TURNKEY

A Zero-Trust Approach to Securing SAP Systems

On-Premise, Hybrid and Cloud

www.turnkeyconsulting.com

Tom Venables

→ STATS

TURNKEY

With new legislation appearing worldwide which is placing a greater emphasis on cybersecurity and data privacy.

- NIS-2
- US National Cybersecurity Strategy
- NIST CSF-2 guidance

All these place a greater emphasis on security, and Zero-Trust is a key principle being referenced. This as a response to some high-profile breaches which have occurred in recent years, such as SolarWinds and the Colonial Pipeline hack.


RESEARCH

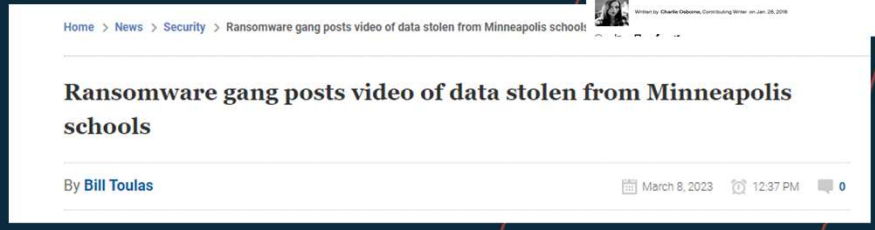
More vulnerabilities in industrial systems raise fresh concerns about critical infrastructure hacks

Researchers have revealed details about flaws in industrial systems th access to the most sensitive networks.

BY CHRISTIAN VASQUEZ • FEBRUARY 22, 2023


NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs

The shipping giant has suffered millions of dollars in damage due to the ransomware attack.


Home > News > Security > Ransomware gang posts video of data stolen from Minneapolis schools

Ransomware gang posts video of data stolen from Minneapolis schools

By Bill Toulas

March 8, 2023 12:37 PM 0

www.turnkeyconsulting.com

TURNKEY

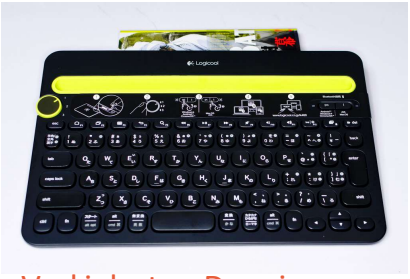
Zero-Trust Introduction

What does Zero-Trust Mean?

Verify Users

Knowing WHO is accessing your systems and data is an essential first step in achieving Zero-Trust approach to securing them.

Are your users knowledgeable and equipped to secure your data?



Validate Devices

Making sure connections are secure between users, applications and databases as digital transformation changes ways of working.

Can you identify a breach?

Intelligently Limit Access

Applying access control within your systems, not only with traditional roles, but consider policy-based controls, or ABAC

Do you know what data is being accessed?

TURNKEY

How does this apply to SAP?

Whether you're on-premise, hybrid or cloud, zero-trust principles can be applied…

Verify Users

SAP is often not fully integrated with enterprise-level Identity and Access Management initiatives, but this is an essential gap to close.

Consistency of identity across the SAP estate is key and control of privileged accounts are essential. Integrating with SSO and MFA allow better protection of systems and data.

Limit Access

Roles and Authorizations have always been at the core of securing SAP, but it is important to consider how we handle edge-cases, such as privileged account management, masking of data and how to detect when access is misused.

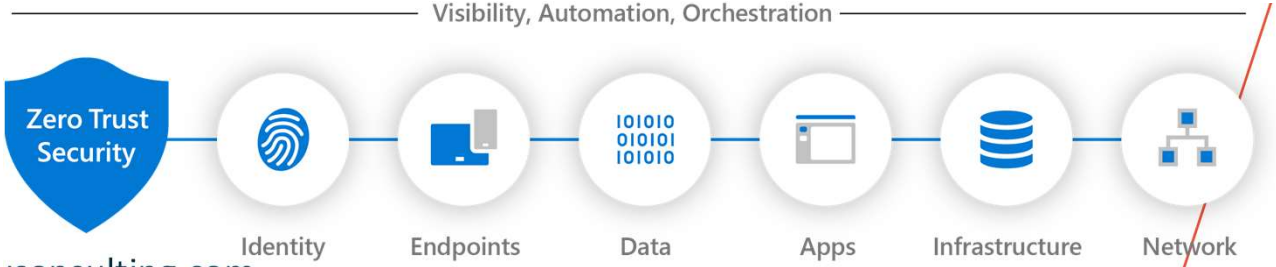
You likely already have tools in place to manage this, but are you aligned with your CISO and the enterprise approach?

Secure Apps & Data

Applying Change controls over code and developments through Solution manager implementing DevSecOps principles across the estate.

ETD – Inbound connections are verified and re-checked, with alerting that can be integrated with enterprise SOC.

Controlling access via endpoints can be achieved through tools like UI masking.



→ STATS

TURNKEY

A Problem Shared is a Problem Halved

SAP Application owners must work with CISOs to tackle the problem

90%

Of the Revenue

SAP systems route a huge volume of the revenue-related data for their customers, meaning SAP application owners take risk in this area very seriously

10%

Of the IT estate

A CIO, or CISO, who has an entire IT (and often OT) estate to secure against threats, may see the risk profile of the SAP applications through a different lens

50%

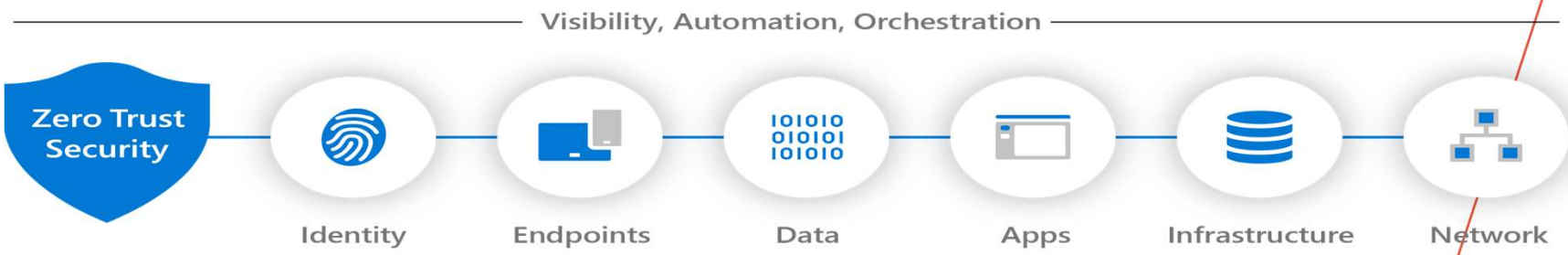
Shared Responsibility

Securing SAP systems is not performed in a vacuum, shared ownership of the risks and the controls allows a more co-ordinated approach and better security outcomes overall.

TURNKEY

Solution Alignment

A Look at how SAP's portfolio helps achieve Zero-Trust



Identity	Endpoints	Data	Apps	Infrastructure
SAP & Enterprise IDAM MFA SSO	Fiori & Mobile Devices (changing the threat vector)	Access Governance UI Masking RAL Data Custodian	DevSecOps (incl. secure coding) ETD BIS CVA	SOC / SIEM / SOAR integrations (via ETD) Patch & Vulnerability Management (both at the application and infrastructure layers)

→ Drilling in

TURNKEY

Identity is the New Perimeter

Changes to working patterns erode the perimeter defence (especially where Cloud solutions are in place)

Are users all created equally?

Do you trust all your users?

Are you allocating and revoking access in a timely fashion?

Do you use MFA and SSO?

Are Third-Parties controlled?

What about database users?

IDM makes sure the right people get access and that access is revoked, based on JML.

PAM (EAM in GRC) permits control over privileged & 3rd party users

Should SAP users receive additional training/phishing testing to ensure your perimeter is secured?

MFA solutions increase the security of identities, while SSO improves user experience and reduces support costs.

Multiple sources of identity

Joiner / Mover / Leaver Automation

Privileged Accounts

User Training

MFA

SSO

PSS

www.turnkeyconsulting.com

→ Who's got what?

TURNKEY

Managing Access

Once your users are in, what can they do?

SAP Access Control

Access Control allows you to apply the principles of PAM to the application, as well as assessing the risks associated to access within the SAP estate.

As organisations migrate to the cloud, analysing risks across systems should be considered.

Automated, preventative controls as part of UADM processes reduce risk further.

SAP Roles & Auths

Strong role design and implementation has always been at the core of enabling users to do their job, while meeting the objective of least-privilege

Migrating to new systems provides the perfect opportunity to re-architect your roles and ensure they're built with this principle in mind.

SAP Cloud IAG

SAP Cloud Identity and Access Governance provides visibility of access allocated across your hybrid and cloud estate.

Incorporating both the principles of IDAM and Access Control, zero trust approaches can be enhanced as you undertake your digital transformation journey

www.turnkeyconsulting.com

→ Overlaying the Access Governance

TURNKEY

Controlling the Data

Visibility of what is happening in your SAP estate

SAP UI Masking

UI Masking provides the capability to show/hide data based on policies and attributes within the SAP applications.

This permits you to hide data from users or connections that you don't trust fully.

Intelligently limiting access to data in this way significantly reduces the risk of a breach.

SAP R.A.L.

Read Access Logging permits you to see who is accessing your data and can alert you to misuse.

Overlaid on strong access controls, this permits not only visibility of who CAN, but who HAS accessed your most sensitive assets.

SAP Data Custodian

As your data moves to cloud estates, having visibility and control, with near real-time insights into placement, movement and access controls can be provided by Data Custodian.

Anomaly detection allows you to react to suspicious behaviour with your data and you can apply intelligent access controls over your data.

TURNKEY

Securing the Applications

Visibility & Control of the application

SAP BIS

Business Integrity Screening allows visibility of the controls being operated within the applications, as well as business partner screening and integrations with your audit and controls operations.

SAP ETD

Enterprise Threat Detection allows you to not only identify vulnerabilities in your SAP estate, but also if those vulnerabilities are actively being exploited.

It also allows you to integrate with enterprise-level SOAR/SIEM and SOC operations to better manage risk.

SAP CVA / SOS

Code Vulnerability Analyzer can showcase where custom code may introduce new risks into your estate, particularly important in manging 3rd parties.

Security Optimisation Services permit you to identify vulnerabilities which may be exploited.

→ Embracing the Cloud

TURNKEY

Cloud Migration Changes

As we transform the ERP estate, Zero-Trust becomes more important

New UX

Adopting new user experiences and applications changes the threat vector for organisations.

Adopting Fiori, moving apps to mobile devices and increased web connectivity of the application estate brings new security requirements.

Identity is the new perimeter!

Hosted Estates

Moving your infrastructure to hosted solutions does allow you to outsource some of the security challenges, like patch & vulnerability management, but you are still responsible for the access to your data

Your processes and contracts need to be robust to ensure you stay protected!

Integrations

While outsourcing some of the technical challenges is an attractive proposition, having good governance over the third parties supporting you has never been more important.

Can you integrate your hosting partners security solutions with your own controls estate?

TURNKEY

Zero-Trust Maturity

A journey of a thousand miles starts with a single step…

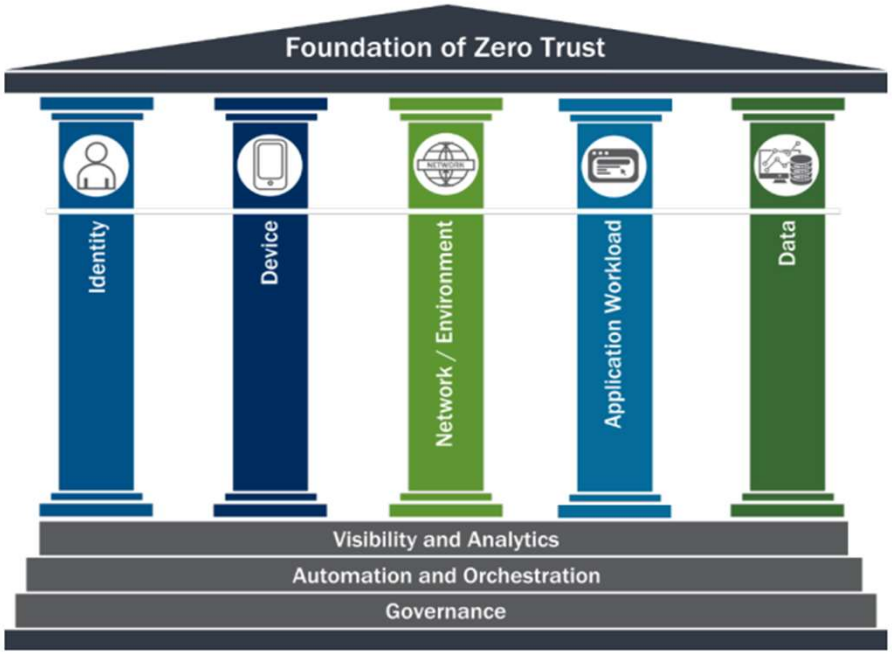


Figure 1: Foundation of Zero Trust[7]

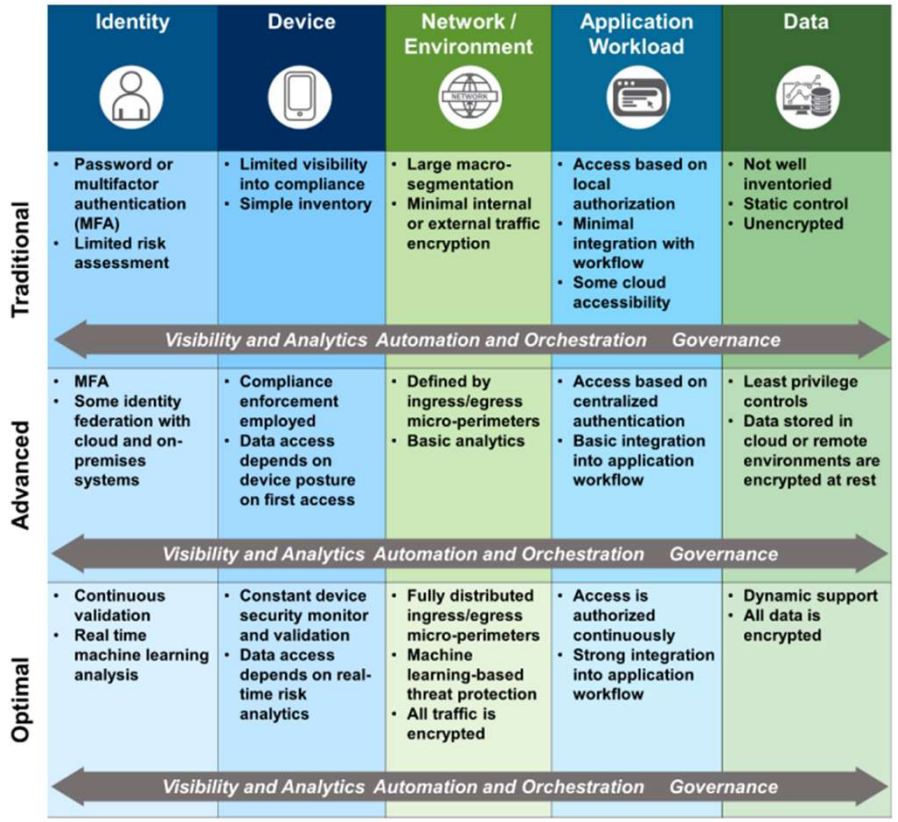


Figure 2: High-Level Zero Trust Maturity Model

→ In Conclusion

TURNKEY

When a conversation about Zero-Trust and how it applies to SAP happens, this should enable you to speak about the solutions you can point to as supporting that objective.

Tom Venables

Solutions Architect & Strategist

www.turnkeyconsulting.com