

# 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<sup>1</sup>.

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 and 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. Each story will address a layer of the Deloitte's Zero Trust Framework, as follows:

- SAP Security Assessment with Deloitte's SAP Security Framework
- Towards Risk-Based and Passwordless Authentication in SAP Applications
- Automated Certificate Management in Large SAP Environments
- 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...)

# SAP Drivers and How Zero Trust can Support?

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.

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 <sup>2</sup>. 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 <sup>3</sup>. 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%) <sup>4</sup>. 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.



<sup>1</sup> Source: The Cost of an SAP Cybersecurity Data Breach: <https://explore.bowbridge.net/blog/cost-sap-cybersecurity-data-breach>

<sup>2</sup> Source: IDC Survey – <https://onapsis.com/IDC-survey-ERP-security-assessment>

<sup>3</sup> Source: IDC Survey – <https://onapsis.com/IDC-survey-ERP-security-assessment>

<sup>4</sup> 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>

# SAP Drivers and How Zero Trust can Support?

The Main Drivers pushing organizations towards a Zero Trust approach are the following:

Driver		How Can Zero Trust Support
Growing Remote Workforce: Work from Home and the ability to work from anywhere results in the exposure of applications;	→	Empower the workforce, by enhancing the user experience whilst maintaining dynamic security posture
Accelerating Cloud Adoption: The adoption of cloud products and services created new interfaces in the SAP landscapes	→	Protect the cloud resources, by leveraging on cloud-native security controls that maintain proactive monitoring
Increasing 3 <sup>rd</sup> Party Access: The demand for efficiency in the supply chain created new ways of sharing information in real-time directly from SAP systems with third-parties and other stakeholders.	→	Secure 3 <sup>rd</sup> party collaboration, by enabling frictionless and least-privileged data collaboration
Expanding Regulatory Compliance: The expansion to other parts of the world requires attention to their local regulatory requirements.	→	Simplify compliance, by standardizing and simplifying cybersecurity controls through an agile Zero Trust architecture
Advancing Digital Transformation: Introduced more complexity in SAP architectural landscape and increases the number of services exposed to the internet	→	Enable digitalization, by segmenting environments to reduce legacy assets exposure and replace legacy technologies
Rising IT Complexity & Cost: SAP environments are becoming more and more large & complex.	→	Promote operational and cost efficiencies, by streamlining the traditional security appliances and reducing the cost

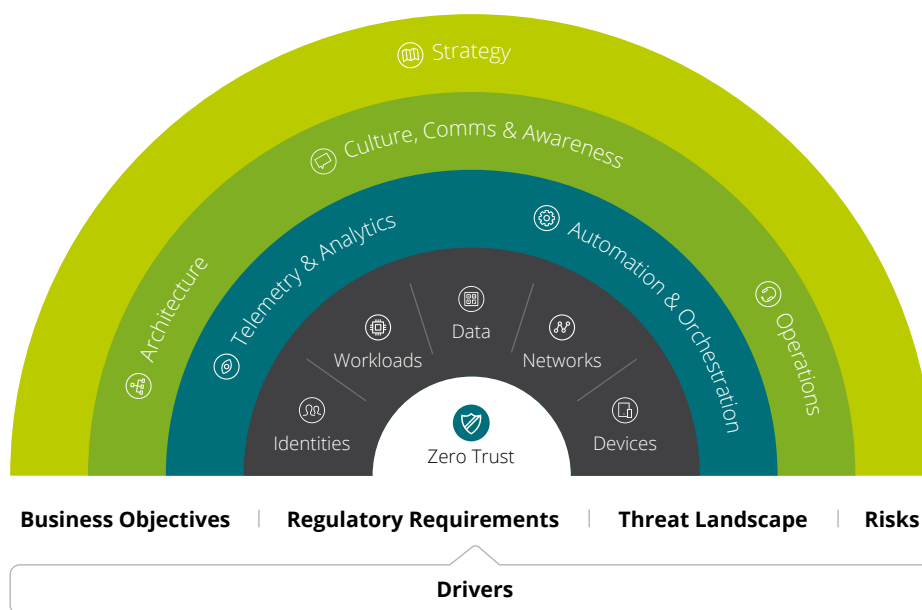


# Zero Trust in SAP environments

## 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.

Deloitte's Multidisciplinary Zero Trust Framework comprises mainly 4 layers as follows:



### STRATEGY LAYER

Zero Trust strategy should be aligned to the business drivers in a way that the journey is supporting the business, ensuring organization-wide adoption, future readiness and agility

### GOVERNANCE LAYER

Zero Trust governance ensures a cohesive top-down strategy that considers stakeholders consensus to achieve necessary cultural, architectural and operational changes

### ENABLING LAYER

Enabling layers help automate & orchestrate enforcement policies while continually analyzing enforcement decisions to identify Zero Trust violations

### CORE DOMAINS

Zero Trust model is built upon strong foundational capabilities across five foundational domains. The maturity across these domains will ultimately determine Zero Trust maturity

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 environments

## Benefits for SAP

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

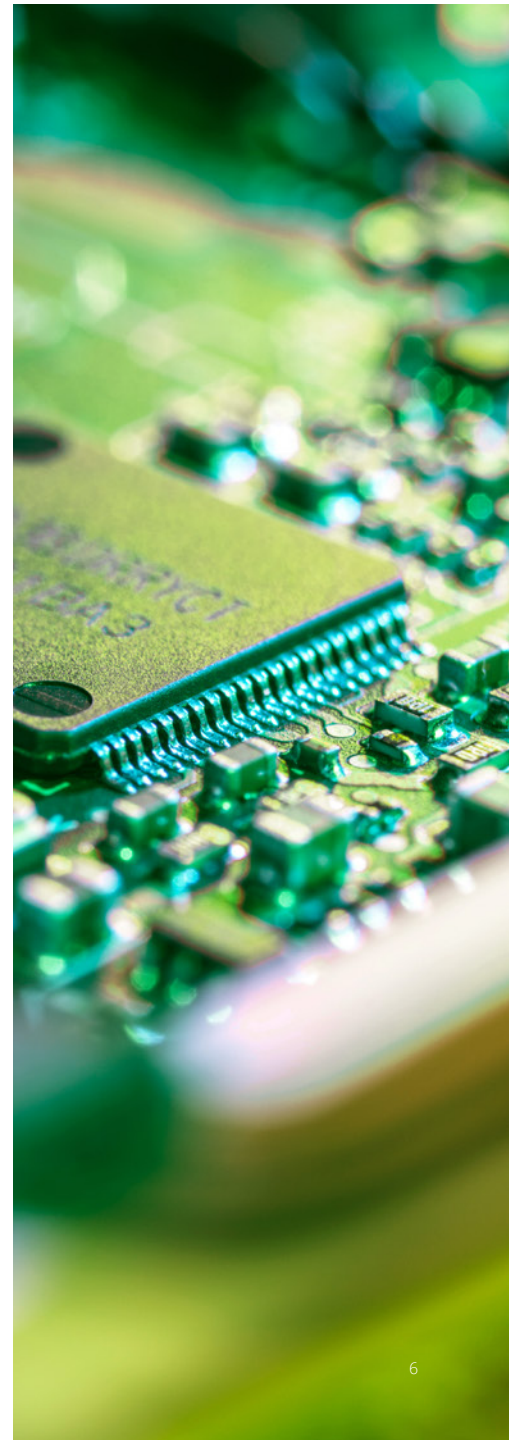
User permissions can be easily added and removed by the security teams in a Web UI. No additional software is required enabling working from anywhere, in or out of the company resulting in scalability and agility.

### 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.

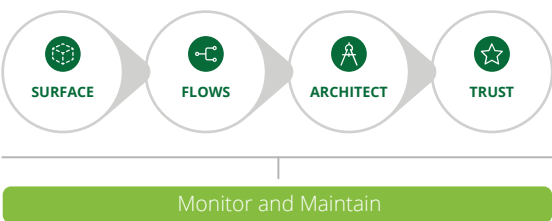
### Seamless

Implementing a Zero Trust architecture in SAP server does not require any changes or modifications to the client server model. Therefore, the implementation seamlessly and users can continue working normally.







# 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:



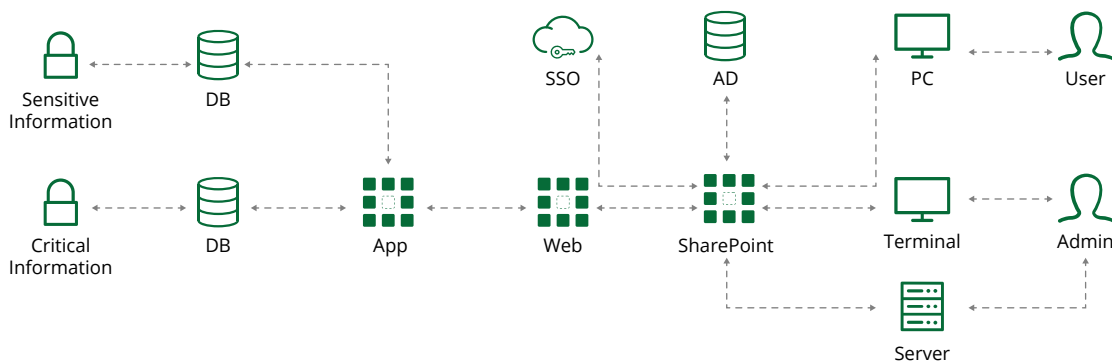
## Surface

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.

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

## Flows

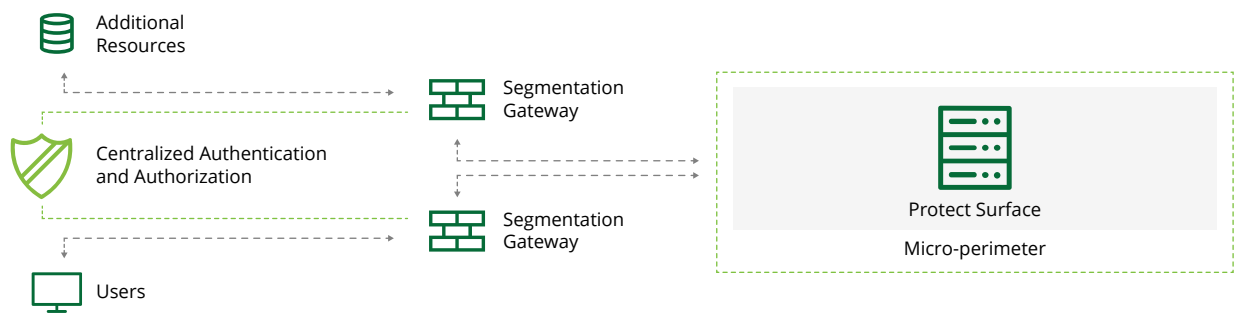
Map all existing flows and interactions in the surface and identify/categorize the type of traffic that is being transmitted. Use automated tools to assist in the mapping of interactions between data, applications, systems, and networks.



# Approach to adopt a Zero Trust posture in SAP

## Architect

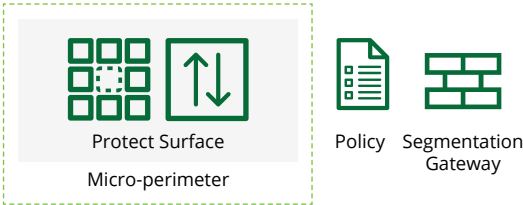
Create segmentation gateways to define the perimeter of the identified surface using virtual, physical, or cloud-based next-gen firewalls (NGFWs) as segmentation gateways. Implement scalable security solutions to reduce bottlenecks, including an advanced and centralized authentication and authorization.



## 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<sup>5</sup>.

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.



---

<sup>5</sup> 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**<sup>6</sup>.

---

<sup>6</sup> <https://deloitte.tt/3E7xes1>



# Authors

## Andre Correia Sousa

Portugal SAP Security Expert  
andrsousa@deloitte.pt  
+351 962753775

## Matthias Sill

Germany SAP Security Expert  
msill@deloitte.de  
+49 15158000306

# Contacts

## Andre Correia Sousa

Portugal SAP Security Expert  
andrsousa@deloitte.pt  
+351 962753775

## Antony Jose Vallookaran

Poland SAP Security Expert  
anvallookaran@deloittece.com  
+48 123944429

## Fabio Bonanni

Italy SAP Security Expert  
fbonanni@deloitte.it  
+39 0283326347

## Gabriele Piersanti

Spain SAP Security Expert  
gpiersanti@deloitte.es  
+34 638315587

## Hans Peersman

Netherlands SAP Security Expert  
hpeersman@deloitte.nl  
+31 882887368

## Marc Noergaard

Denmark SAP Security Expert  
mnoergaard@deloitte.dk  
+45 22300140

## Marisa Geldenhuys

UK SAP Security Expert  
mgeldenhuys@deloitte.co.uk  
+44 7552 549146

## Matthias Sill

Germany SAP Security Expert  
msill@deloitte.de  
+49 15158000306

## Rajwinder Singh

USI SAP Security Expert  
rajwindsingh@deloitte.com  
+1 (470) 3624637

## Vaibhav Jani

Canada SAP Security Expert  
vajjani@deloitte.ca  
+1 4167757269

## Vikas Bhan

Belgium SAP Security Expert  
vbhan@deloitte.be  
+ 32 24558752

# Deloitte.

"Deloitte," "us," "we" and "our" refer to one or more of Deloitte Touche Tohmatsu Limited ("DTTL") 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 and, therefore, do not bind each other for all intents and purposes. Accordingly, each entity is only liable for its own acts and omissions and cannot be held liable for the acts and omissions of the other. Furthermore, DTTL does not provide services to clients. To learn more, please consult [www.deloitte.com/about](http://www.deloitte.com/about)

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® among thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. To learn how Deloitte's 415,000 people worldwide make an impact that matters please consult [www.deloitte.com](http://www.deloitte.com).

This communication contains general information only, and neither Deloitte Touche Tohmatsu Limited ("DTTL") nor 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. Accordingly, before deciding or taking any action that may affect your finances or your business, on the basis of this communication 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 therefore neither the issuer, nor DTTL or its network of member firms, related entities, employees or agents may be held liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.

