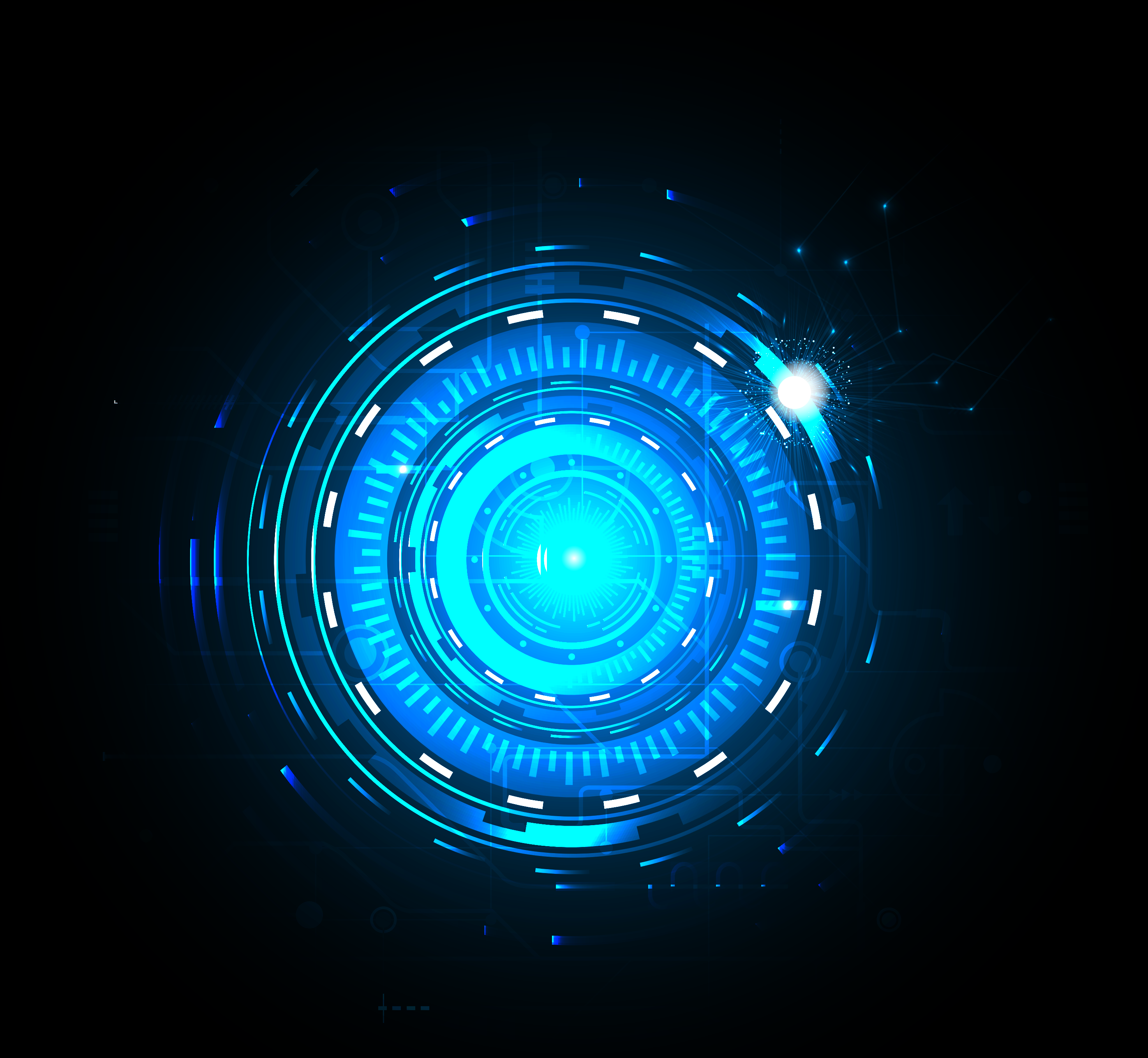


Towards a Zero Trust Architecture in SAP landscape

Executive Summary

In order to remain competitive, flagship organizations are running an array of technologies implemented throughout digital transformation programs that amplified their attack surface across the entire IT landscape. This exposure lead to a significant increase in the number of cyber security incidents, as the annual cost of cybercrime has risen by 72% over the past five years[1].

Cyber attackers are very sophisticated and are outmatching current cyber defenses. Therefore, a new security posture should be adopted to limit the access to valuable information in the event of a cyber incident. Zero Trust posture adopts the moto: “Never trust, always verify”. Our approach is based on this premise and it stands assuming every component may be vulnerable, every device needs authentication and validation.

For many organizations, SAP is a mission critical application.

This is why we launched a series of stories aiming to describe how organizations can protect SAP applications against cyber attacks proposing approaches and solutions in the market. The following stories will focus on different subjects:

- SAP Security Assessment with Deloitte’s SAP Security Framework
- Towards Passwordless Authentication in SAP Applications
- Efficient Access Governance in SAP Applications using SAP IAG
- Integrating a third-party IAM and PAM Solutions to Manage Identities in SAP Applications
- Continuous Monitoring and Threat Detection in SAP Applications
- Safeguarding Organization’s Data using AI Detection Tools to Detect Suspicious Behavior in Cloud Applications
- (More to come...)

Problem

Attacks on SAP ecosystems are becoming more popular as SAP applications run business critical processes for organizations. SAP stores critical data and supports business processes which make them more attractive for cyber attackers, who can create more damage and benefit from stealing data such as personal identifiable information, financial and transactional data.

There are many reasons that lead to this increase in exposure to SAP environments:

- **Digitization programs** introduced more complexity in the SAP architectural landscape and increases the number of services exposed to the internet;
- **Work from Home** and the ability to work from anywhere also results in the exposure of applications;
- The **adoption of cloud products and services** created new interfaces in the SAP landscapes;
- The demand for **efficiency in the supply chain** also created new ways of sharing information in real-time directly from SAP systems with third parties and other stakeholders.

According to the IDC survey from 2021, 62% of ERP systems may have critical vulnerabilities and 74% of ERP applications are accessible from the Internet [2]. These 2 factors combined create a perfect storm for the attacker to explore and exploit SAP services and applications, resulting in 64% of ERP deployments having experienced security breaches in the past 24 months [3]. This trend is causing severe losses for organizations that do not take actions to increase the maturity levels for SAP security.

One of the greatest barriers to manage cybersecurity across an organization is data management traversing complex perimeters (44%), followed by a need for better prioritization of cyber risk across the enterprise (31%) [4]. Security in SAP is challenging since the landscape is extremely complex not only on the architecture side with several interfaces but also on the complexity around each component in SAP.

[1] Source: The Cost of an SAP Cybersecurity Data Breach: https://explore.bowbridge.net/blog/cost-sap-cybersecurity-data-breach
[2] Source: IDC Survey – https://onapsis.com/IDC-survey-ERP-security-assessment
[3] Source: IDC Survey – https://onapsis.com/IDC-survey-ERP-security-assessment
[4] Source: Deloitte Cyber - 2021 Future of Cyber Survey – https://www2.deloitte.com/mm/en/pages/risk/articles/deloitte-global-2021-future-of-cyber-survey-finds-rapid-increase-in-cyberattacks.html

Zero Trust in SAP landscape

What is it?

Zero Trust changes the previous mindset with regards to trusted connections in a specific network: it drives to a trust no one attitude, replacing simple verification of user access with real-time access decisions based on a continuous risk assessment. Recent advances in computational power leveraged the possibility of continuous validation and the possibility to undertake that every component in an architecture is vulnerable, every layer needs protection and to be validated.

By requiring authentication and authorization for all connections to the system, the adoption of Zero Trust drives to:

1) A granular user access control considering the least privilege principle

2) Segmentation of the architecture requiring authentication mechanisms and preventing lateral movement;

3) Reducing risk by limiting the attack surface.

Zero trust is not a new technology, it reflects a cultural change and a set of architectural policies that are based on the fundamental principle of "never trust, always verify", where trusted connections are established based on internal and external factors, which are constantly revalidated.

Overall, the zero trust concept safeguards the network both from the outside and the inside by providing access service to users that are required to complete an authorized task. In the SAP context, it makes sure that no threat actors have access to data that is valuable, even if they are connected to the network environment. This can be achieved by authenticating devices and users on an ongoing basis, every time they use an asset.

Zero Trust in SAP landscape

Benefits

Zero Trust brings several strategic advantages:

Secure Connectivity

Attackers are not able to access any valuable data or the crown jewels by ensuring user authentication is performed in each possible interaction, specifically, accessing features, table visualization, program execution, and other actions that may be used to expose or exfiltrate information. This mindset helps safeguard against harmful security breaches even if the attacker is able to access the SAP environment, in particular, if third-parties or remote employees are compromised, attackers will have limited access to assets (to only applications they are authorized to access).

Optimized Performance

Other security concepts require extra layer such as firewalls, VPNs, and other technologies to assist in security. This concept leverages the existing functionalities to implement the segmentation, granular control and thus, secure the environment. Therefore, not comprising performance to achieve that.

Agility and Scalability

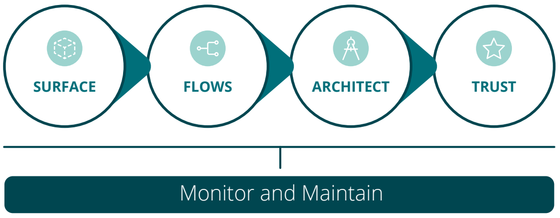
User permissions can be easily added and removed by the security teams in a Web UI. No additional software is required enabling working from anywhere, in or out of the company resulting in scalability and agility.

Productivity

Remote employees and third-party users can work directly in SAP instead of connecting to it. This transparent and smooth connection minimizes time, reduces frustration and overheads and increases productive work.

Approach to adopt a Zero Trust posture in SAP

While Zero Trust is relevant across all industries and sectors, there is no one-size-fits-all solution. The following practices should be considered to develop and implement a Zero Trust strategy in a SAP environment:



SURFACE

FLOWS

ARCHITECT

TRUST

Monitor and Maintain

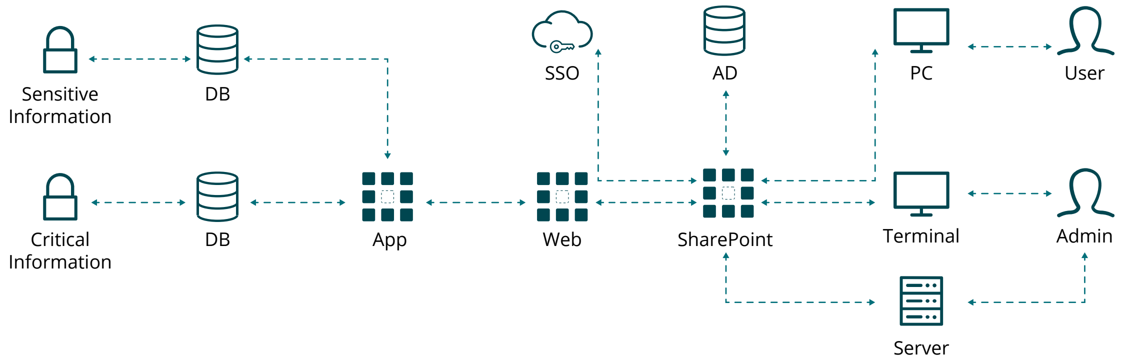
Surface

Investigate and locate which individual units/surface in the SAP environment must be isolated and protected. Identify applications, data, services and assets to be segmented and classify them according with their value.

D	Data	Protect surface **Sensitive Information (PPI - Personally Identifiable Information, Strategic, Financial, etc)**
A	Apps	Protect surface **SharePoint, etc...**
A	Assets	Protect surface **Infrastructure-related (Router, Switches, Cloud, IoT, Supply Chain, Desktops, etc)**
S	Services	Protect surface **Identity and Access Management (IAM), Previleged Access Management (PAM), etc**

Flows

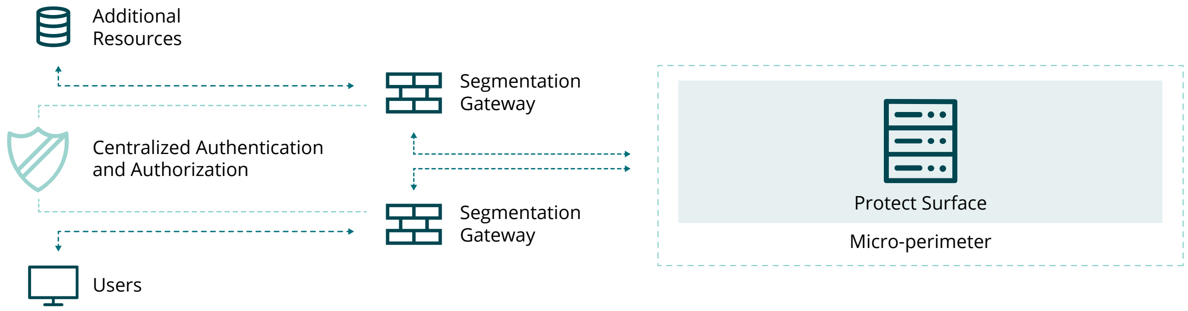
Map all existing flows and interactions in the surface and identify/categorize the type of traffic that is being transmitted. Use automated tools to assist in the mapping of interactions between data, applications, systems, and networks.



Approach to adopt a Zero Trust posture in SAP

Architect

Create segmentation gateways to define the perimeter of the identified surface using virtual, physical, or cloud-based next-gen firewalls (NGFWs) as segmentation gateways. Implement scalable security solutions to reduce bottlenecks, including an advanced and centralized authentication and authorization.



Trust

Create and implement a policy that identifies the following items:

- Who can access what;
- When is access granted or restricted;
- Where the user is located;
- How the resource is accessed;
- Why the user requires access.

Policy

Who	What	When	Where	Why	How	Action
User ID	**App ID**	**Time**	**System Object**	**Classification**	**Content ID**	
RH_User1	SAP ERP	Working Hours	Europe	Hiring Process	SAP GUI / SAP Fiori Launchpad	Allow
Admin_1	Domain Controller	Any	USA	User Management	PAM	Allow
...	...	...	...	...	...	...

All other authentication tentatives are refused

Approach to adopt a Zero Trust posture in SAP

Monitor and continuous improvement

Ensure event log collection and forward to SOC.

Security monitoring technologies compatible with SAP environments can assist by doing event correlation and threat detection to raise alerts which will be investigated by SOC teams. Deloitte has launched MSSP services specific for SAP environments that include constant monitoring, detection, and incident management in SAP ecosystems.

Continuous evaluation and lessons learned from possible security incidents in SAP ecosystems are also key to adopt a continuous improvement approach which is one of the pillars for a Zero Trust posture.

> Deloitte has launched MSSP services specific for SAP environments that include constant monitoring, detection, and incident management in SAP ecosystems.

[5] Security Operations Center: Centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

How can organizations begin this journey?

This journey starts with the identification of what to protect and prioritization on how to implement security controls. Since Zero Trust posture is not a one-size-fits-all approach, each organization considering this journey will face pitfalls and obstacles that requires technical expertise and commitment from the business to adopt a new way of working with SAP.

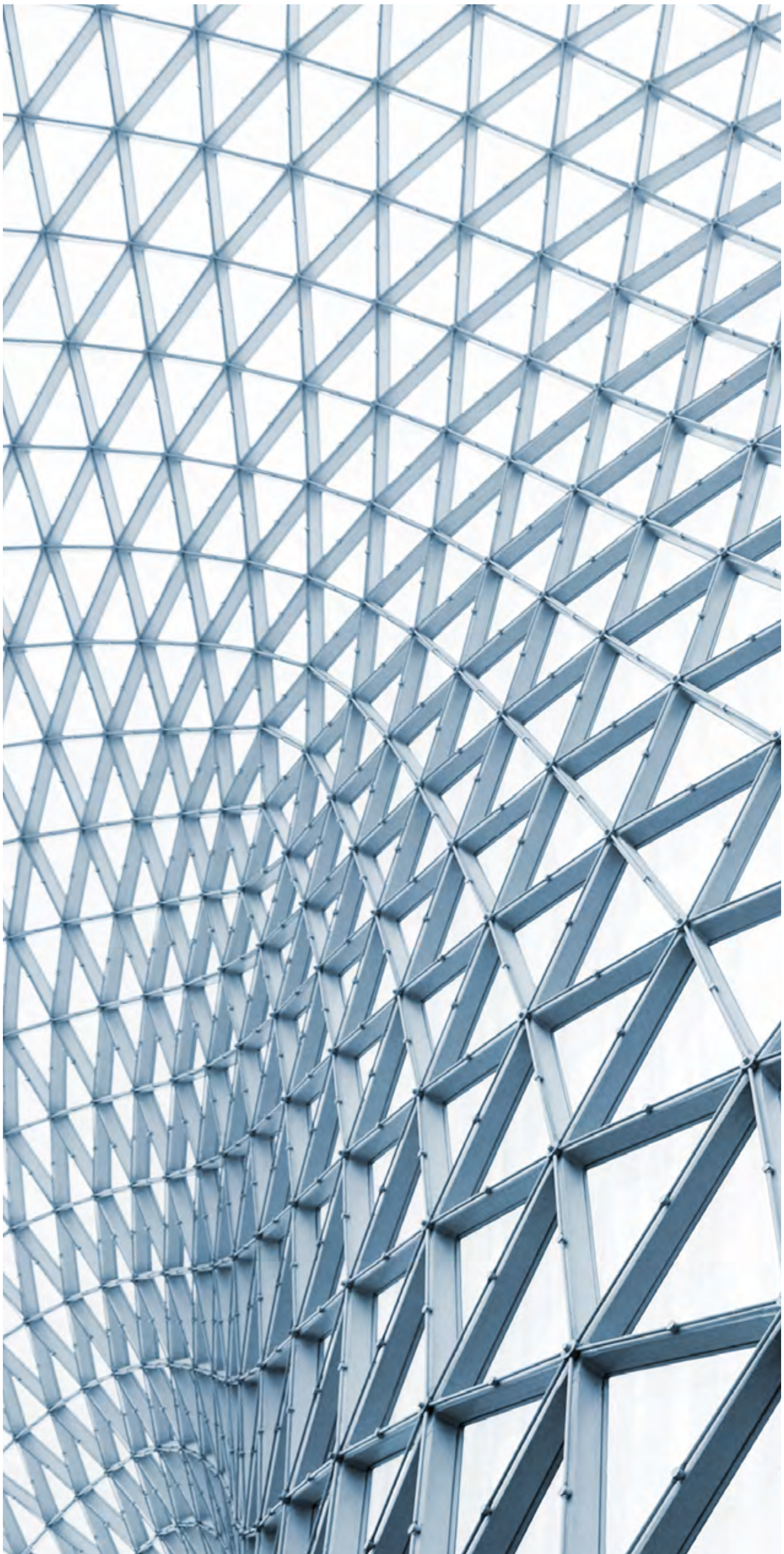
Deloitte created a **"SAP Security Assessment Framework"** which relies on a technical and functional security assessment and includes 3 main types of activities:

- **Vulnerability Assessment**, delivering a detailed report about vulnerabilities found in the SAP application landscape;
- **Code Assessment**, delivering a detailed report for the custom code developed in SAP systems
- **Penetration testing**, delivering a detailed report on exploited vulnerabilities found in the SAP systems.

These inputs together with security workshop interviews will provide information to determine the current state for security maturity, a gap assessment and a strategic roadmap with detailed initiatives to be adopted in the SAP environment driving the organization towards a Zero Trust posture.

Read more about Deloitte's SAP Security Assessment **here**.

SCAN



Contacts

Frederico Macias
fremacias@deloitte.pt
+351 210422836

André Sousa
andrsousa@deloitte.pt
+351 962753775

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's more than 345,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2022. For information, contact Deloitte Risk Advisory, S.A.