result, they have to rethink security seriously to ensure customer data and enterprise information is protected, and data privacy policies in each country conducting business are respected.

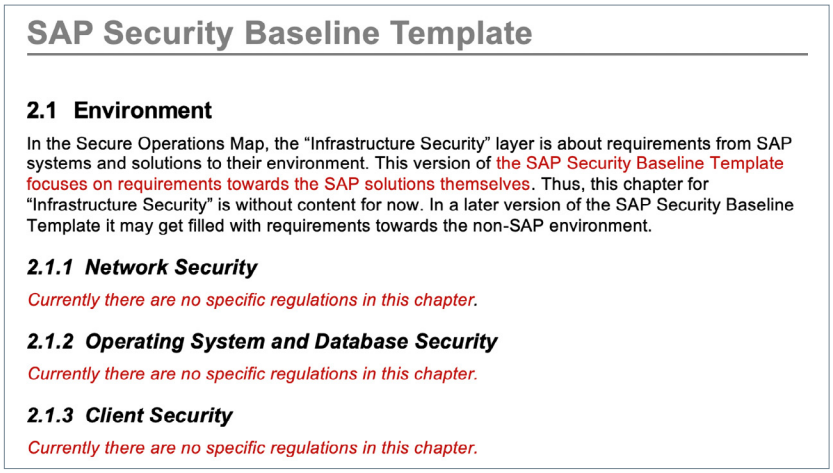
Problem Statement 2 – Can you patch your SAP systems in time?

SAP Security Updates are periodically released. Customers are recommended to implement patches promptly. However, SAP systems' uptime requirements create a burden to the SAP basis team to upload, test, and validate every SAP patch. Security-driven networking can help mitigate many risks.

Problem Statement 3 – SAP security baseline template provides no guidelines for infrastructure security

The latest SAP Security Baseline Template published in February 2020 offers many recommendations to secure SAP systems mainly regarding:

- SAP ABAP Application Server
- SAP Java Application Server
- SAP HANA
- Others, like Web Dispatcher or SAP GUI


SAP Security Baseline Template

2.1 Environment

In the Secure Operations Map, the "Infrastructure Security" layer is about requirements from SAP systems and solutions to their environment. This version of the SAP Security Baseline Template focuses on requirements towards the SAP solutions themselves. Thus, this chapter for "Infrastructure Security" is without content for now. In a later version of the SAP Security Baseline Template it may get filled with requirements towards the non-SAP environment.

2.1.1 Network Security

Currently there are no specific regulations in this chapter.

2.1.2 Operating System and Database Security

Currently there are no specific regulations in this chapter.

2.1.3 Client Security

Currently there are no specific regulations in this chapter.

Figure 2 Extract from SAP Secure Baseline Template – Infrastructure and Network Security are not considered

Specific recommendations or regulations regarding network, operating system or client security (infrastructure security) are relevant. Still, SAP does not provide any rules on how SAP systems can prevent security attacks with today's technologies available to cyber criminals. Here's where Fortinet adds value to ensure a secure SAP environment.

As a lot of information about S/4HANA is covered in other documents, this document will focus on the aspects that change due to a Fortinet SAP secure implementation.

As part of this document, the focus will primarily be on the environment and application security of the SAP Secure Operations Map while also focusing on the ecosystem surrounding it, including segmentation, web application firewall (WAF) security, and the recommended network security practices.

This paper's primary goal is to present and promote an SAP secure execution model to help organizations adopt the SAP architecture to do it securely. The secondary goal is to identify applicable risks, threats, and vulnerabilities followed by recommendations for security controls and best practices needed to secure an SAP environment.

Section Summaries

Each section will start with a summary that includes the key findings, along with explanations and references within each section to benefit a high-level reader.

4. What Makes SAP So Relevant

4.1 High-Level Summary

SAP customers will have to convert their SAP systems to SAP S/4HANA by 2027.[2] The majority of SAP S/4HANA systems will be deployed in the cloud at one of the top global hyperscalers (cloud providers).[3] Fortinet is well-positioned to provide higher-level security for SAP systems. **Fortinet secures the Intelligent Enterprise running SAP—**by protecting all SAP data generated by edge devices, endpoint systems, users, AI, applications, databases, third-party systems in multi-cloud environments, and on-premises.

SAP is the world's largest provider of enterprise application software. SAP software is an integrated software suite that addresses needs from all areas and organizations within an enterprise. All SAP systems are mission-critical and demand no downtime.

4.2 SAP Software Is Mission-Critical

What drives customers to use SAP software? SAP software is an integrated software suite that addresses needs from all areas and organizations within an enterprise. SAP enhances the competitiveness of enterprises by modernizing and transforming processes into digital solutions. Implementations of SAP software can take between four months to several years. SAP systems are always business-critical, and most of the time, they also are mission-critical; thus, downtime is unacceptable. Customers can have dozens if not hundreds of SAP systems deployed.

4.3 SAP Is the Gorilla in the Enterprise Application Software Market

SAP is the world's largest provider of enterprise application software. Founded 1972 in Germany, SAP today is the largest European software company and delivers its business solutions to more than 400,000 customers worldwide. SAP Concur, SAP SuccessFactors, SAP Ariba, and several other smaller acquisitions are major drivers to SAP's cloud revenue today. While SAP Business Suite achieves the dominant part of SAP revenue, SAP S/4HANA is the successor of SAP Business Suite.

92% of the Forbes Global 2000 are SAP customers. 77% of the world's transaction revenue touches an SAP system. SAP is the gorilla in the enterprise application software market with revenues of €27,6 bn in FY2019 and more than 100,000 employees.[4]

4.4 SAP S/4 and the Benefits of HANA

SAP S/4HANA is SAP's successor of SAP Business Suite. Based on a simplified data model, S/4HANA provides an immediate benefit to the line of business (LOB) by improving productivity. While S/4HANA offers faster and more flexible processes at significantly less IT costs, it sits at the core of enterprises to enable them to reach their next level of digital transformation by using embedded artificial intelligence, real-time analytics, and more.

S/4HANA is an architectural redesign of SAP's traditional application architecture based on SAP R/3 from 1992. Although S/4HANA was developed to achieve maximum benefit of SAP HANA—**H**igh-Performance **An**alytical **A**ppliance—it also supports traditional database management systems (DBMS) like Oracle, DB/2, MSSQL, Sybase, etc.

SAP HANA is an in-memory, column-oriented DBMS that allows real-time OLTP and OLAP operations in a single system, thus avoiding the need for additional data warehouse systems that enable data mining on OLTP data. Such data warehouse systems are not capable of screening real-time data. SAP HANA has that capability due to its ability to store data in-memory and in columns. Scale-out systems of SAP HANA can span up to 16 nodes and hold up to 24 TB of data in-memory for a single SAP system.

4.5 The Role of Cloud Providers

Major cloud providers like Amazon Web Services, Microsoft Azure, Google Cloud, Alibaba Cloud, and others offer dedicated services for SAP users. SAP can be deployed in their clouds to offload costs of running on-premises systems into the cloud and pay by OPEX instead of CAPEX. However, many customers will prefer a hybrid model, where the majority of SAP systems will run in the cloud and where dedicated production systems remain on-premises.

No matter which model is selected, the need for higher security for data of mission-critical systems is increasing as the attack surface shifts when moving to the cloud.[5]

SAP announced a Go-To-Market agreement in 2019 and renewed its strategic partnership with Microsoft - Project Embrace.[6] Embrace provides Market-Approved Journeys (MAJ) to customers, giving them an easy path to upgrade their SAP systems to S/4HANA on Microsoft Azure. Microsoft also became a reseller of SAP Cloud Platform on Azure.

Also, Google is heavily investing to take SAP customers to their Google Cloud. In June 2020, Google opened up a new data center in Frankfurt, Germany, that is planned to exclusively host SAP customers providing all the benefits of a cloud.[7]

Cloud providers make it easy to migrate SAP systems from on-premises to the cloud, promising lower TCO. Therefore, customers have to decide whether to continue deploying applications in their own data centers or move them to the cloud to free resources up for more innovative tasks, resulting in faster digital transformation and increased competitiveness for the enterprise. It is not an easy decision when considering that myriad network security solutions must be deployed.

4.6 What Drives the Market To Implement SAP S/4HANA

SAP announced that standard support for SAP Business Suite would end by 2027. By that date, all customers will have to be converted to SAP S/4HANA unless they prefer to pay a premium for their SAP support fees. Converting old systems to S/4HANA is not necessarily straightforward. This type of project requires careful planning and consulting expertise, as well as significant budget to execute in time.

The majority of S/4HANA systems are expected to move to the cloud at one of the cloud providers mentioned in 4.5 above. Fortinet is well-positioned to provide a higher level of security for SAP systems. **Fortinet secures the Intelligent Enterprise running SAP—**by protecting all SAP data generated by edge devices, endpoint systems, users, AI, applications, databases, third-party systems in multi-cloud environments, and on-premises.

5. Why Fortinet Secures the Intelligent Enterprise

Fortinet, the number one cybersecurity leader with more than 20 years of history protecting assets, optimizing content delivery, detecting malicious actors, and mitigating threats, saw a rising in the attacks targeting SAP systems. As these systems are one of the most critical assets of organizations, Fortinet decided to secure those landscapes.

By applying the Fortinet unified portfolio, organizations can have a consistent security framework for SAP across multiple locations and regions. Leveraging the Security Fabric, 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.

As data is the new oil and SAP systems contain confidential data, Fortinet provides capabilities addressing the data's lineage, providing confidentiality, integrity, and availability. Fortinet capabilities in data loss prevention (DLP), preventing exfiltration of data, and integration with leading vendors as part of the Security Fabric create a unique value in data security, as it consolidates it in a single pane of glass.

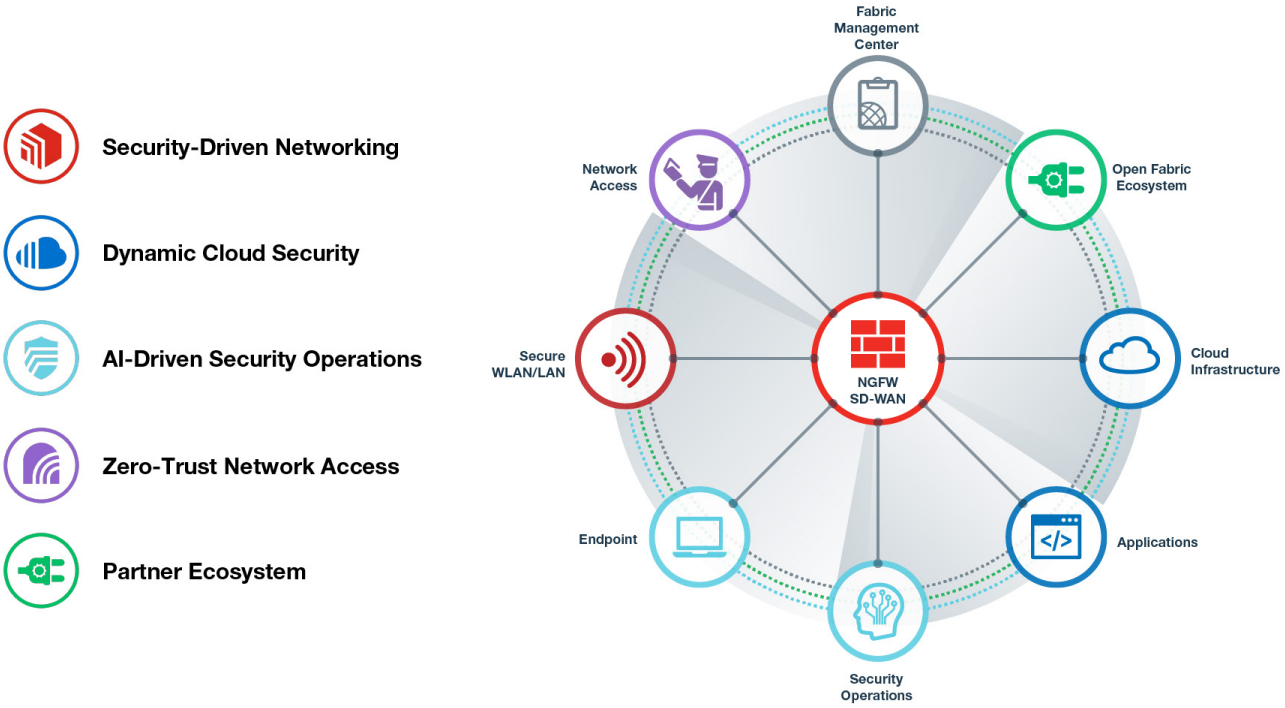


Figure 3 Fortinet Security Fabric Diagram

The single-pane-of-glass management enabled by the Fortinet portfolio provides a complete and consolidated view across various network edges. It simplifies operations and provides networkwide security, visibility, and analytics, in every environment, centralizing operations for complex landscapes such as SAP, delivering scale, performance, and resiliency for SAP.

As SAP systems are becoming more prevalent in the cloud, Fortinet has integrated next-generation firewalls (NGFWs) that can be deployed in cloud environments supporting the majority of the cloud providers. Customers can leverage consistent multilayer security protection, automation, and deep integrations, no matter how many clouds they adopt and provide protection to the SAP ecosystem and beyond.

Fortinet reduces the time to deploy S/4HANA with prepackaged Infrastructure-as-Code templates, enabling the organization to be more agile, adopt DevOps best practices, and provide 360 protection to the SAP landscape.

Fortinet wants to accelerate the security in your SAP ecosystem by protecting all SAP data generated by edge devices, endpoint systems, users, AI, applications, databases, third-party systems in multi-cloud environments, and on-premises. Fortinet will provide an integrated experience to ensure that your critical assets stay protected and empower you to focus on your core business.

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks number one in the most security appliances shipped worldwide and more than 450,000 customers trust Fortinet to protect their businesses.

Fortinet is the only security leader to develop and build custom security processing unit (SPU) technology to offer the best performance and cost value in the industry with a Security Compute Rating that ranges between 3 to 47x the performance of other software approaches. Each day Fortinet FortiGuard Labs uses one of the most effective and proven AI and ML systems in the industry to process and analyze more than 10 billion events, sending actionable real-time threat intelligence to customers. The combination of FortiOS, purpose-built SPU technology, and AI-powered threat intelligence showcases the Fortinet commitment to cybersecurity innovation and excellence.

The Fortinet flagship enterprise firewall platform, FortiGate, is available in a wide range of sizes and form factors to fit any environment and provides a broad array of next-generation security and networking functions. The Fortinet market position and solution effectiveness have been widely validated by industry analysts, independent testing labs, business organizations, and media outlets worldwide. Fortinet is proud to count the majority of Fortune 500 companies among its satisfied customers.

Fortinet is headquartered in Sunnyvale, California, owns a 200,000 square foot manufacturing assembly and operations center in Union City, California, and has offices around the globe. Founded in 2000 by Ken Xie, the visionary founder and former president and CEO of NetScreen, Fortinet is led by a strong management team with deep experience in networking and security.

Fortinet technologies can secure the demanding needs of any organization and help drive digital innovation from within.

6. How SAP Systems Are Being Attacked

6.1 High-Level Summary

Securing SAP systems is becoming more and more relevant in today's world. The threat landscape is constantly expanding, and it does not stop at SAP systems. It exposes companies of all sizes and industries to the risk of cyberattacks with severe consequences such as data leaks or damage to the company's reputation.

Some of the vulnerabilities of SAP systems have been given well-known codenames such as RECON or 10KBLAZE. Besides these known vulnerabilities, easy-to-use exploits are found on the internet and used by threat actors without much knowledge of SAP.

Every month, SAP publishes security advisories about current vulnerabilities or bugs that could endanger the entire SAP landscape. These notes should be implemented in the SAP systems at regular intervals to ensure secure operation and often requires system downtime.

This section discusses how SAP systems are being attacked, the type of data that is exposed, and how modern architecture can prevent attacks on SAP systems.

6.2 Overview of Published SAP Security Updates

Due to the size and complexity of SAP software, SAP carries out numerous tests, validations, and checks for compliance with programming guidelines before a new software component is released.

Nevertheless, there are always vulnerabilities, without knowing where and which ones are currently in the SAP code. These vulnerabilities exist among other large software providers that offer complex software. It is similar, for example, with Microsoft Windows or even Linux as a representative of the open-source community.

Let's take a closer look at the SAP Security Updates. The chart below shows the number of vulnerabilities that SAP[8] has closed per month between May 2019 and May 2020.

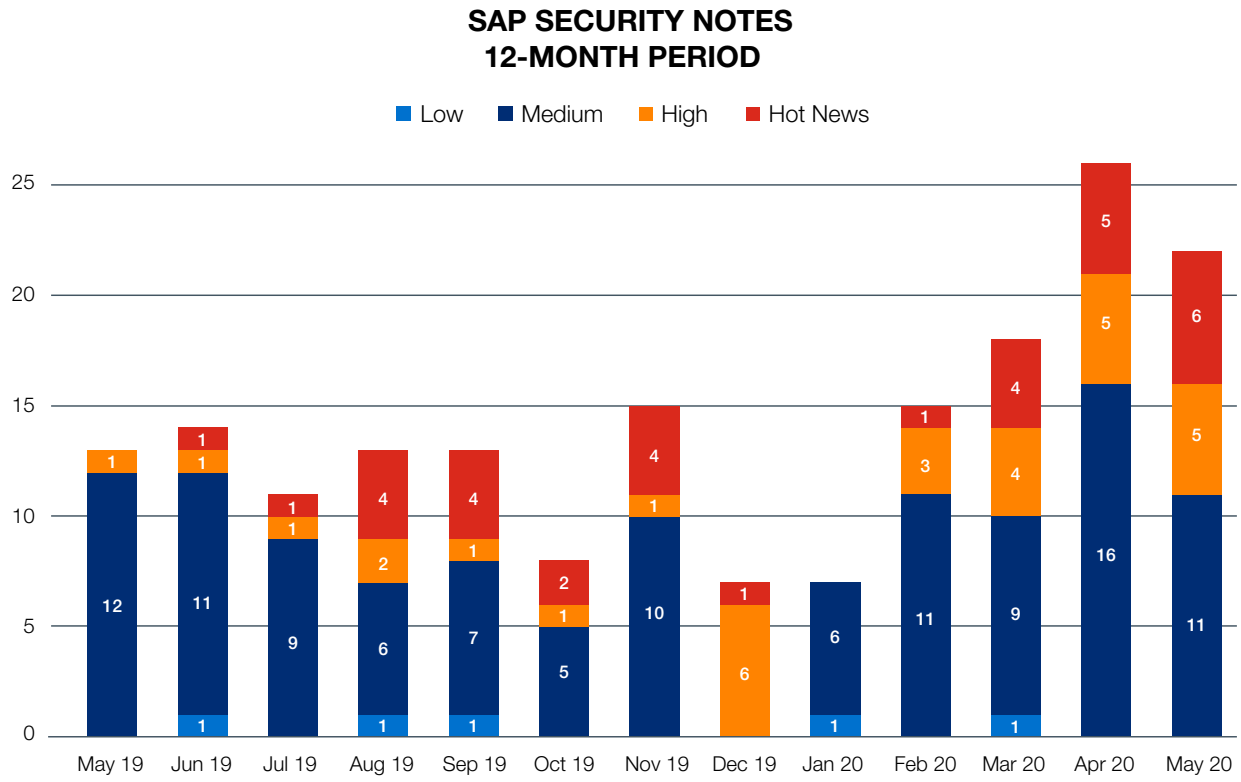


Figure 4 SAP Security Notes over one year

During this period, a total of 182 vulnerabilities were closed. The vulnerabilities are divided into four different types of SAP Security Notes, based on their Common Vulnerability Scoring System (CVSS) score:

Security Note Priority	CVSS v3 Base Score
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Hot News	9.0 – 10.0

Table 1 SAP Security Note CVSS translation

6.3 Analysis of Published SAP Security Updates

Related to the period from May 2019 to May 2020, Figure 6 shows that most vulnerabilities are rated medium. They are usually fixed during the regular import of new SAP Support Package Stacks along with those of type Low, High, and Hot News. SAP Security Notes of type Hot News should always be imported immediately since they impose a serious threat to the system. With notes of type High, you must weigh the advantages of applying them as quickly as possible versus importing them with the next SAP Support Package Stack, based on the system landscape and vulnerability exposure. Thus, an SAP system directly accessed from the internet must be patched with a higher priority due to its higher exposure to potential attacks.

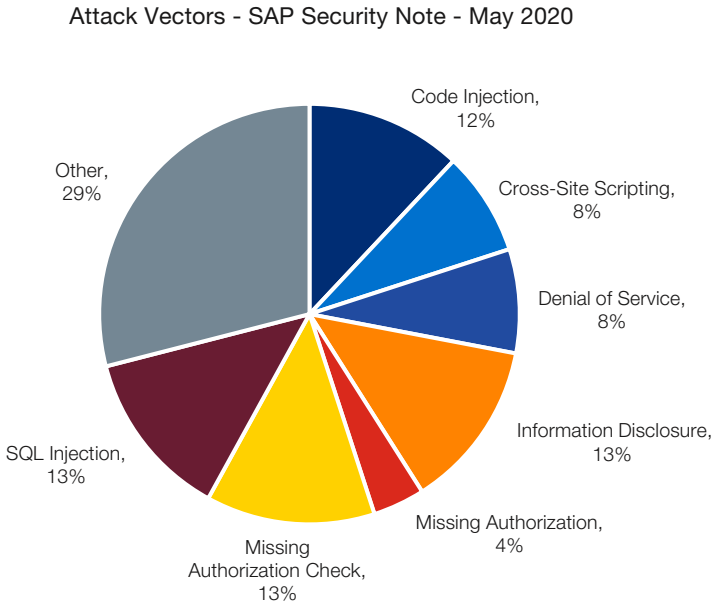


Figure 5 Attack Vectors SAP Security Note May 2020

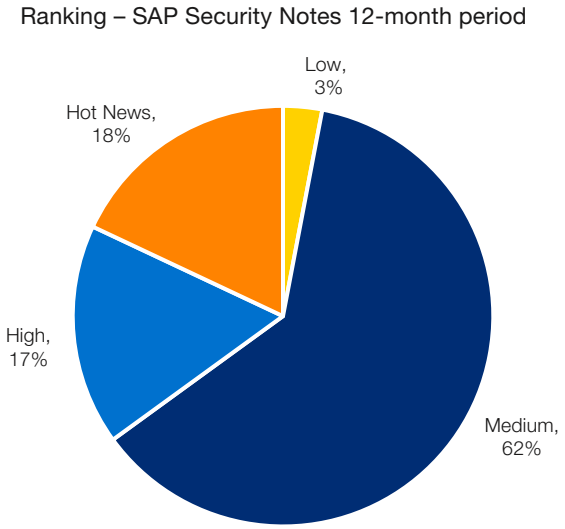


Figure 6 SAP Vulnerability Ranking May 2019 2020

Figure 5 above shows the attack vectors. One of the main vulnerabilities is the disclosure of information, which could help an attacker find the right tool or attack point. Also, SQL injections allow an attacker to read parts of the database and view data that is not intended for that user. Another possibility is to inject code into the SAP system, which could lead to a remote code execution.

6.4 A Closer Look Into Two Current SAP Threats

In this chapter, we now dive into two SAP threats, one of them codenamed 10KBLAZE, the other is a SQL injection. Both had very high attention because the vulnerabilities were emerging, simple, and presented high threats to SAP data and systems.

The first example under codename 10KBLAZE is a threat that contains a chain of multiple vulnerabilities. One of them is an unauthenticated remote code execution in the SAP RFC Gateway. The second example is an SQL injection in the SAP UDDI (Universal Description, Discovery, and Integration) Service application of the SAP NetWeaver Java.

By exploiting these vulnerabilities, an internal or external attacker can escalate their privileges and obtain sensitive technical and business-related information stored in the vulnerable SAP system.

6.4.1 Example 1: 10KBLAZE - Remote Code Execution via SAP RFC Gateway

This vulnerability, also known as 10KBLAZE, is a current threat for SAP systems, taken up by various computer magazines.[9] It discovered vulnerable SAP applications could be compromised by a remote, unauthenticated attacker who only had network access to the system (without requiring a valid SAP user ID and password). For example, this could be the visibility of a port on the internet. The attacker can gain unrestricted access to SAP systems, enabling them to compromise the platform with all its information, change or extract this information, or shut down the system.

A presentation at the April 2019 Operation for Community Development and Empowerment (OPCDE) cybersecurity conference describes SAP systems with insecure configurations exposed to the internet. In one of the sessions, it showed that **more than 3,280 SAP Gateways** were **exposed** to the internet on Port 3300 and 3301 TCP. Also, **more than 9,209 SAP Router and 1,981 Message Server** with Port 39xx should only be intended for internal use.[10]

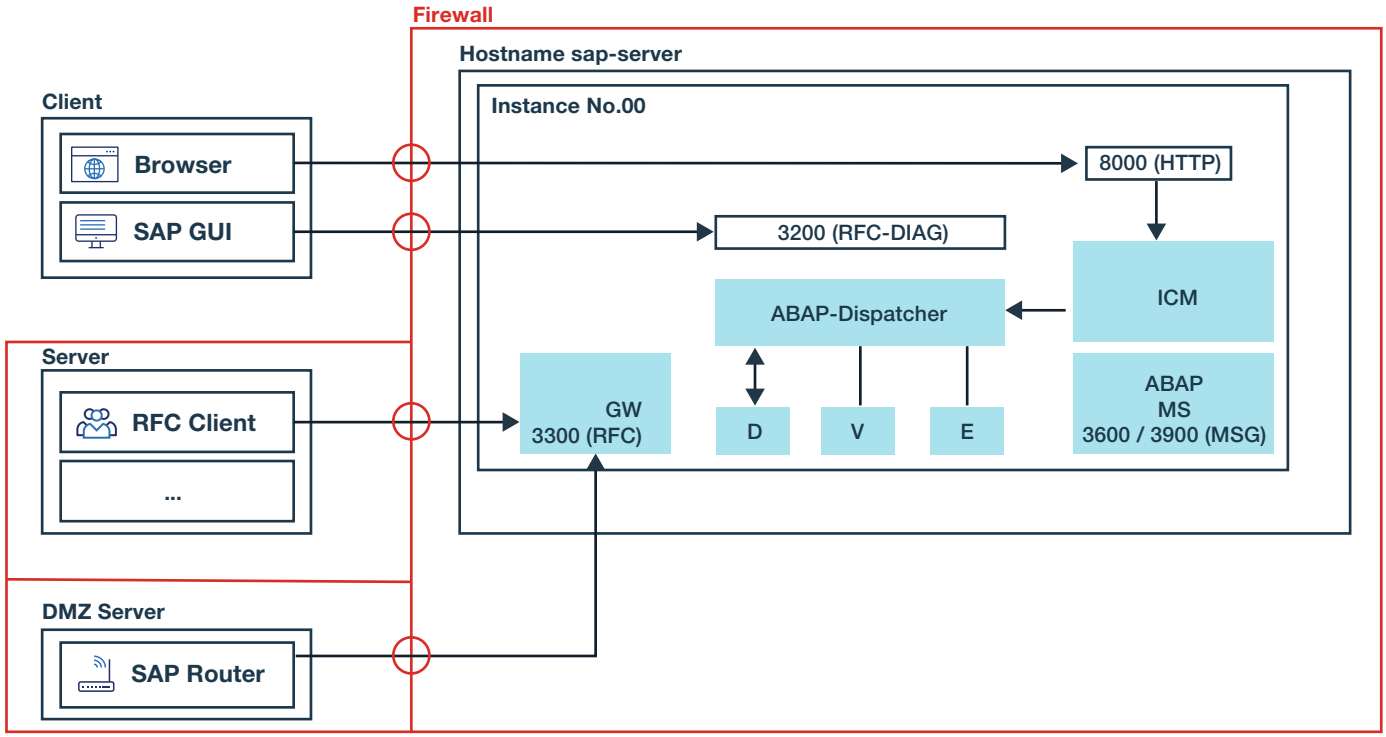


Figure 7 Example SAP Communication Diagram

The SAP Gateway (GW), the SAP Router, and the SAP Message Server (MS) were not optimally configured in security or deployed at a suboptimal location.

The SAP Gateway and the SAP Message Server are part of every SAP system and were insecurely configured in the past by many administrators for purposes of convenience. The SAP Gateway handles communication between SAP and non-SAP applications; SAP Message Server handles communication between SAP application servers and their users.

An SAP Router is required to provide SAP Enterprise Support access to SAP customer systems for support purposes, allowing customers to access and implement SAP notes or obtain the latest security information from SAP. In other words, the SAP Router is a program that helps to connect SAP systems with external networks. The SAP Router requires internet access and, therefore, is exposed to potential attackers.

In combination, Fortinet provides higher security to protect SAP Router and SAP components on the network layer (Environment Layer on Secure Operations Map) before an attacker can access the SAP system.

How 10KBLAZE compromises SAP components to gain access and control

There are two possibilities to attack SAP systems under this 10KBLAZE threat. Either use an upstream SAP Router or access the SAP Message Server monitor port.

In the first case regarding an attack via the SAP Router, a configuration vulnerability is used. This vulnerability allows the SAP Router to be used as a proxy to access the SAP system. It occurs when the SAP Router is either deployed locally on the SAP system or a system belonging to the SAP systems in the internal corporate network. In most configurations of SAP systems, the SAP Router has direct access to the SAP RFC Gateway. Under these conditions, attackers can misuse the SAP Router as a proxy. The attackers' requests then appear to the gateway as if they were coming directly from the SAP Router and should be allowed to pass through. In this case, attackers bypass any access control lists (ACLs).

In the second case, attackers require access to an unprotected monitor port (39xx) of an SAP Message Server. Attackers can add a malicious system to the SAP System's trust list—without the requirement to log in with a password or other proper authentication. The tampered trust list allows attackers to bypass the gateway ACL from their system and access the gateway directly.

Having exploited either one of the above vulnerabilities, further known attacks against the SAP Gateway can be carried out. For example, sending operation system (OS) commands to start compromising the entire system.

How remote code execution works

The SAP RFC Gateway can execute OS commands on the server where its own OS process is running, and this is an intended functionality and not a vulnerability. One reason is the "tp" command that can be called from any other server within the SAP transport landscape. In a typical scenario, the SAP System Administrator would execute predefined remote commands only, via Transaction SM49 or SM69.

An ACL file controls the executions and validates if the program is allowed to be executed by the user from the specific user host in the request. The ACL file is the only "authentication" for the RFC Gateway. Often, the ACL file contains a very vague or a blank configuration so that an attacker can fake an internal system to bypass this ACL and execute any command they want. This scenario will lead to unauthenticated remote code execution.

The first solution was to configure the security mechanisms implemented by SAP many years ago so that they could also fulfill their function as protection against unauthorized access. But not only the SAP systems as such can protect against threats. Another possibility to prevent future attacks is to connect a **firewall** in front of the SAP ports, which are connected to the internet to run corresponding **intrusion detection system (IDS)** and **intrusion prevention system (IPS)** rules to detect and block an attack before it is passed on to SAP. An IPS/IDS also provides security before the software vendor provides a patch for a vulnerability. Also, a patch does not resolve all security-related problems. Often a misconfiguration of an ACL file will cause access to a system.

6.4.2 Example 2: SQL Injection Vulnerability

SQL injection vulnerability means that code includes an SQL statement that contains strings that can be altered by an attacker. The manipulated SQL statement can be used to gain additional data from the database or modify data in the database.

How SQL injection compromises SAP systems

For example, CVE 2016-2386, which is an SQL injection for SAP NetWeaver AS Java.

This vulnerability affects SAP UDDI, which is one of the most used applications in SAP deployments. Thus, the SAP NetWeaver versions 7.11 – 7.50 are susceptible to this threat. To exploit the vulnerability, an attacker merely sends an HTTP query of the following type:

```
POST /UDDISecurityService/UDDISecurityImplBean HTTP/1.1
Content-Type: text/xml

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <SOAP-ENV:Body>
        <m:deletePermissionById xmlns:m="http://sap.com/esi/uddi/ejb/security/">
            <permissionId>x' AND 1=(SELECT COUNT(*) FROM BC_UDV3_EL8EM_KEY) or '1'='1</permissionId>
        </m:deletePermissionById>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Figure 8 Attack HTTP Query

The vulnerability is contained in **permissionId** that can keep any SQL command. When the SAP application receives the code, it will execute it. For example, an SAP server will execute this SQL command and return a count of rows from the **BC_UDV3_EL8EM_KEY** table.

```
SELECT COUNT(*) FROM BC_UDV3_EL8EM_KEY
```

Figure 9 SQL Query launched by CVE 2016-2386

By exploiting this vulnerability, attackers can obtain the hash of user passwords from the **UME_STRINGS** table. After that, they will need to get passwords from the hash, which they can achieve by:

- Using a brute-force attack
- Finding another vulnerability in the password crypto algorithm

How can we protect the SAP system from such attacks to avoid data exploits and a compromised system? Generic protection for threats such as SQL injections or cross-site scripting is a **web application firewall (WAF)**.

6.5 Expanding the SAP Threat Landscape

The SAP world is moving in the cloud direction and the new front end, SAP Fiori, for end-users. Fiori is a modern user web interface to access SAP applications, which is HTML5 based, and is about to replace the traditional fat client SAP GUI. With SAP Fiori , SAP applications now have usability comparable to consumer apps. In the past, using the SAP GUI, SAP interfaces were overloaded with many functions that most users would never use. Users needed long training periods and had difficulty finding their way around in the GUI. Today, (different) SAP applications offer the same range of functions, but the interfaces are clear and tidy. They are tailored to the end-user's respective role (e.g., accounting) and only show the functions needed by the end-user. SAP Fiori creates a consistent, role-specific, and intuitive user experience across the various enterprise applications—independent of the endpoint devices used.

6.5.1 Compromised SAP System in the Cloud

In addition to classical on-premises solutions, SAP also offers its customers additional cloud or hybrid solutions. SAP does not limit itself to SAP HANA Enterprise Cloud (HEC) and enables operations of SAP solutions in AWS, Microsoft Azure, and Google Cloud Platform.

As a result, SAP systems are no longer available only internally within company boundaries but can also be externally accessed. Hybrid deployments are deployments where SAP is partly available in the cloud as well as on-premises. As described in 6.5.2 below, even more emphasis must be placed on security-driven networking to avoid attacks like 10KBLAZE or the latest RECON hack.

In the future, HTTPS or similar connections coming from outside of an SAP landscape should be scanned for any known threats by using a WAF in combination with an IDS and an IPS. So far, SAP security is often not yet taken seriously enough by companies, opening doors to attackers and risking the loss of valuable data and unrestorable reputation.

6.5.2 Smart Devices Connected To SAP Systems Are Exposed To Attackers

Companies such as energy suppliers are supported by SAP and offer more customer-friendly digital services. These include the deployment of smart electricity meters that automatically send consumption data to the utility provider or corresponding self-service portals for customers to enter the meter reading themselves or look at their consumption hourly. In the future, such self-service portals will be based on SAP Fiori and are therefore also targets for attacks as they can easily be reached from any internet browser. The transmission of consumption data from smart electricity meters to systems such as SAP Leonardo must also be protected against manipulating the data.

Fortinet secures the Intelligent Enterprise running SAP—by protecting all SAP data generated by edge devices, endpoint systems, users, AI, applications, databases, third-party systems in multi-cloud environments, and on-premises.

Figure 10 EVB Energy Smart Meter[11]

7. How Fortinet Provides Higher Security for SAP

7.1 High-Level Summary of This Section

The modern SAP system, and its migration to the cloud, enable ever more interfaces—connections to other SAP and non-SAP systems that are internal and external to an organization. Defending what is typically a business's most vital application is as complex as it is critical. An SAP deployment may involve multiple landscapes spread across a hybrid premises and cloud footprint running on a variety of software-defined networks (SDNs). Front ends, application servers, and databases must be segmented against lateral infection and unauthorized access. With user connections and data largely encrypted by secure sockets layer (SSL), high-performing, in-line 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. With respect to infrastructure, SAP's Security Baseline Template leaves these problems to the customer to solve. The Fortinet 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.

7.2 SAP Well-Architected Security

SAP's well-architected security starts with considering how SAP traffic will transit the infrastructure and where boundaries of trust reside. Segmenting SAP from other workloads ensures a minimum boundary of trust and inspection. Critically, this includes the internal segmentation of application servers, front ends, and databases to prevent lateral attacks through impersonation or privilege escalation. The best practice of segmentation enables the FortiGate to high-performance, low-latency SAP security through the deep packet and content inspection specific to SAP services. With unmatched security effectiveness, the real key to success is the performance in a way that doesn't impact transaction times for users or impede database processes. Fortinet FortiOS operating systems bring various forms of hardware and software acceleration to bear, removing the compromise between security and performance.

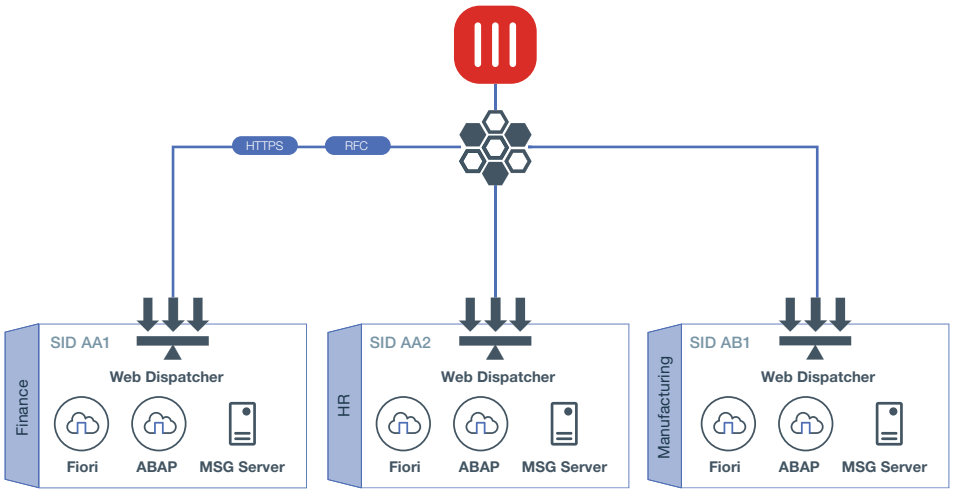


Figure 11 SAP East/West Segmentation

7.3 High-Performance Intrusion Prevention and Content Inspection

Addressing targeted SAP threats requires the security apparatus to be application-aware of the SAP systems running within the security boundary. The Fortinet FortiGate NGFW provides many features tailored to SAP. The FortiGate, combined with FortiGuard Threat Intelligence, delivers validated industry-leading IPS technology. FortiGuard Labs delivers SAP threat intelligence to the FortiGate's IPS engine to protect from well-known and emerging threats. Common exploits such as relay attacks, command execution, SQL injections in SAP NetWeaver ABAP and Java, and other services are mitigated with microsecond latency. Configuration errors are minimized as SAP heuristics, and signatures are enabled in the default IPS policy. Figure 12 shows a sampling of these.

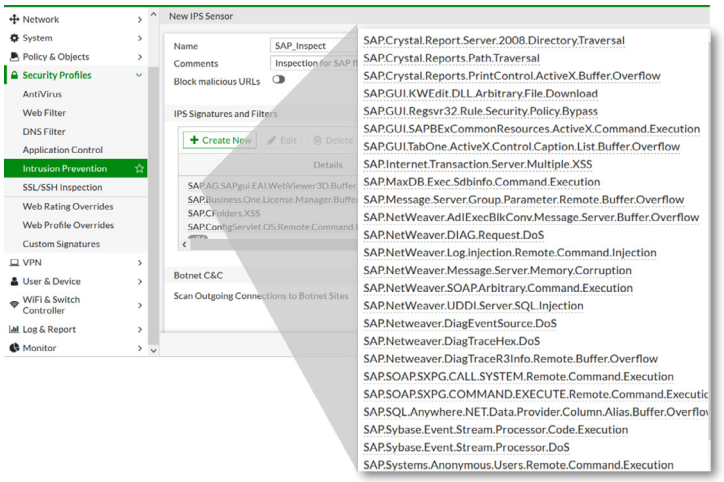
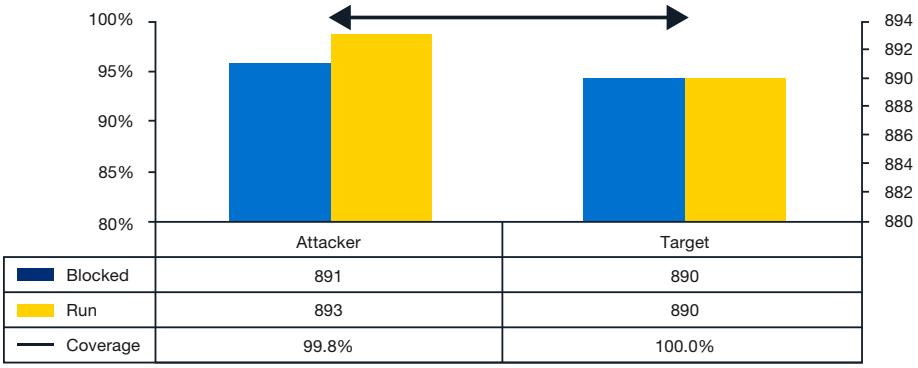


Figure 12 Sample of IPS Signatures for SAP

Year after year, Fortinet has been reported as a standout leader in next-generation IPS through independent studies such as those by NSS Labs and Virus Bulletin. Fortinet's catch rate for exploit and exploit evasion attempts is among the highest in the industry.



	Attacker	Target
Blocked	891	890
Run	893	890
Coverage	99.8%	100.0%

Figure 13 Fortinet NSS tested catch rates

As malicious actors evolve their attack and evasion techniques against SAP, static signatures and even heuristics may miss novel attacks. Traditional signature detection is reactive, as the signatures are merely fingerprints of threats that have already been seen. Fortinet's patented compact pattern recognition language (CPRL) is a deep-inspection, proactive signature-detection technology developed through years of research by FortiGuard Labs. A single CPRL signature can catch 50,000 or more variants of a family of malware. It includes decryption, unpacking, and emulation of code for robust static analysis, which reduces the volume of code that needs full sandboxing. CPRL proactive signature detection helps cast a wider net over the attacks and methods of modern advanced persistent threats (APTs) and advanced evasion techniques (AETs), preserving full sandbox analysis for the most sophisticated threats.

APTs pursue SAP systems because they target multistage attacks that are aimed at an organization's most valuable data. Further, threat actors may attempt reconnaissance and social engineering to aid infiltration. APTs against SAP require the advanced countermeasures that FortiSandbox enables. FortiSandbox is a rigorous inspection tool that can fully execute and analyze content and executable code to uncover APTs. FortiSandbox explores all code execution paths. Combining sandboxing with proactive signature detection minimizes the opportunity for APTs. With Fortinet Security Fabric integration, threat intelligence is distributed across the network footprint in real time to elevate the security posture continually.

7.4 SSL Inspection

It's no secret that the majority of HTTP traffic is SSL encrypted for apparent reasons. As SAP has embraced HTTP as a protocol for a modern S/4 deployment and customers move away from the SAP GUI thick client, the guidance has been to "maintain end-to-end encryption." In general, this is very sound advice. However, because encryption is merely a tool, it can protect any traffic from detection, including malware. Today more than 60% of malware is encrypted. In this seemingly conflicting guidance, supporting localized SSL inspection (decrypt, inspect, re-encrypt) provides both the visibility into malicious traffic flows and maintains the best practice of "end-to-end encryption." While this is a sound security approach when done correctly, performance impacts can cause user experience and database lock times to suffer. For instance, NSA Labs has found that, on average, the performance hit for deep packet inspection is 60%, connection rates decrease by an average of 92%, and response times increased by a whopping 672%. Fortinet removes this compromise between security and performance in a variety of ways.

Physical FortiGate NGFWs are equipped with proprietary hardware acceleration that offloads encryption functions to a security processing unit. This Fortinet-only capability boasts performance advantages of up to 20x that of competitors in the latest-generation devices. To deliver differentiated performance in virtual form factors, FortiGate implements the virtual security processing unit (vSPU) as a virtualized application-specific integrated circuit (ASIC) in conjunction with a unique decryption load-balancing service. The FortiGate running as a VM in a public or private cloud delivers 5-7x the performance of competitive NGFWs.

With Fortinet, SAP decision-makers can be assured that Fortinet provides the highest security catch rates with the most significant performance levels possible.

7.5 Hybrid Cloud Security Context

SAP S/4HANA is the core of SAP's modern Intelligent Enterprise solution that extends line-of-business applications from the data center to the cloud. By adopting the cloud, SAP allows the enterprise to focus on activities that create brand value. A hybrid loud deployment permits flexibility between customization and speed to market. This opportunity is not without cyber risks. The hybrid footprint makes a challenge to protecting dynamic edges where SAP systems may federate across these platforms. For every bit of brand value SAP creates, poor administration and poor security practices can destroy that value. Security implemented for SAP systems must unify these various platforms and edges in a single security context. The Fortinet Security Fabric does this by generating real-time threat intelligence shared across the entire SAP security boundary.

Hybrid cloud-data center deployments present multiple, continually evolving edges that require a single security context. A high-level view of a two-tiered, hybrid deployment is depicted in Figure 14. The data center shows the typical enterprise resource planning (ERP) system on a software-defined stack. Network segmentation is implemented as microsegmentation with FortiGate NGFW policies attached at each virtual network interface card (VNIC). Similarly, the cloud is deployed on the cloud provider's SDN with subnet-level segmentation with east-west and north-south inspection between application tiers. This model aligns with version 2.0 of the SAP Security Baseline Template for segmenting SAP application zones. Identity services are synchronized from the data center into cloud single sign-on (SSO).

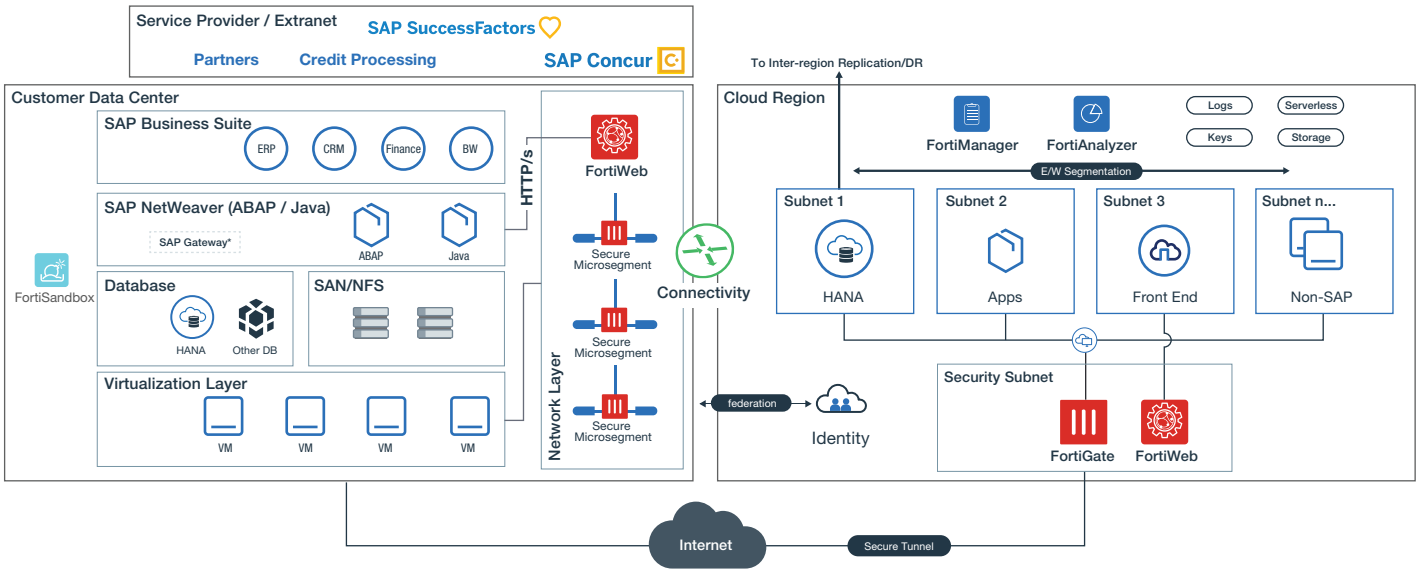


Figure 14 Hybrid Infrastructure Security

A single-point truth and management for policies are deployed in the cloud (though it can be deployed anywhere) and manage security across the entire domain. Threat intelligence should be coordinated to ensure a single view of the active threat landscape. In this way, policy can be activated in real time, relative to correlated indicators of compromise across the hybrid footprint. Fortinet FortiManager and FortiAnalyzer coordinate the management and threat intelligence everywhere Fortinet network security is deployed. FortiManager and FortiAnalyzer can be deployed on-premises or in the cloud. In Figure 14, management is deployed into the cloud to coordinate the entire security deployment across the hybrid environment.

Next-generation software-defined data centers (SDDCs) and clouds run on SDNs that are API-driven. The rich metadata of the SDN benefits security by providing information on the objects and networks in the SDN. FortiGate NGFWs farm this metadata through Fabric Connectors to implement dynamic policies. As SAP workloads are pushed into production, metadata filters inform the FortiGate on how to apply policy. This automation drives business intent and non-blocking production security for new service deployments.

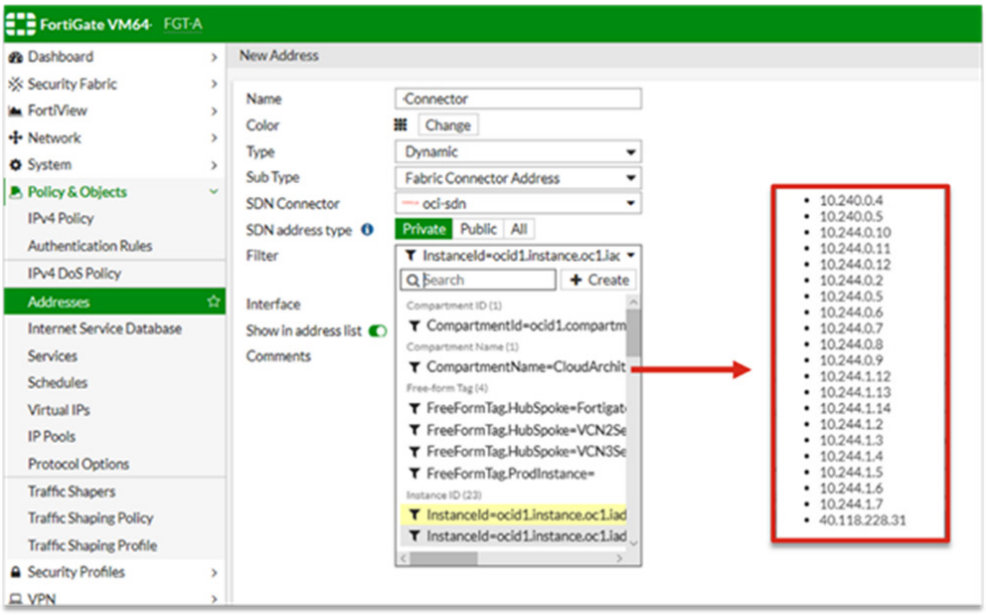


Figure 15 Fabric Connector Dynamic Filter

7.6 The SAP Web Dispatcher Case

SAP S/4 shifts much of SAP's user interaction from SAP GUI to a user's browser and HTTP/s protocol. As this encrypted web traffic grows, the opportunity to exploit common web vulnerabilities expands, creating a larger attack surface. Web Dispatchers are deployed for load balancing to SAP Fiori systems. Still, they lack any ability to protect back-end resources from cross-site scripting, SQL injection, JavaScript exploits, and other common Open Web Application Security Project (OWASP) attacks. SAP recommends maintaining end-to-end encryption along with appropriate patching. While this is a best practice, most malware is encrypted as well, which still leaves a gap in protection.

FortiWeb web application firewall (WAF) is a dedicated HTTP/s protection platform that goes beyond protecting known OWASP Top 10 threats to implementing auto tuning and machine learning. FortiWeb does this while maintaining full-length encryption and only decrypting locally to support inspection. FortiWeb lifts the burden of cumbersome manual tuning and distracting false positives. FortiWeb looks for the user's habits and patterns to build security tailored to the sessions that should be permitted. FortiWeb goes beyond firewalling to providing virtual patching. FortiWeb can be deployed as a physical or virtual instance or as Software-as-a-Service (SaaS) as the most effective way to protect your web services in SAP.

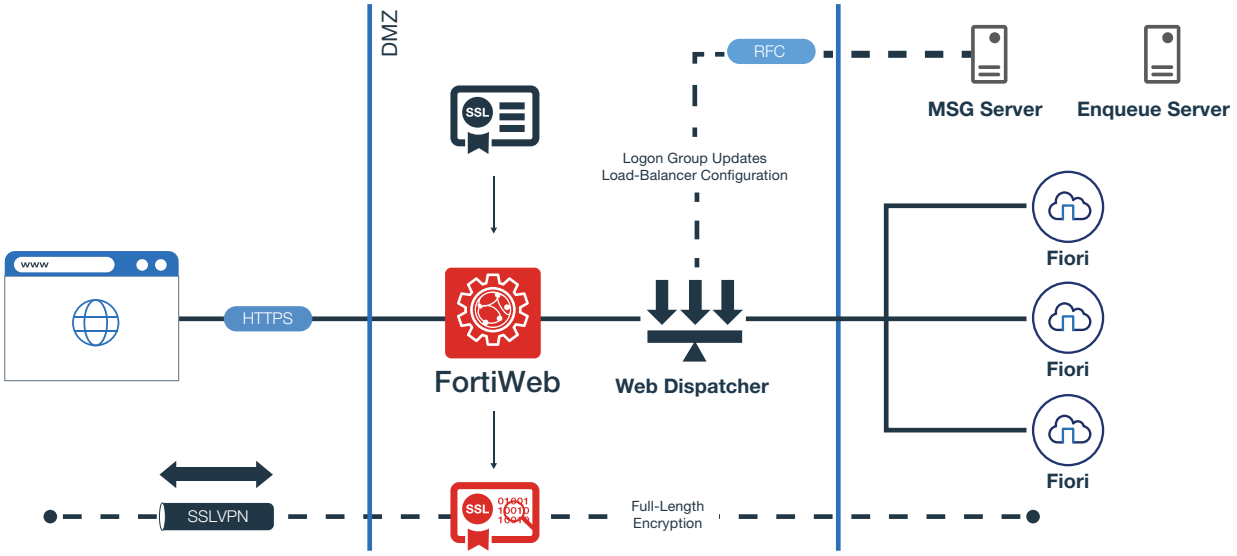


Figure 16 FortiWeb Web Application Firewall protects SAP Web Dispatcher traffic using AI and ML

7.7 SAP Compliance

With the increase in hybrid architectures and cloud usage, userbase and resources have become perimeterless, in the sense that they are now distributed across landscapes and infrastructure, especially in the cloud world as organizations adopt multi-cloud environments to reduce concentration risk. Fortinet brings tools to security teams such as FortiCWP cloud workload protection (CWP). Using FortiCWP, security teams can evaluate their cloud configuration security posture, detect potential threats originating from misconfiguration of cloud resources, analyze traffic across cloud resources (in and out of the cloud), and evaluate cloud configuration against best practices. It enables the ability to manage risk throughout multi-cloud infrastructures, provides regulatory compliance reporting, and integrates remediation into the cloud infrastructure life cycle automation framework. Fortinet enables automatic tracking of risk and compliance that is monitored continuously. Reports are generated in a single centralized dashboard across your public cloud providers for holistic monitoring. Fortinet enables a holistic understanding of the risk posture and compliance levels of SAP resources deployed in the cloud, considering the overall ecosystem and not only the SAP landscape.

This level of granularity gives the CISO teams a single pane of glass to track risk and generate the National Institute of Standards and Technology (NIST), Security Operations Center (SOC), and General Data Protection Regulation (GDPR) reports. CISCO teams can provide a security health snapshot of the SAP landscape within the organizational context.

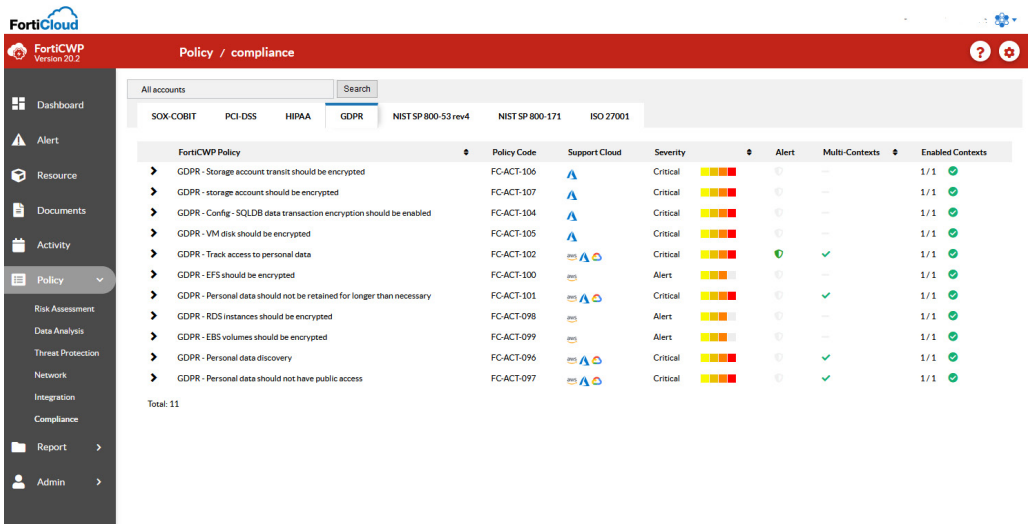


Figure 17 FortiCWP GDPR security controls

FORTINET

Executive Summary

Compliant with this Policy | Non-compliant with this Policy | This Compliant Policy is disabled

Reference	GDPRGuideline	Policy	Result	Description
Article 5 (1)e)	Checks if Personal data have exceeded retention time	GDPR - Personal data should not be retained for longer than necessary	✗	4950 pass/166 fail
Article32 (1)	Article 32 (1), Security of processing: the controller and the processor shall implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk, including inter alia, as appropriate: the pseudonymization and encryption of personal data	GDPR - RDS instances should be encrypted	✗	0 pass/1 fail
		GDPR - EBS volumes should be encrypted	✗	0 pass/15 fail
		GDPR - EFS should be encrypted	✗	0 pass/1 fail
		GDPR - Config - SQLDB data transaction encryption should be enabled	✓	1 pass/0 fail
		GDPR - VM disk should be encrypted	✗	0 pass/6 fail
		GDPR - Storage account transit should be encrypted	✗	15 pass/2 fail
		GDPR - storage account should be encrypted	✓	17 pass/0 fail
Article30(1)(2)	Article 30 (1) (2) Records of processing activities	GDPR - Track access to personal data	✓	0 access logs

Figure 18 FortiCWP GDPR example compliance report

8. Fortinet Reference Architecture for SAP

8.1 High-Level Summary of This Section

Each public cloud provider referenced below offers SAP reference architectures based on their best practices. These formed a baseline together with the Fortinet best practices to secure public cloud. The resulting architectures provide added security and optimized connectivity of an SAP landscape in the public cloud toward other SAP landscapes, users, and third parties on-premises as well as in the cloud.

8.2 Reference Architectures for SAP S/4HANA in Public Cloud

8.2.1 SAP S/4HANA on Microsoft Azure

Microsoft Azure's architecture starts from a Hub-Spoke setup where each SAP landscape can be segmented and inspected at a hub location. This setup aligns well with the Fortinet Cloud Security Service Hub concept. In the central hub, a FortiGate and FortiWeb installation is set up to scan the traffic. Both FortiGate and FortiWeb can be deployed as an Active/Passive High Availability setup, an Active/Active setup, or an Autoscaling setup. Depending on the environment requirements, these setups are the most optimal based on throughput, uptime, and complexity requirements. To take a head start, templates in ARM and Terraform are available on our github.

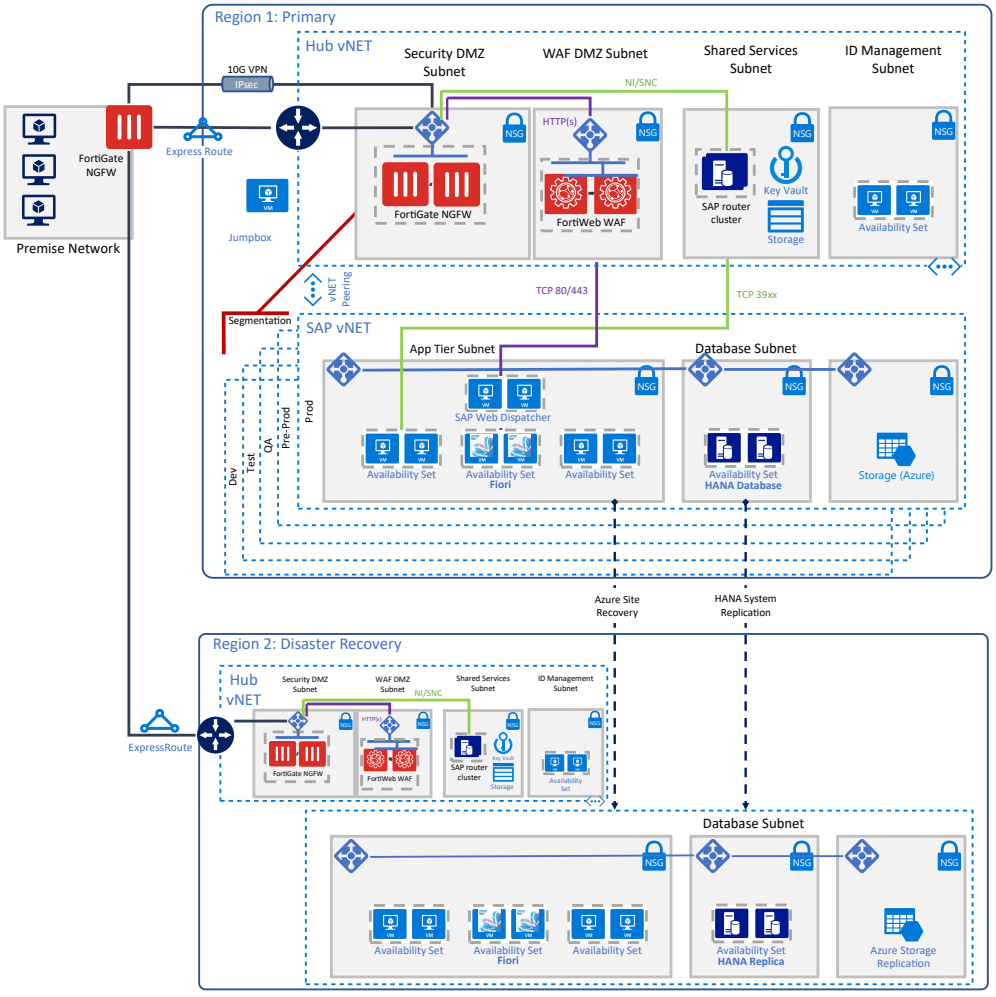


Figure 19 Fortinet Reference Architecture for SAP S/4HANA on Microsoft Azure

8.2.2 SAP S/4HANA on Amazon Web Services (AWS)

AWS provides Quick Start reference architectures in both single AZ and multi-AZ environments. These reference architectures include a DMZ/Public subnet where the FortiGate and FortiWeb instances are deployed. The FortiGate provides the connectivity security entry point into the network. Over Direct Connect as well as via Internet Protocol security (IPsec) over the internet, inbound connections are controlled and passed on to the back-end systems after inspection.

For any HTTP(S) related services such as SAP Fiori, we direct the traffic toward the FortiWeb for inspection at the Layer 7, including machine learning of a model of your traffic as well as authentication and protection against different common web vulnerabilities.

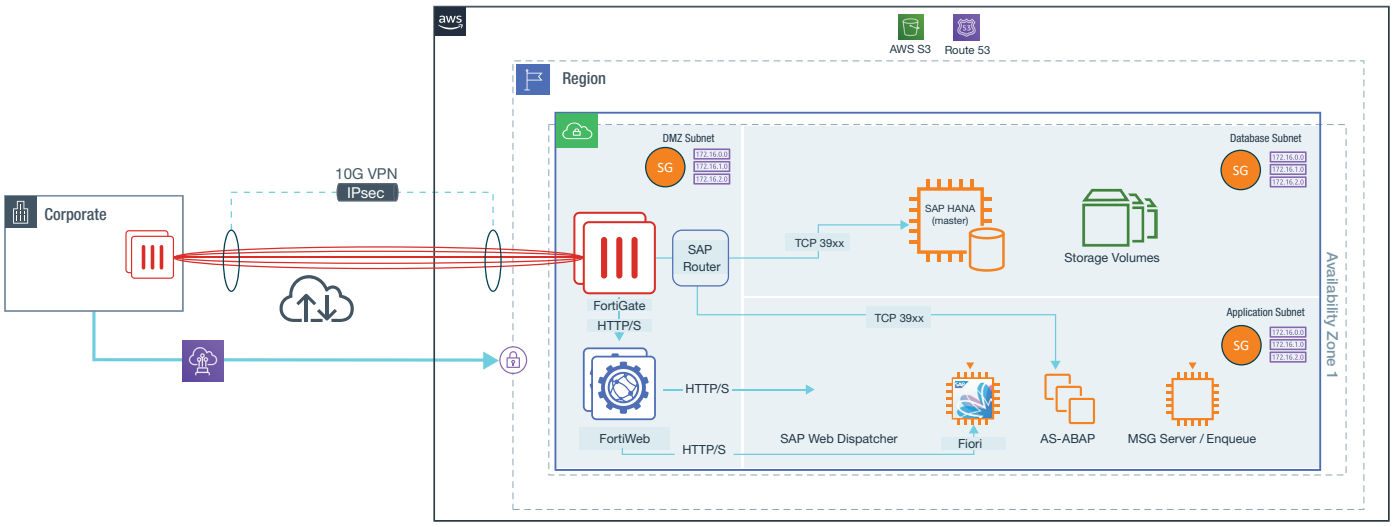


Figure 20 Fortinet Reference Architecture for SAP S/4HANA on AWS

8.2.3 SAP S/4HANA on Google Cloud

Google Cloud offers specific SAP architectures and advisories to their customers. Based on these architectures, we can start adding additional security and optimize the connectivity of an SAP landscape toward other SAP landscapes, users, and third parties.

Google Cloud SAP Architectures:

For Google Cloud, the architecture includes protection and traffic inspection for both north-south and east-west traffic flows between the different virtual private cloud (VPC) networks containing an SAP landscape or shared services. The diverse SAP landscapes can be either in a different stage in the production (development, test, production) or SAP landscapes that are unrelated to each other and performing various functions for different parts of the operations.

In this design, traffic between the shared services such as the SAP Router and the Application Server in the production VPC is inspected using the FortiGate. All inbound traffic, as depicted in Figure 21 (Fortinet Reference Architecture for SAP S/4HANA on Google Cloud) is examined by FortiGate (TCP 39xx, NI RCP/DIAG/…, HTTPS) or by the FortiWeb (HTTPS). Once inside the VPC, traffic between the SAP landscapes can be allowed or blocked using the ACLs in Google Cloud.

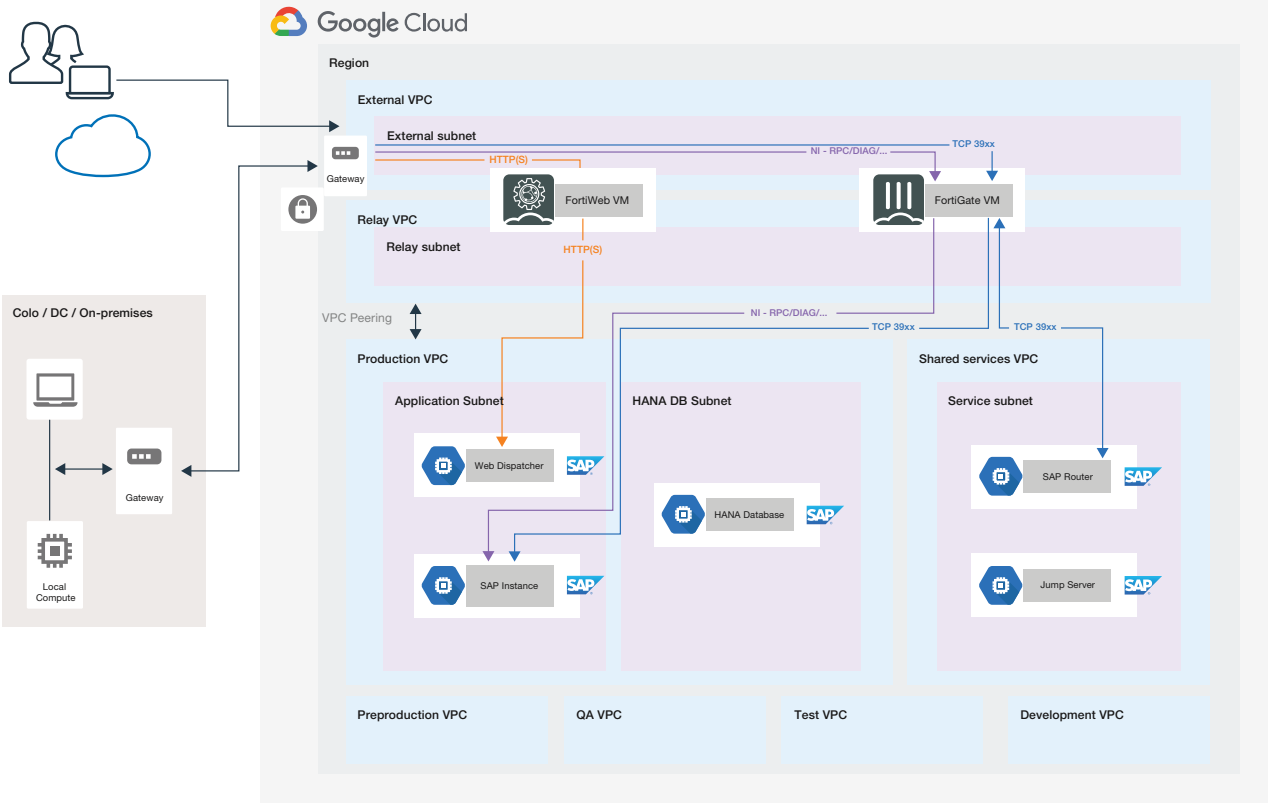


Figure 21 Fortinet Reference Architecture for SAP S/4HANA on Google Cloud

SAP landscapes are an essential part of the business engine driving your company. As such, it is important to have a disaster recovery strategy for these environments. Various components in the SAP landscape can be replicated as suggested by Google in this link.

The FortiGate and FortiWeb can be deployed in the DR environment either with a backup config using cloud-init or linked to a central management system.

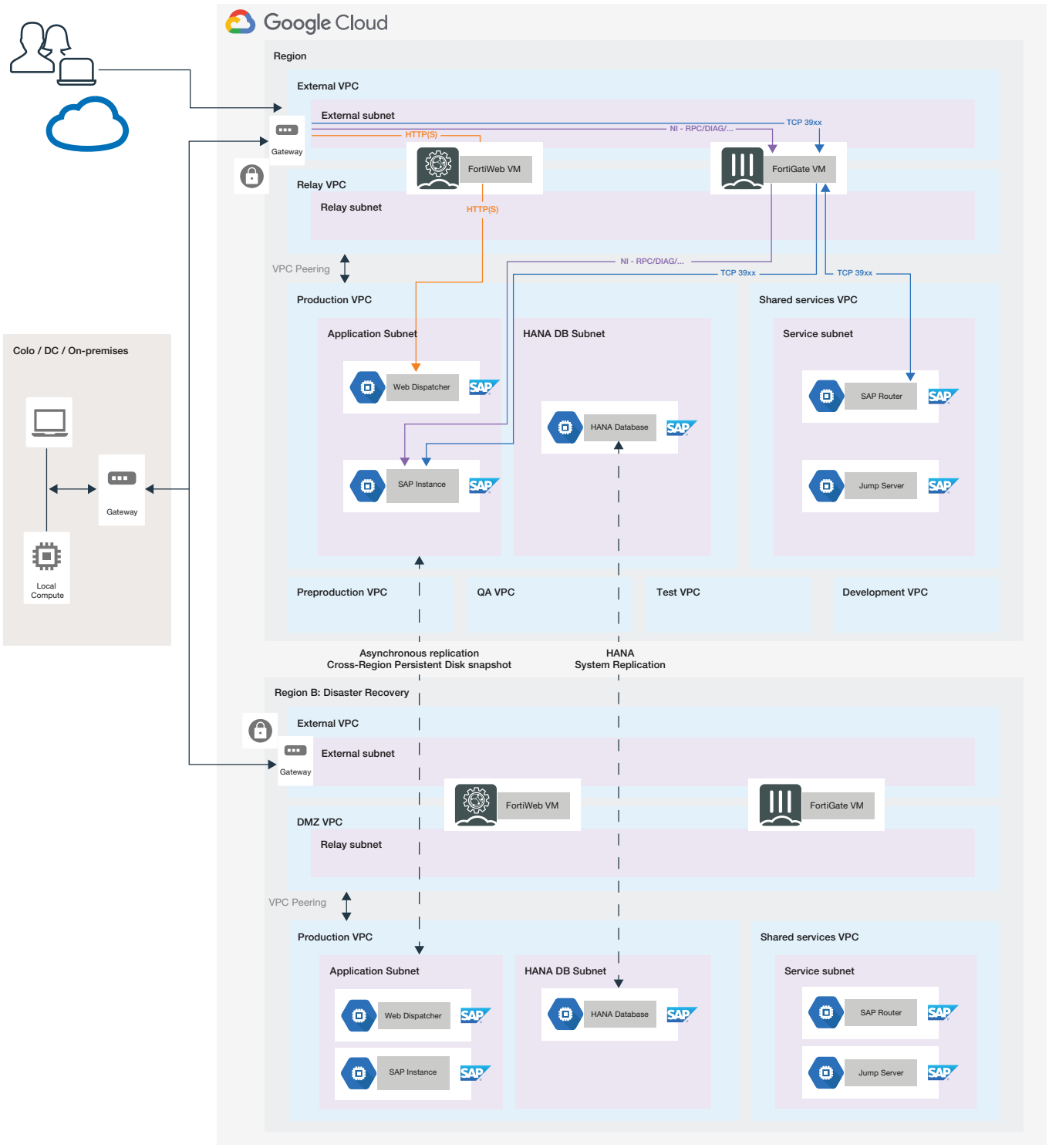


Figure 22 Fortinet Reference Architecture for SAP S/4HANA on Google Cloud with disaster recovery

8.3 Reference Architecture for Hybrid Environment

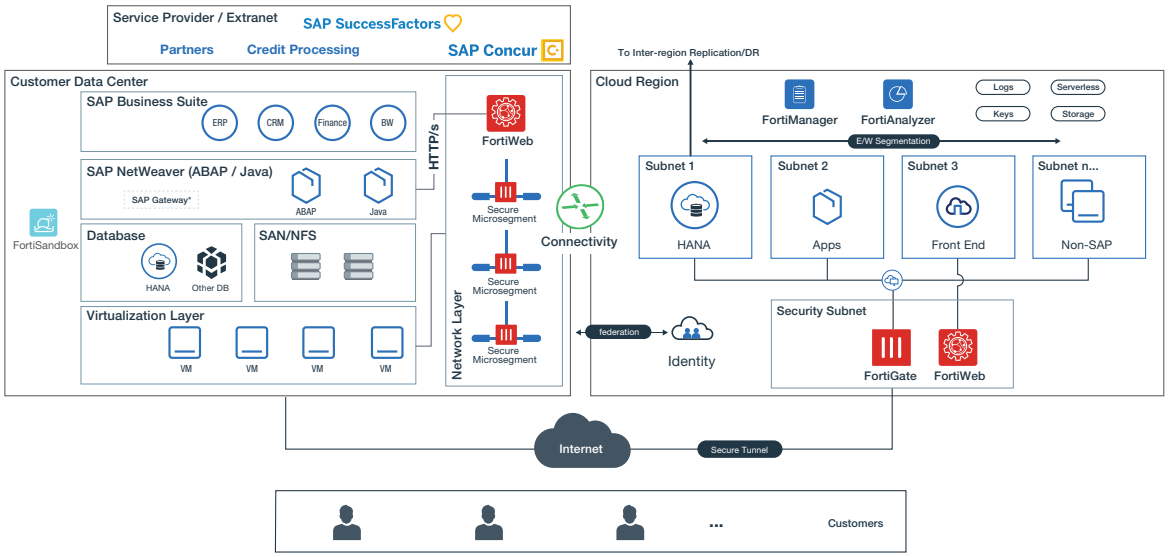


Figure 23 Fortinet Reference Architecture for SAP S/4HANA in Hybrid Environment

9. Conclusion and Actions

SAP is a business's most critical business application in its ability to create value by organizing, operationalizing, and monetizing complex data. For these reasons, great care must be given to protect SAP's infrastructure and systems. This becomes especially difficult for migrations from traditional data centers to S/4HANA running in the cloud, creating the opportunity for blind spots in the security posture. While cloud providers have solutions for basic network filtering, they lack deep application visibility and have no effectiveness beyond their own edge. Fortinet's holistic coverage ensures SAP systems are protected and that security policy and visibility remain unified across the hybrid and multi-cloud footprints. Fortinet eases skills gaps and correlates events through machine learning and workflow automation, multiplying the scale of basis, network, and security administrators.

Fortinet's contributions to SAP's protection align with and fill gaps in SAP's security baseline template by addressing infrastructure security and aligns to the SAP Secure Operations Map. User web interfaces and other HTTP front ends are protected by the Fortinet advanced web application firewall, FortiWeb, using advanced machine learning that monitors SAP users' behavior to tailor protection and minimize false positives. FortiWeb protects against OWASP attacks, including SQL injections, cross-site scripting, DoS, and novel attacks such as 10KBLAZE. The Fortinet FortiGate NGFW addresses the security baseline by providing east-west segmentation with the ability to inspect SAP transactions for known CVEs and evolving exploits. The need for this protection is pronounced by the difficulty in patching complex SAP production systems and the continual onslaught of advanced persistent threats.

Executives and Management Approaches to Protecting Your Business

	Topics of Concern	Challenge	Approach	Fortinet Solution
Executive and Management Chief Information Security Officer (CISO) Head of IT Infrastructure Lines of Business Manager SAP Program and Security Manager	Threat landscape for SAP software is shifting	Attack surface is broader and deeper due to SAP Fiori, IoT, etc. Adding more security products creates complexity	Integration for real-time visibility Break down security silos for multi-cloud environments Manage all security entry points (Fiori, IoT devices)	Reduces risk exposure by dynamically adapting to changes in the attack surface such as new endpoints and access points High-performance security intelligently adapts to traffic fluctuations and scales to address requirements such as SSL inspection
	Cloud deployments increase complexity	Proliferation of point products Sophistication of threats makes it increasingly more difficult to manage security	Automate manual intrusion and prevention and detection and incident response processes Agile scale and flexibility to accommodate new security requirements	Integration of different security products into a single fabric streamlines communications, reduces complexity, and enables virtual real-time responses Built-in (within the OS) regulatory/ standards controls and reporting that help support efforts for compliance for execs and board Automates manual security processes
	Rapidly changing advanced threats	Traditional security technologies are ineffective Volume of security alerts is overwhelming and leads to paralysis when it comes to prioritizing vulnerabilities	Solutions that enable transition from reactive to proactive security posture Use AI and ML, including automation, to reduce time-to-detection and time-to-response	Security fabric that includes end-to-end security capabilities—from identification and detection of threats, to prevention of threats, to detection and response of breaches, to recovery from intrusions and/or breaches Advanced threat prevention using sandboxing and intelligence network that seamlessly integrates with the entire security fabric Comprehensive threat posture scoring; compliance tracking and reporting for the boardroom

9.1 Technical and Operations Approaches To Protecting Your Business

	Topics of Concern	Challenge	Approach	Fortinet Solution
Technical and Operations SAP Basis Consultant SAP Security Architect or SAP Security Administrator SAP Application Architect Risk Management and Security Professional	Threat landscape for SAP software is shifting	Attack surface is broader and deeper due to SAP Fiori and smart devices The modern SAP system connects to more interfaces—connections to other SAP and non-SAP systems that are internal and external to an organization	Fragmented security architectural approaches must be replaced with a security fabric that broadly addresses an expanded attack surface perimeter, integrates each of the security elements for real-time threat intelligence sharing, and automates detection, prevention, and remediation processes	The Fortinet Security Fabric is the only true end-to-end network security solution that addresses digital transformation through automated device recognition and network, application, and user segmentation that blocks malicious intrusions and prevents them from spreading
	SAP deployments may involve multiple landscapes spread across a hybrid premises and cloud footprint	SAP deployments are more complex, making it challenging to protect against Many organizations end up with a proliferation of point products that leads to more complexity	Organizations require a new architectural approach that integrates the various security elements into a fabric that automates manual detection, prevention, and remediation processes as well as compliance tracking and reporting	By integrating security elements into a holistic architecture, the Fortinet Security Fabric enables organizations to unlock automation processes related to threat detection, prevention, and remediation and demonstration of compliance with security and industry regulations
Others Anyone responsible for the security of the SAP landscape	Cloud infrastructure increases security risk for SAP	Currently SAP does not provide guidance on infrastructure security SAP does not provide any rules on how SAP systems can prevent security attacks with today's technologies available to cyber criminals	A security architecture must deliver advanced threat protection by enabling real-time threat intelligence sharing and sandboxing for proactive threat detection, prevention, and remediation Modern security architectures must leverage AI/ML capabilities that deliver real-time threat intelligence that keep pace with threat volume, velocity, and sophistication	Fortinet provides higher security to protect SAP Router and SAP components on the network layer before an attacker can access the SAP system Fortinet web application firewall (WAF) protects the SAP system from SQL injections or cross-site scripting Physical FortiGate NGFWs are equipped with proprietary hardware acceleration that offloads encryption functions to a security processing unit The Fortinet Security Fabric provides proactive advanced threat detection, prevention, and remediation capabilities through sandboxing and threat intelligence across each security element in real time, which shrinks intrusion-to-detection and detection-to-remediation windows Advanced persistent threat (APT) and advanced evasion technique (AET) capabilities that integrate AI/ML-enabled threat intelligence features

10. References

[1] "SAP S/4HANA Intelligent ERP System," SAP, accessed July 20, 2020.

[2] "Strategy - Extended Innovation Commitment for SAP S/4HANA Clarity and Choice on SAP Business Suite 7," SAP, accessed March 10, 2020.

[3] "Make the move to SAP S/4HANA with Microsoft Azure," SAP, accessed July 14, 2020.

[4] "SAP Company Information," SAP, accessed June 10, 2020.

[5] Steve Evans, "Cloud Use Increases Attack Surface, But Security Not Keeping Up," Infosecurity, August 22, 2016.

[6] Stefan Hoechbauer, "Embracing the Hyperscalers, Your Fast Lane to Becoming an Intelligent Enterprise in the Cloud," SAP, May 9, 2019.

[7] Gary Slater, "SAP and Google Cloud partnership: Our joint cloud journey continues," SAP, June 12, 2020.

[8] "SAP ONE Support Launchpad," SAP, accessed October 6, 2020.

[9] "Alert (AA19-122A)," Cybersecurity & Infrastructure Security Agency, May 3, 2019.

[10] "Comae Technologies/OPCDE Repository," GitHub, accessed June 10, 2020.

[11] "EVB Energy Ltd Smart Meter," Wikimedia Commons, accessed July 21, 2020.

11. Table of Figures

Name	Severity
IPS Signature 53/2056	
SAP.Crystal.Reports.Path.Traversal	
SAP.EnjoySAP.ActiveX.Control.Command.Execution	
SAP.GUI.BI.Wadmxhtml.DLL.ActiveX.Control.Access	
SAP.GUI.Regsvr32.Rule.Security.Policy.Bypass	
SAP.GUI.SAPBExCommonResources.ActiveX.Command.Execution	
SAP.MaxDB.Malformed.Handshake.Request.Code.Execution	
SAP.Message.Server.Group.Parameter.Remote.Buffer.Overflow	
SAP.NetWeaver.AdIExecBlkConv.Message.Server.Buffer.Overflow	
SAP.NetWeaver.LM.Configuration.Wizard.Authentication.Bypass	
SAP.NetWeaver.Message.Server.Memory.Corruption	
SAP.NetWeaver.SOAP.Arbitrary.Command.Execution	
SAP.NetWeaver.UDDI.Server.SQL.Injection	
SAP.Netweaver.DiagTraceR3Info.Remote.Buffer.Overflow	
SAP.Systems.Anonymous.Users.Remote.Command.Execution	

Figure 24 Sample of Fortinet IPS Signatures for SAP with High Severity

Application Signature 4/675			
SAP.Diag	Business	Client-Server	★★★★☆
SAP.Message.Server	Business	Client-Server	★★★★☆
SAP.Router	Business	Client-Server	★★★★☆
SAP.Web.Dispatcher	Business	Client-Server	★★★★☆

Figure 25 Fortinet Application Signatures for SAP

Name
Predefined Internet Services 15/524
SAP-DNS
SAP-FTP
SAP-HANA
SAP-ICMP
SAP-Inbound_Email
SAP-LDAP
SAP-NetBIOS.Name.Service
SAP-NetBIOS.Session.Service
SAP-NTP
SAP-Other
SAP-Outbound_Email
SAP-RTMP
SAP-SSH
SAP-SuccessFactors
SAP-Web

Figure 26 Fortinet predefined Internet Services for SAP

www.fortinet.com

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, Cloud, or mobile environments. Fortinet ranks number one in the most security appliances shipped worldwide and more than 450,000 customers trust Fortinet to protect their businesses.
Fortinet, 899 Kifer Road, Sunnyvale, CA 94086, USA