



SAP Cybersecurity

Why is it important? Why now?

Customer Perspective:

sanofi

Prepared for ASUG – Oct. 2023

Karl Batchelor



www.securitybridge.com

Sun Tzu 'The Art of War' principles for Cybersecurity

**“Visibility and Risk
are Inversely
Proportional”**



“Know thy self, know thy enemy.”

- This principle addresses the importance of preparation, which begins with **VISIBILITY** – identifying business-critical assets and understanding and prioritizing risk

“Subdue the enemy without fighting.”

- Sun Tzu states the best tacticians are those who can control situations through intelligence and leverage information to dictate the choices of their adversaries

AGENDA: SAP Vulnerability Management

- SAP applications are used by businesses of all sizes to manage critical business processes, including financials, supply chain, and human resources
- As a result, SAP applications are a prime target for cyber attacks



Overview of Application Security

Why it's important & what roles are involved

Why is it so difficult?

Challenges faced by Siloed organizations

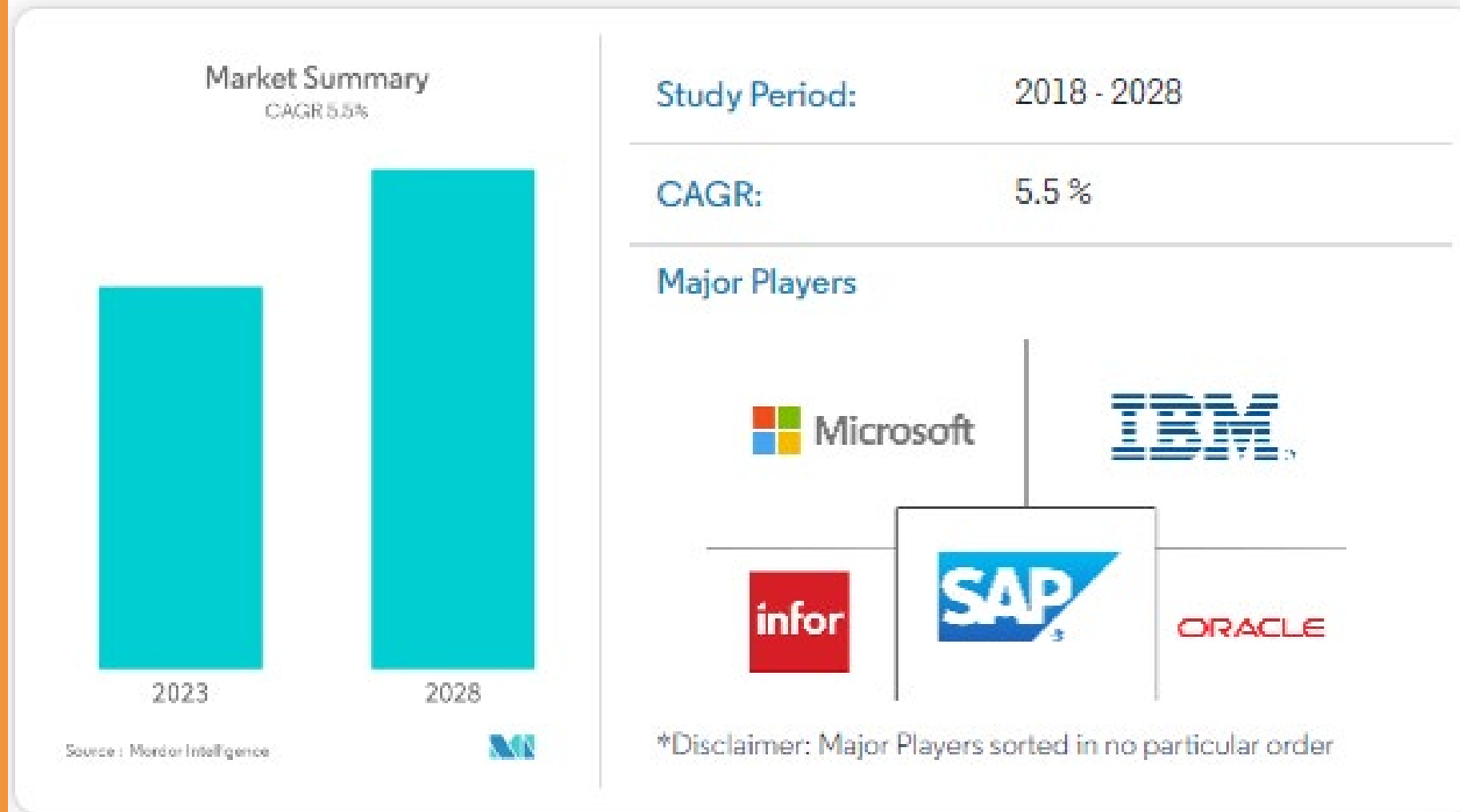
What Methods may be employed to help?

Tools, Processes & Automation

MARKET TRENDS

Increased demand for security

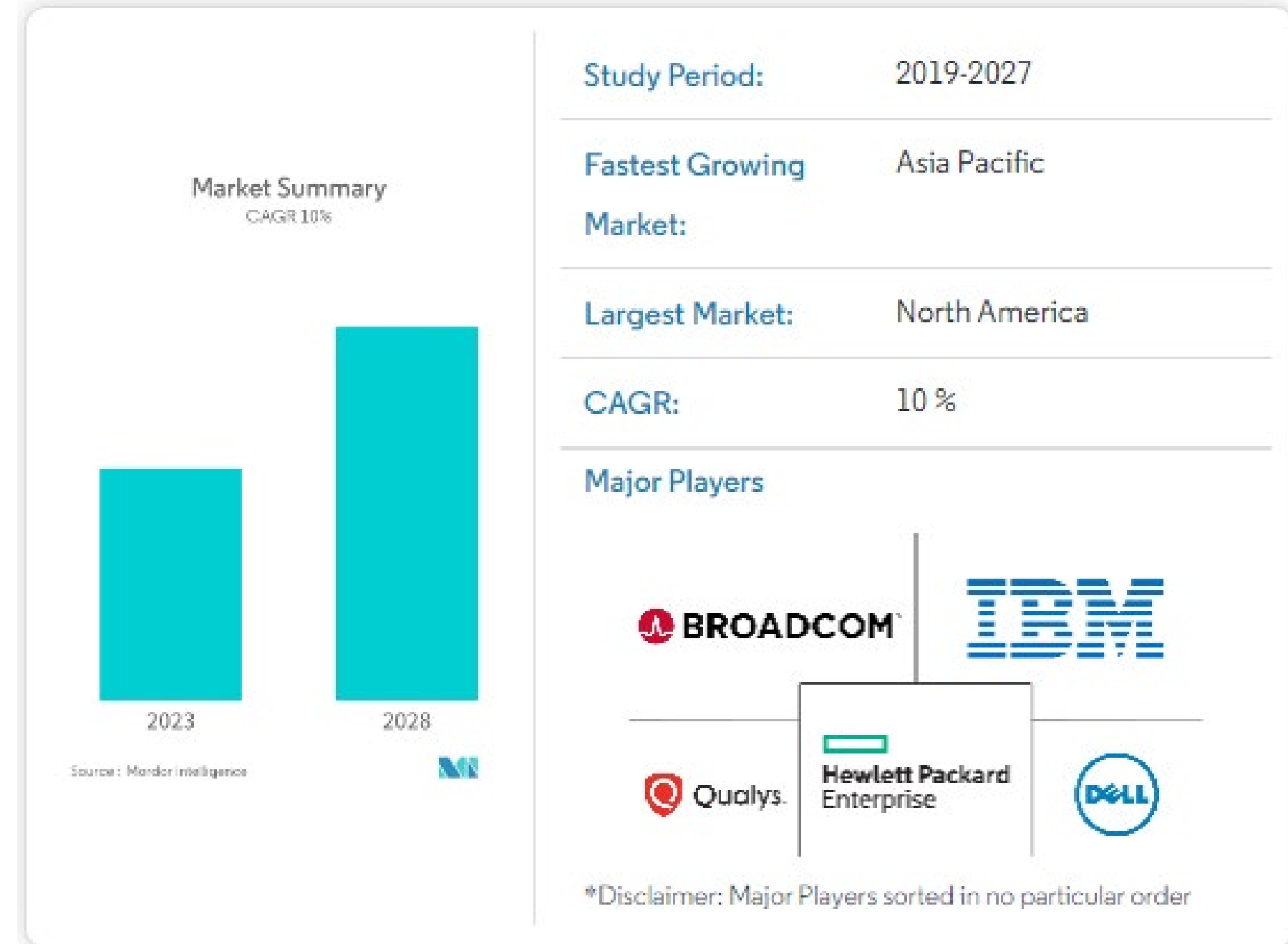
North America Enterprise Resource Planning Industry Overview



<https://www.mordorintelligence.com/industry-reports/north-america-enterprise-resource-planning-market>

**Need for Vuln Mgmt. Solutions almost
DOUBLES ERP market growth!**

Security & Vulnerability Management Industry Overview



<https://www.mordorintelligence.com/industry-reports/security-and-vulnerability-management-market>

SAP – Application Security

Why Care?

- Attacks on the APPLICATION LAYER increasing in frequency
- Example, CISA Announcement on April 6, 2021...
- On April 6, 2021, the Cybersecurity & Infrastructure Security Agency (CISA) released a warning that cybercriminals are actively targeting known vulnerabilities in SAP applications that could allow them to take over the app, infect network systems and take complete control.

As SAP reported in its warning posted earlier today:

“These are the applications that 92 percent of the Forbes Global 2000 have standardized on SAP to power their operations and fuel the global economy,” the alert noted. “With more than 400,000 organizations using SAP, 77 percent of the world’s transactional revenue touches an SAP system. These organizations include the vast majority of pharmaceutical, critical infrastructure and utility companies, food distributors, defense and many more.”

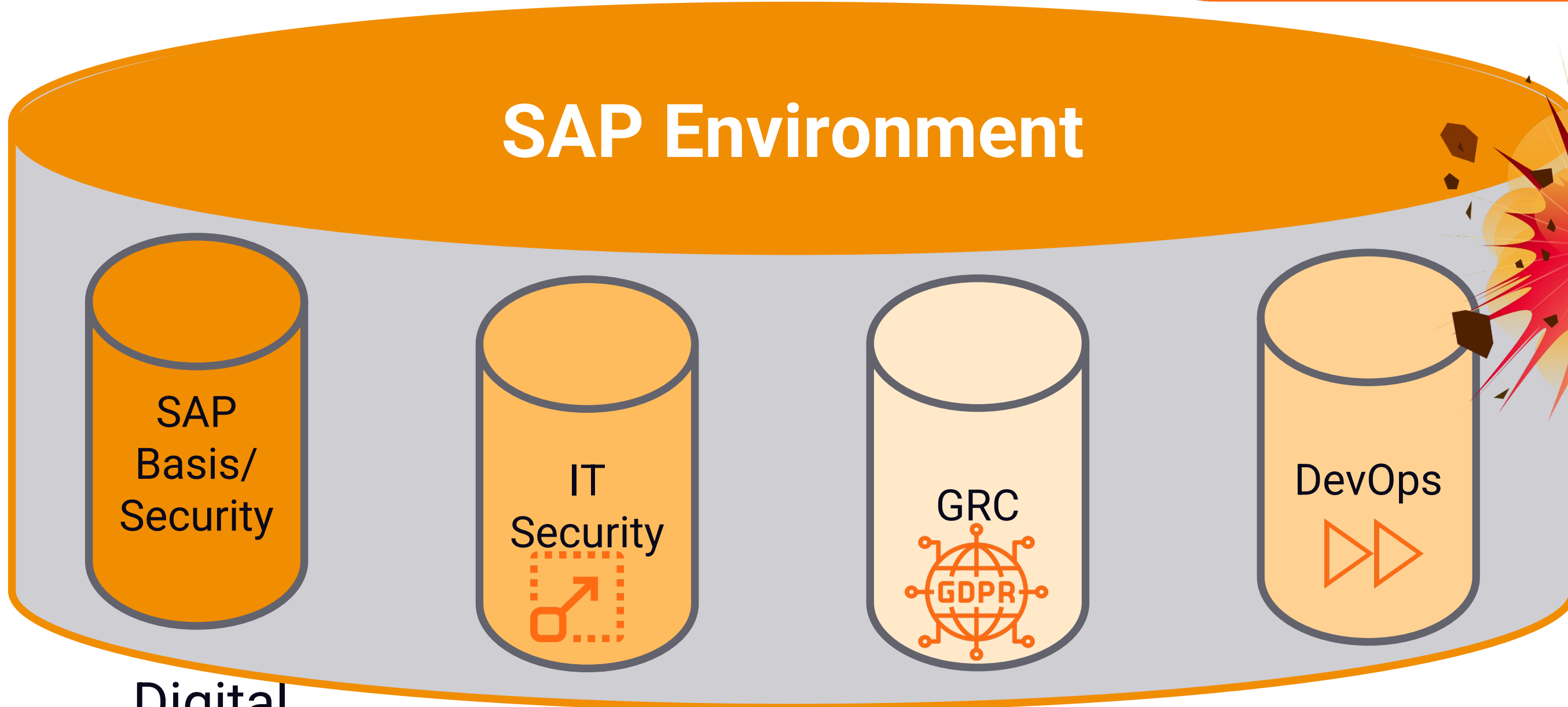
Based on the verticals listed, these are products and services that impacts us

Directly in our Daily Lives

Modern Enterprises Are Facing New Challenges...



EVAPORATING THE PERIMETER TO ENABLE REMOTE WORKERS, PARTNERS, SUPPLY CHAIN, ETC.



Threat Actors

EVOLVED TO TARGET MULTIPLE, NEW ATTACK VECTORS

Digital Transformation
FREQUENTLY FAVORING EXPEDIENCY
NOT SECURITY

Compliance
DRIVING STRICTER AND
MORE COMPLEX CONTROLS

Constant Change
DISRUPTING BUSINESS OPERATIONS

Some common SAP vulnerabilities attackers try to exploit



**CVE- Multiple
aka "10Kblaze"**

Remote Code Execution Vulnerability

**CVE-2020-6287
aka "RECON"**

Critical vulnerability in SAP NetWeaver
Appl. Server Java Remote
unauthenticated attacker takes
complete control of affected SAP



**CVE-2022-22536
aka "ICMAD"**

Critical request smuggling and
request concatenation vulnerability
in SAP NetWeaver Application
Server



LOG4J



Log4j

Non-SAP vulnerability, impacting
SAP

SAP – Patching... What are the facts for Enterprises?

20%

of all vulnerabilities caused by unpatched software are classified as High Risk or Critical²

67 days

Average time to close a discovered vulnerability (caused by unpatched software and apps)³

80%

Who had data breach, or failed audit could have prevented it by **patching on time** or doing **configuration updates**¹

37%

Admitted that they **don't even scan for vulnerabilities**³

46%

Upon a breach or failed audit, **took longer than 10 days** to remedy the situation and apply patches **WHY?**
Difficult!¹

SAP – Patching... Why is it so Difficult?

12 days

Average time for teams to coordinate tasks for applying a patch across all devices

61%

Feel that they are disadvantages for relying on **manual processes** for applying software patches

TIME

65%

Too difficult for them to **decide correctly on the priority level** of each software patch
(**RBVM** -Risk Based Vulnerability Mgmt)

55%

Patching requires manually **navigating the various processes** is more involved than patching vulnerabilities

Better Processes, Tools & Automation Needed

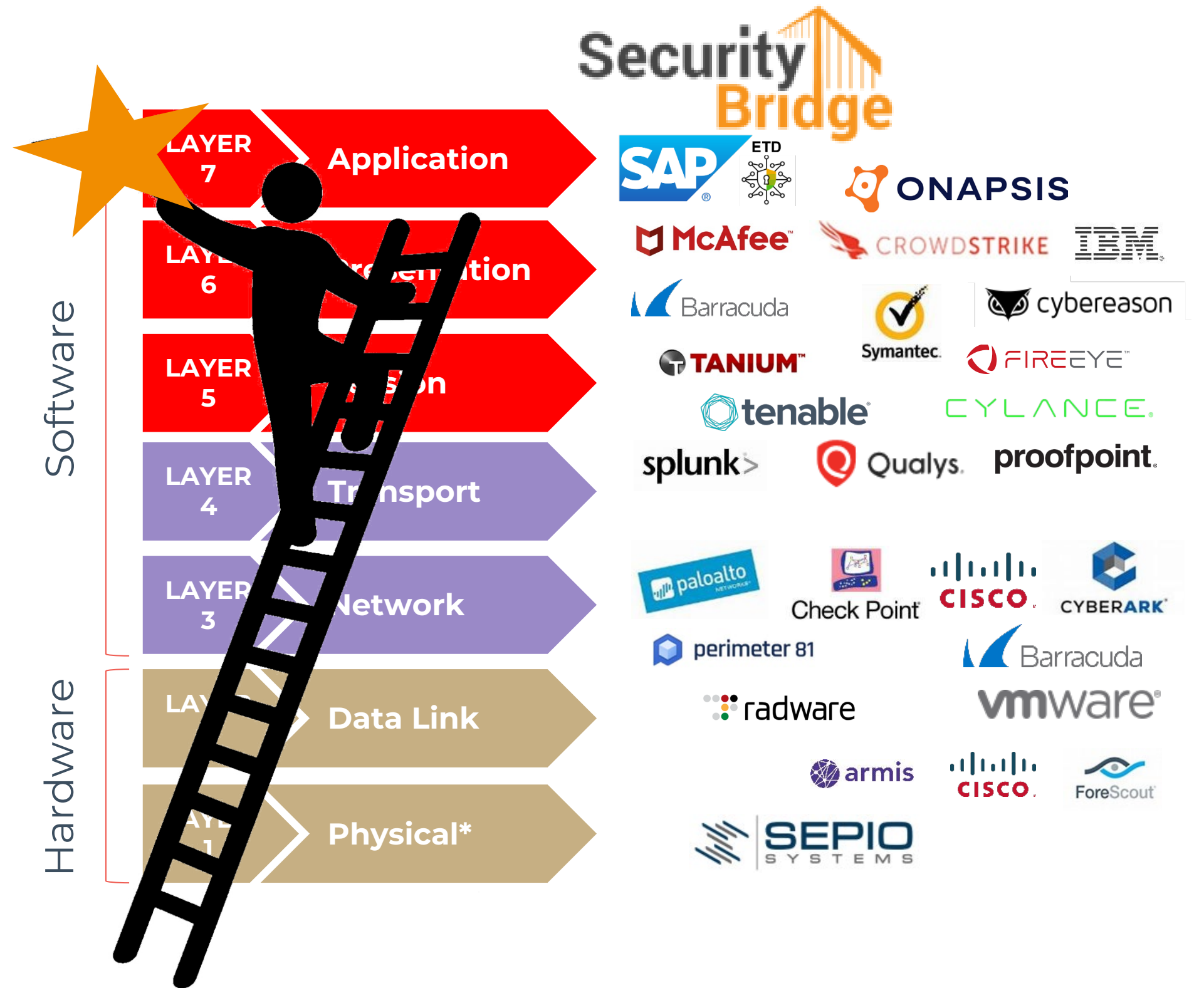
Security In Depth – Protect the Application Layer

The Seven Layer OSI model

Application Layer →
Largest Surface Area for Attacks to Occur

All the solutions listed are in place to
protect the
APPLICATION LAYER

↓
**Corporate
DATA**



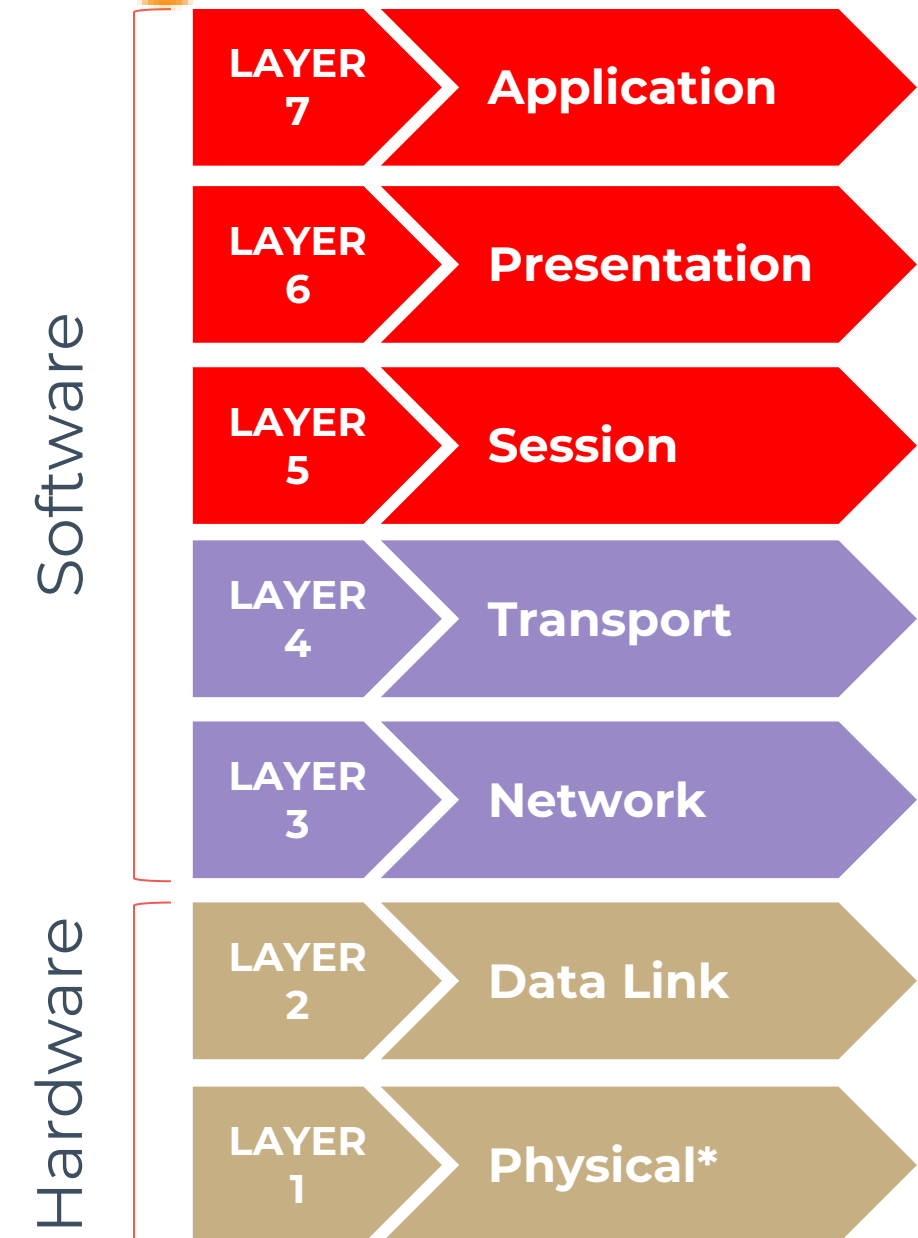
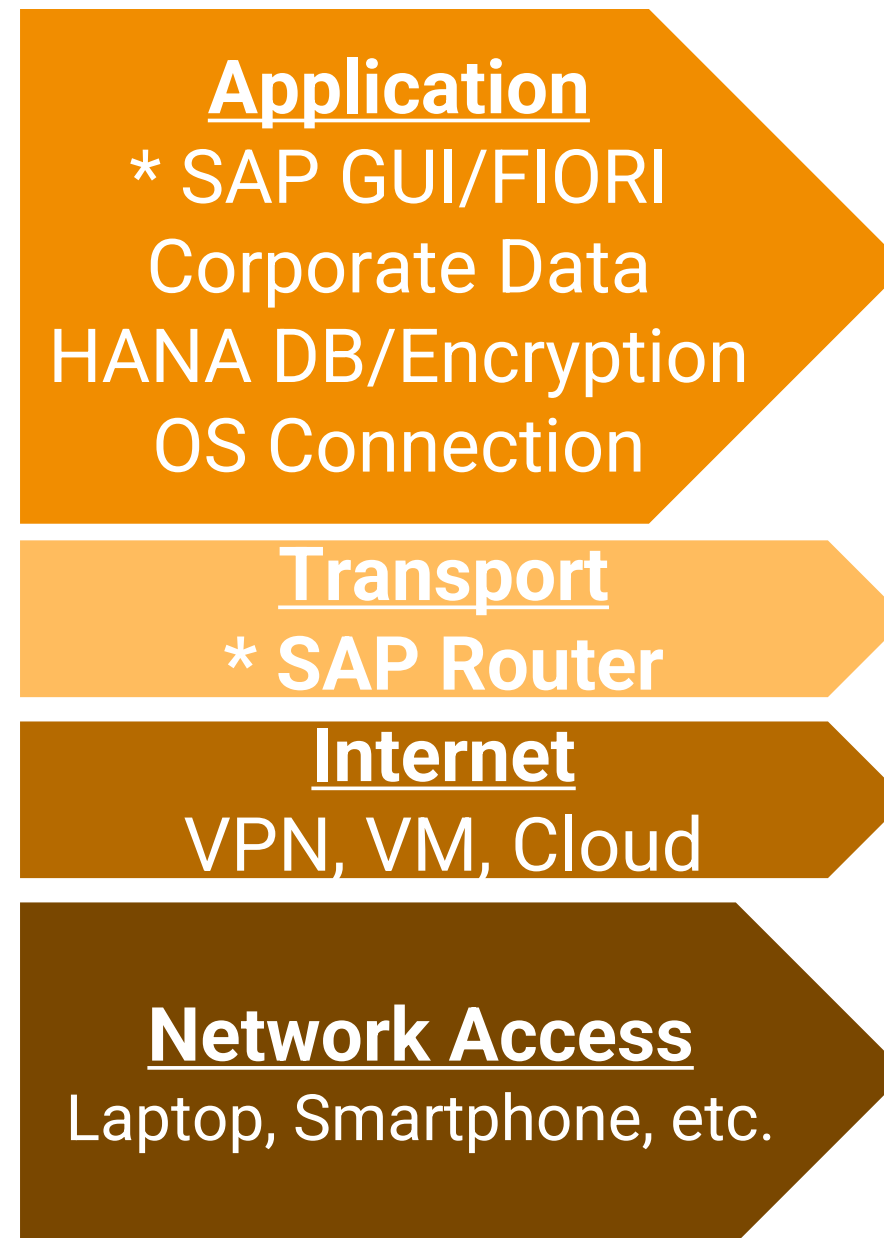
The Seven Layer OSI model

... as it Relates to SAP



Application Layer →

Everyone has access
Internal Threats are REAL
“Trust But Verify”



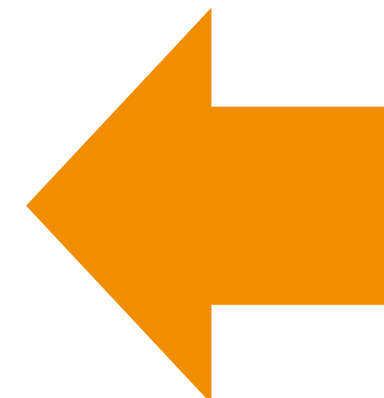
How are security systems defeated today?



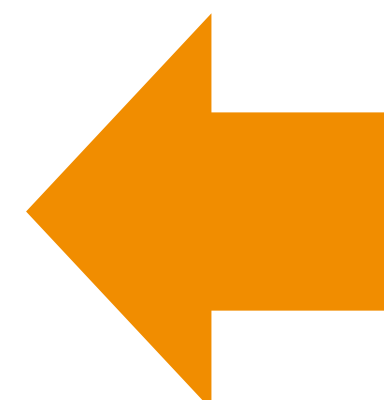
Rubber Ducky



USB Ninja Cable



Off-the-shelf pen-testing tools used for demonstrating vulnerabilities; running below radar of all EDR/EDP, NACs...



Tier 1 Bank Leaking Data; Attackers used Transparent Network Devices. Running out-of-band, undetected for months.

Social Engineering – the psychological manipulation of people into performing actions or divulging confidential info.

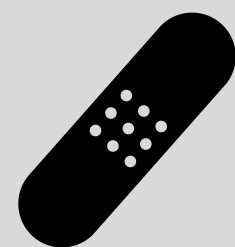


ATTACK VECTORS

- Misconfigurations
- Default Passwords/IDs
- Escalation of Privileges

**CONFIGURATION
VULNERABILITY**

- SAP Issues Patches & Notes to address
- Patch prioritization issues
- Time consuming
- Disruptive



**KNOWN PRODUCT
ERROR**

- Custom Dev Necessary
- Migration to cloud
- Third Party dev

**1010
1010**

**CUSTOMER CODE
VULNERABILITY**

- No Pre-Patch protection
- Escalation of Privileges late detection
- Lack of useful logs



**ZERO
DAY**



ATTACK VECTORS

**VULNERABILITY
MANAGEMENT**

**CONFIGURATION
VULNERABILITY**

**PATCH
MANAGEMENT**

**KNOWN PRODUCT
ERROR**

**CODE
SCANNER**

**1010
1010**

**CUSTOMER CODE
VULNERABILITY**

**THREAT
DETECTION**

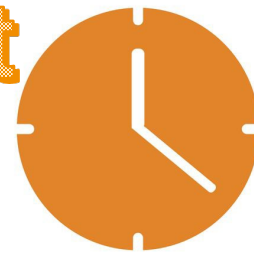


**ZERO
DAY**

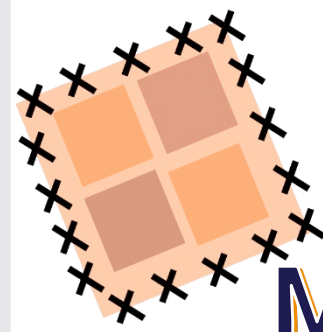
4 Security Functions to Effectively Protect Against Zero-day Exploitation



Real-time Threat Detection



Detect and analyze security-related events and anomalies within an SAP system



Patch Management

SAP systems remains secure and up-to-date by managing installation of software patches and updates in a timely and efficient manner



Secure Configuration & Assessments



Confirm SAP systems are configured securely and remain secure over time. Establishing baseline of secure configuration settings, regularly assessing

Code Vulnerability Scan



Identify and report potential security vulnerabilities within software code



 www.securitybridge.com

Get complete visibility into **your SAP Security, custom code risks, and vulnerabilities** with the SecurityBridge Platform



 [linkedin.com/company/securitybridge](https://www.linkedin.com/company/securitybridge)

 SecurityBridge

 @_SecurityBridge

A CUSTOMER'S PERSPECTIVE: SANOFI - A global healthcare company



Stephane Peteytas

SAP Cybersecurity Management at



Extracted from:



HOW TO ACCELERATE SAP SECURITY?

Join and listen to Sanofi's SAP Security Leader speaking about their journey in securing a large SAP landscape across an enterprise in the cloud and on-premise.



SecurityBridge

built in SAP, for SAP RISE

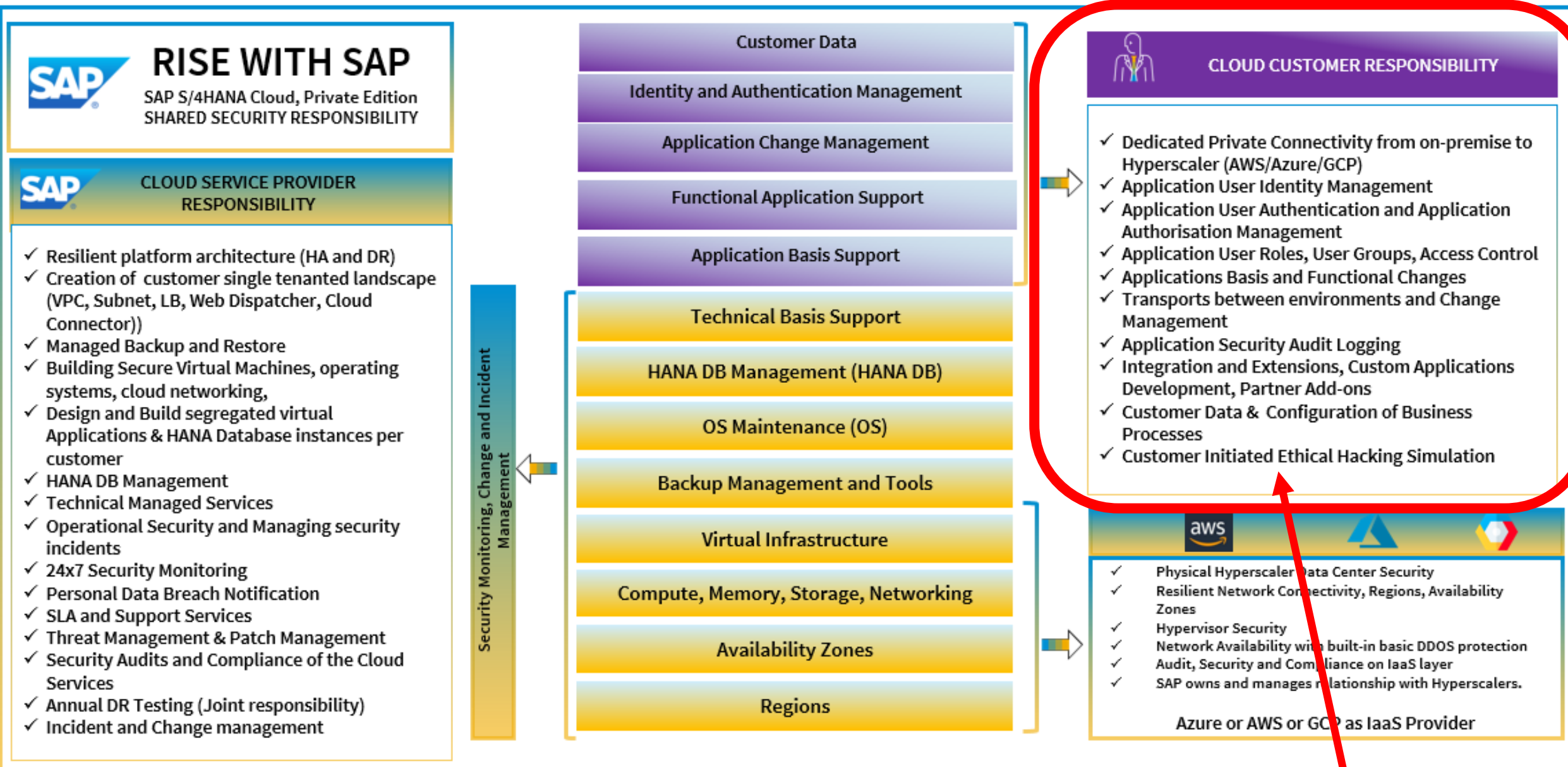


Integrate SecurityBridge in RISE ✓

- Monitor User Roles, Access Controls
- Monitor Transports & Change Mgmt
- Security Audit Logging
- **Establish a 360° view on SAP cybersecurity**
 - Threat detection
 - Vulnerability management
 - Compliance management
- ONE platform and all installed in just a few hours!

SAP Security
“Trust but Verify”

Customer Responsibility

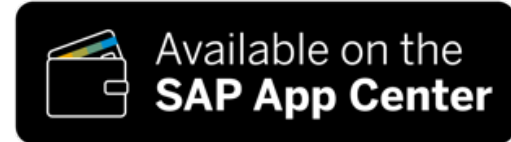


RISE WITH SAP
SAP S/4HANA Cloud, Private Edition
SHARED SECURITY RESPONSIBILITY

CLOUD SERVICE PROVIDER RESPONSIBILITY

- ✓ Resilient platform architecture (HA and DR)
- ✓ Creation of customer single tenanted landscape (VPC, Subnet, LB, Web Dispatcher, Cloud Connector)
- ✓ Managed Backup and Restore
- ✓ Building Secure Virtual Machines, operating systems, cloud networking,
- ✓ Design and Build segregated virtual Applications & HANA Database instances per customer
- ✓ HANA DB Management
- ✓ Technical Managed Services
- ✓ Operational Security and Managing security incidents
- ✓ 24x7 Security Monitoring
- ✓ Personal Data Breach Notification
- ✓ SLA and Support Services
- ✓ Threat Management & Patch Management
- ✓ Security Audits and Compliance of the Cloud Services
- ✓ Annual DR Testing (Joint responsibility)
- ✓ Incident and Change management

Security Monitoring, Change and Incident Management

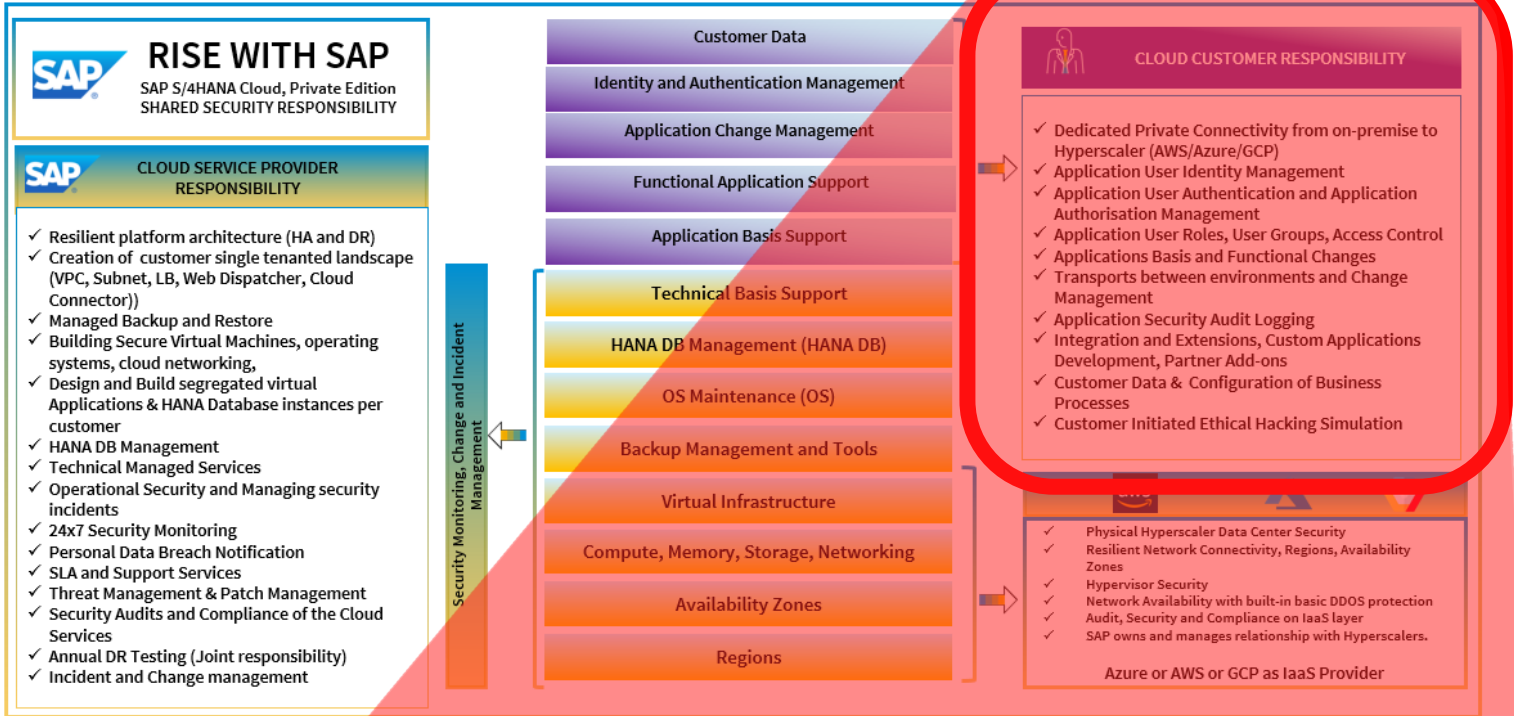


Compatible with SAP S/4HANA Cloud, private edition
Works with RISE with SAP

SecurityBridge

SAP RISE Functional Mapping...

Security for SAP Anywhere
"Trust but Verify"



Integrate SecurityBridge in RISE ✓

- Monitor User Roles, Access Controls
- Monitor Transports & Change Mgmt
- Security Audit Logging
- Code Vulnerability Analysis
- **Additionally... Establish a 360° view on SAP cybersecurity**
 - Threat detection
 - Vulnerability management
 - Compliance management
- ONE platform, all installed in just a few hours!



Final Thoughts...





“Invincibility lies in the defense; the possibility of victory in the attack.” – Sun Tzu

**SecurityBridge Increases Visibility into Business-Critical Apps
Bridging the Gap between Siloed Departments, Providing a 360°
Security view of your SAP Landscape**

GET IN TOUCH WITH US

 www.securitybridge.com

 Muenchener Str. 49, Ingolstadt, 85051, Germany
228 Park Ave S, PMB 89765, New York, New York
10003-1502 US

 DE: +49 (841) 93914840
USA: +1 (416) 821 0850

 [linkedin.com/company/securitybridge](https://www.linkedin.com/company/securitybridge)

 SecurityBridge

 @_SecurityBridge

