SAP SYSTEMS ANALYSIS

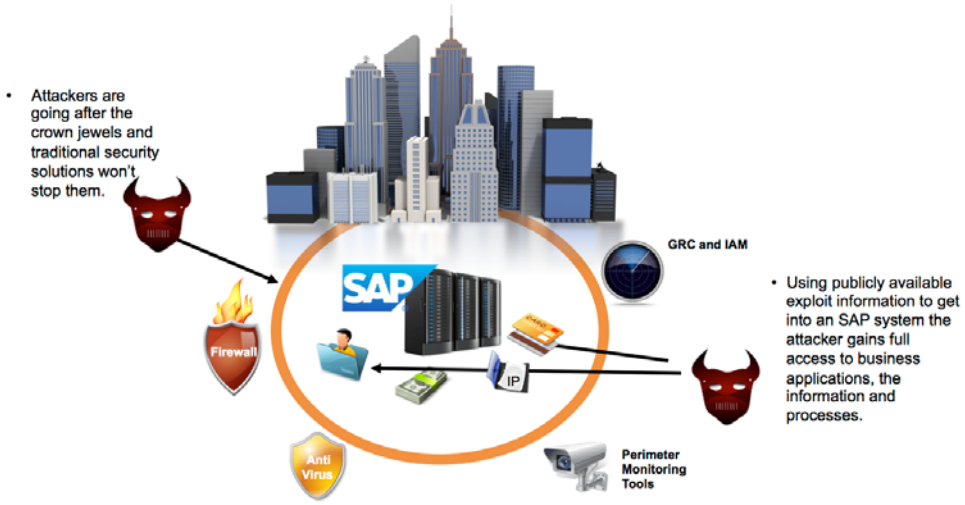
Business Risk Illustration

onapsis

Key Trends in Business Critical Application Security

Virtually every SAP application is vulnerable to financial fraud, sabotage or espionage from cyber-attacks targeting these business-critical enterprise systems.

They are the lifeblood of the world's largest companies as they manage their most sensitive information and processes such as ERP, HCM, CRM, BI and Supply Chain Management. Despite housing an organization's "crown jewels" - intellectual property, financial, credit card, customer data, supplier data and database warehouse information – SAP systems and their application layer are not protected by traditional security solutions.



"Traditional security methods such as Segregation of Duties (SoD) and having SAP Access Controls in place have never been an effective means for preventing cyber-attacks against the application layer. Additionally, traditional security vendors do not continuously monitor and secure SAP applications let alone offer detection and response capabilities necessary for a fully scalable and enterprise class solution to secure the SAP enterprise application layer from attacks. In today's day and age there is no longer an "internal" Network as many enterprise applications such as SAP are connected to the Internet (Web apps, HANA, Mobile, Cloud deployments, etc). As these applications are increasingly moving to a hybrid cloud model, with mobile and IoT environments, their attack surface is expanding.

> *A recent study by the Onapsis Research Labs found that over 95% of SAP systems assessed are exposed to vulnerabilities that could lead to full compromise of the company's business processes/information. Most vulnerabilities could be exploited anonymously and remotely.*

Quick Stats in Business Critical Application Security

- SAP has released 3300+ security patches to date.
- In 2014 alone, 391 were released - averaging 30+/month; Over 46 percent of them were ranked as "high priority."
- Based on a sample of 152 vulnerabilities reported by Onapsis in the period 2009-2014, on average: SAP spent 12 months fixing vulnerabilities (from the moment a researcher finds a vulnerability and reports it to SAP, until SAP delivers a patch to the market).
- In 2015 the Chinese Breach of USIS targeted SAP, this went unnoticed for over six months and compromised over 48,000 employee records of DHS and OPM.
- Oracle spent almost two years fixing 20 vulnerabilities reported and it is taking over five months to fix a more recent set of newly discovered vulnerabilities.
- Applying a patch could take customers more than six months- from the time the patch is delivered to the market until its deployed. Often, companies are running systems without a clear update and patching process.

Critical Assets and Processes are Targets of Attack

Business-critical applications running on SAP continue to be the best "economics" for cyber attackers as these systems house the most critical assets and support the most mission-critical business process. Unfortunately, they are also the highest cost blind spot for many Chief Information Security Officers, as their current security products do not include business-critical applications running on SAP.

Intellectual Property

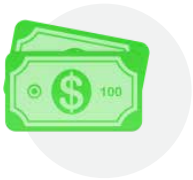
High value industy data

Sensitive Customer Information

High volume customer data

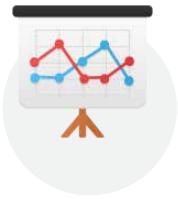
Business process trade data

Competitive insights



Treasury and Cash

Corporate bank accounts



Financial reporting insights

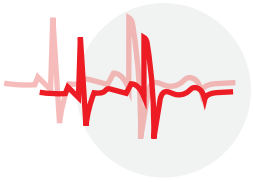
Inside financial information

Sensitive employee information

High volume employee data

Network front door

Access point to
the corporate network



Life blood of the business

Single point of
operational failure

In addition to not having proper security products for protecting SAP enterprise applications, organizations also struggle to understand the complete scope of all of critical assets and processes housed on these systems. Additionally, each industry has different priorities based on the nature of their business and faces different compliance pressures such as PCI, SOX, FISMA, and NERC.

Onapsis Business Risk Illustration

The Onapsis Business Risk Illustration (BRI) helps an organization frame the business risk of an SAP cyber attack. This is achieved by examining your organization's SAP application layer for existing known vulnerabilities.

To do so, Onapsis engages on-site with multiple people across your organization such as the CIO, Chief Information Security Officer, Information Security professionals, Compliance and Audit departments, as well as members of SAP security teams to:

Understand your SAP landscape, its primary usage and processes as well as the key informational assets it manages.

Install BRI software on your organization's BRI host machine. Hardware to be fingerprinted.

Run the Business Risk Illustration

Correlate results of found vulnerabilities to your organizations corporate risk posture to determine top risks to the business.

Provide recommendations for security coverage.

Our Approach

The methodology and tools that power the Onapsis Business Risk Illustration leverage our expertise in SAP enterprise application security. Our patented technology adapts to understand known vulnerabilities in an SAP system and outlines different threat vectors and approaches that attackers can use to exploit them.

Our Patented Technology

As of April 14th, 2015, Onapsis has been issued **U.S. Patent No. 9,009,837** entitled "Automated Security Assessment of Business-Critical Systems and Applications," which describes certain algorithms and capabilities behind the technology powering the Onapsis Security Platform™ and Onapsis X1™ software platforms.

Our SAP Experts

Onapsis Research Labs provides the industry's leading intelligence on security threats impacting SAP systems. Our experts continuously work to discover, investigate and disclose evolving vulnerability information relating to SAP.

Onapsis Analysis of Business Risk Illustration Results

BRI Results are Designed to Provide Actionable Insight

Upon an initial scan of your organization's SAP systems, our Business Risk Illustration will identify and prioritize remediation for existing vulnerabilities within your systems, and will tell you which systems are specifically effected. The results of the Business Risk Illustration are broken down based upon effected SAP systems. An explanation of the business impact for each critical risk found is provided.

RISK	LEVEL RISK	BUSINESS IMPACT
External RFC Server Registration Enabled	 **HIGH**	It is possible to execute administrative methods without specifying valid access credentials in the SAP Mgmt Console. Under this configuration, a malicious party will be able to perform sensitive operations on the SAP system, such as obtaining configuration information and launching Denial of Service attacks.
Insecure remote connection to SAP Message Server	 **HIGH**	In this scenario, a remote attacker would be able to perform complex attacks such as Denial of Service (DoS), man in the middle, and traffic sniffing. These attacks may result in the entire compromise of the SAP system.
ICM WebGUI BSP Application is Enabled	 **HIGH**	The WebGUI service is enabled in the SAP ICM server. This service provides an SAP GUI interface over the HTTP protocol. If a remote attacker is able to obtain login credentials, he would be able to operate the SAP system interactively with a Web browser.

Building the Business Case

Organizations are challenged to prioritize budget dollars from their security spend and align it to a security strategy that will provide the best impact for business. The results of the Onapsis Business Risk Illustration will allow a security organization to map out their economic, financial, compliance and lost data risks to determine the best course of action. As the leading experts in SAP cybersecurity, Onapsis is the only vendor that can provide a Business Risk Illustration for your organization. This analysis helps to effectively show the impact of vulnerabilities that can be used to compromise your key data and business processes, and provides recommendations for how to prioritize and implement remediation's moving forward.

Operationalizing SAP Security

During the Business Risk Illustration engagement, Onapsis experts will educate a cross functional team from your organization to operationalize your organization on SAP cybersecurity best practices, and key elements from the provided illustration readout. Additionally, Onapsis will provide feedback on the best approach your organization can take to incorporate SAP into the information security vulnerability management process, initiate the remediation processes, implement detection controls, incorporate SAP into incident response, and leverage advanced threat intelligence from the Onapsis Research Labs.

Planning → Vulnerability Management → Remediation Program → Detection Controls → Response Program → Advanced Thread & Intelligence

Case Studies

Different industries use SAP for very specific business processes. Over the course of the last year, we've gathered data across various industries in order to understand the risks facing SAP systems and applications.

> *If our company's SAP system is breached it will cost us $22 million per minute.*
> *CISO of a Fortune 500 Company*

Manufacturing

When executing BRI's in this industry we found on average, 480 vulnerabilities including several critical risk vulnerabilities that would allow an attacker to take complete control of the SAP Application Server remotely. If impacted, manufacturing processes and designs could be stolen, and manufacturing systems could become disrupted.

Oil & Gas

When executing BRI's in this industry we found, on average, 127 vulnerabilities including many critical risk vulnerabilities that would allow an attacker access to or the ability change sensitive information on the SAP system. Specifically Capital Spend Effectiveness & Procurement, Digital Oilfield Operations, Hydrocarbon Supply Chain, Operational Integrity, Human Resources, and Finances could be accessed.

Aerospace

When executing BRI's in this industry we found on average 145 vulnerabilities including several critical risk vulnerabilities that would allow an anonymous remote attacker to read, write, delete or copy any business information. If impacted intellectual property could be stolen by nation states, which would compromise national security.

Pharma

When executing BRI's in this industry, we found that on average 130 vulnerabilities including several critical risk vulnerabilities that would allow the attacker to take complete control of the SAP Application Server remotely. If impacted, controlled drug recipes could be obtained, and replicated.

About Onapsis

Onapsis provides the most comprehensive solutions for securing SAP and Oracle business critical applications. As the leading experts in SAP cybersecurity, Onapsis enables security and audit teams to have visibility, confidence and control of advanced threats, cyber risks and compliance gaps affecting their enterprise applications.

Headquartered in Boston, Onapsis serves over 180 Global 2000 customers, including 10 top retailers, 20 top energy firms and 20 top manufacturers. Onapsis' solutions are also the de-facto standard for leading consulting and audit firms such as Accenture, IBM, Deloitte, E&Y, KPMG and PwC.

Onapsis solutions include the Onapsis Security Platform (OSP), which is the most widely-used SAP-certified cybersecurity solution in the market. Unlike generic security products, Onapsis' context-aware solutions deliver both preventative vulnerability and compliance controls, as well as real-time detection and incident response capabilities to reduce risks affecting critical business processes and data. Through open interfaces, the platform can be integrated with leading SIEM, GRC and network security products, seamlessly incorporating enterprise applications into existing vulnerability, risk and incident response management programs.

These solutions are powered by the Onapsis Research Labs which continuously provide leading intelligence on security threats affecting SAP enterprise applications. Experts of the Onapsis Research Labs were the first to lecture on SAP cyber attacks and have uncovered and helped fix hundreds of security vulnerabilities to date affecting SAP Business Suite, SAP HANA, SAP Cloud and SAP Mobile applications, as well as Oracle JD Edwards and Oracle E-Business Suite platforms.
For more information, please visit **www.onapsis.com**, or connect with us on **Twitter**, **Google+**, or **LinkedIn.**

To schedule an Onapsis Business Risk Illustration for your organization please contact Onapsis at

https://www.onapsis.com/services/business-risk-illustration

onapsis
RESEARCH LABS

About Onapsis Research Labs

Onapsis Research Labs provides the industry analysis of key security issues that impact business-critical systems and applications. Delivering frequent and timely security and compliance advisories with associated risk levels, Onapsis Research Labs combine in-depth knowledge and experience to deliver technical and business-context with sound security judgment to the broader information security community

Onapsis Security Platform

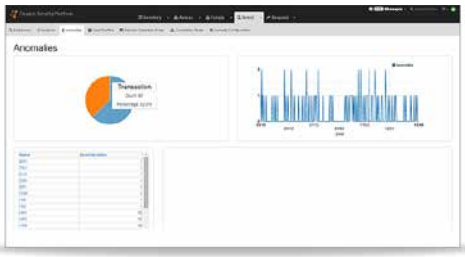
Provides organizations a holistically adaptive approach to focus on the factors that matter most to their business – critical applications running on SAP that house vital data and run mission-critical business processes. Delivers three solutions:

Vulnerability and Compliance

Identify all SAP infrastructure and generate graphical topology maps along with the connections between systems and applications.

Assess risks based on vulnerabilities and tie business context into remediation planning processes.

Performs audits to Identify compliance gaps and report when systems don't meet requirements based on policies and industry regulations.



Detection and Response

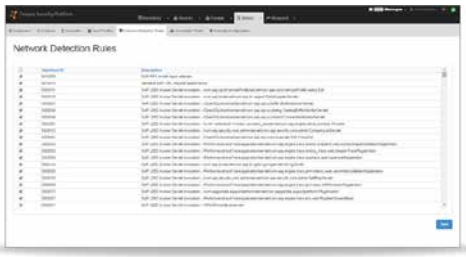
Continuous monitoring of advanced threats and anomalous user behavior on SAP infrastructure.

Provides visibility into attacks, with context, to determine if the attack is likely to be successful.

Leverages real-time reporting on the likelihood and impact of threats from SAP exploits.

Delivers attack signatures to identify anomalous user behaviors.

Detects system changes that make organizations more vulnerable to attack.



Advanced Threat Protection

Provides protection against SAP security issues for which no SAP note has been released for Onapsis customers to eliminate the risks.

Eliminates the window of exploitability and protects customers against known but unpublished vulnerabilities.

Customers who subscribe to Advanced Threat Protection receive signatures for exploitation attempts against zero day vulnerabilities.