Managed Security Service

Current Threats in Cloud environments

Uemit Oezdurmus,
2020

SAP® Cloud Application Services
We help The Best Run better

THE BEST RUN SAP

Disclaimer

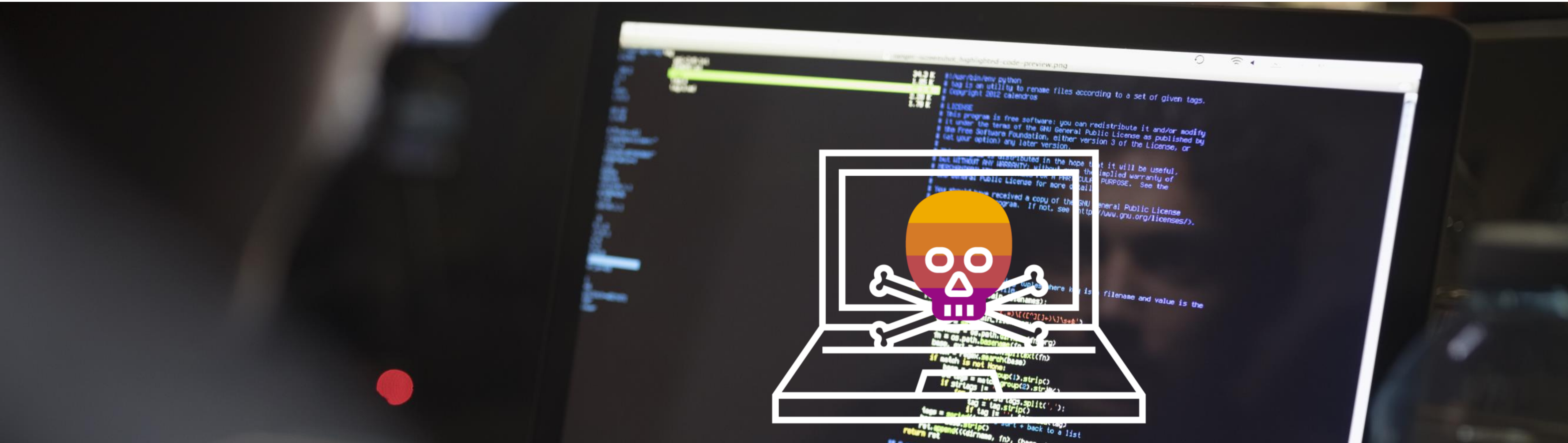
The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP’s intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

Motivation

Why do our customers need Security Services?



Common Security Breaches

Equifax Hack – 2017

An example that SAP Notes should used immediately.
The security gap what is used here, was known months ago before the hack took place:

- **Massive data breach**,
- Equifax has confirmed that attackers entered its system in mid-May through a **web-application vulnerability** that had a **patch available in March**.
- **Exposed personal data (social security numbers and adresses) of 143 million** due to not applying any patches

Source:
https://www.wired.com/story/equifax-breach-no-excuse/

10KBLAZE / Potential SAP hacks 2019

“50,000 companies exposed to hacks of 'business critical' SAP systems: researchers” (Reuters)

- New ways to exploit vulnerabilities of systems that haven’t been properly protected
- If a **company’s security settings are not configured correctly**, he said, a hacker can trick an application into thinking they are another SAP product and **gain full access** without the need for any **login credentials**.

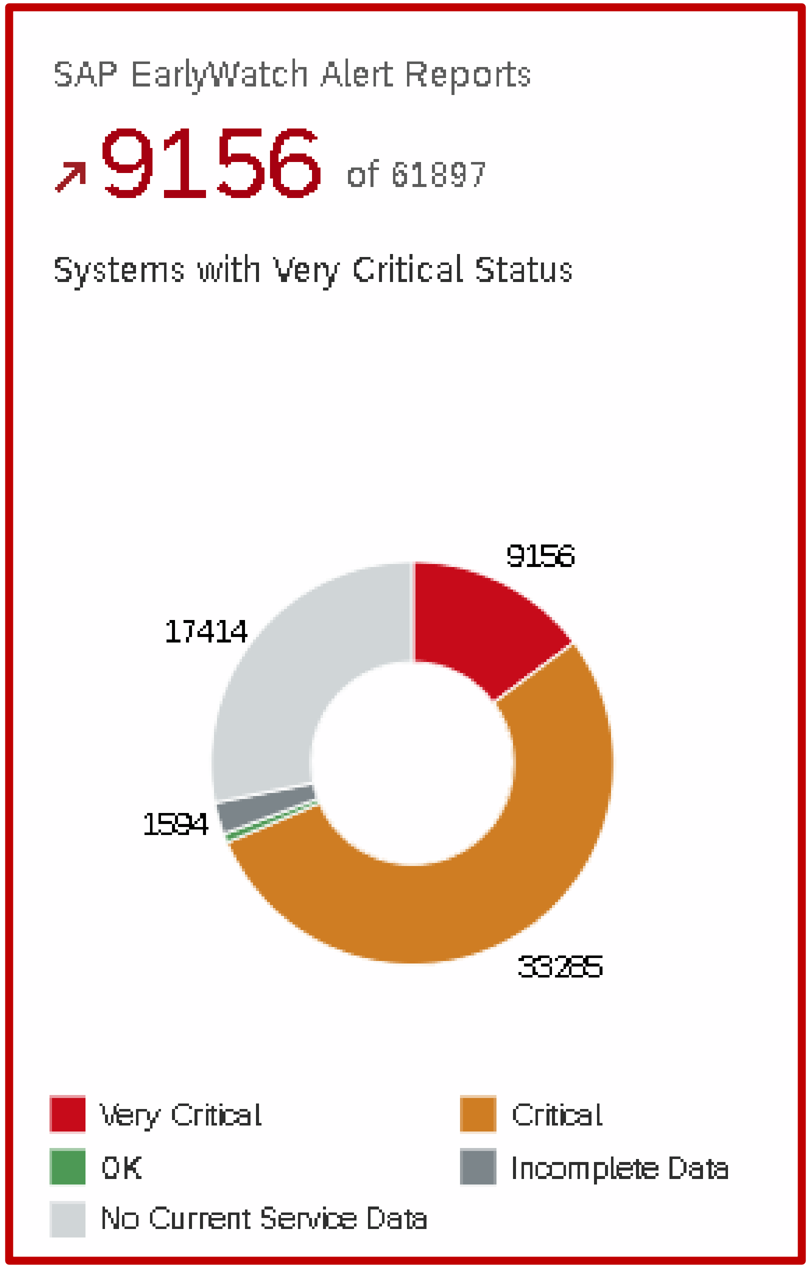
Source: https://www.reuters.com/article/us-sap-security/50000-companies-exposed-to-hacks-of-business-critical-sap-systems-researchers-idUSKCN1S80VJ

Our Cloud Application Services Solution

Just Do It!

Perform
Security Note Patching!

ca. 70% of all systems with critical and very critical status



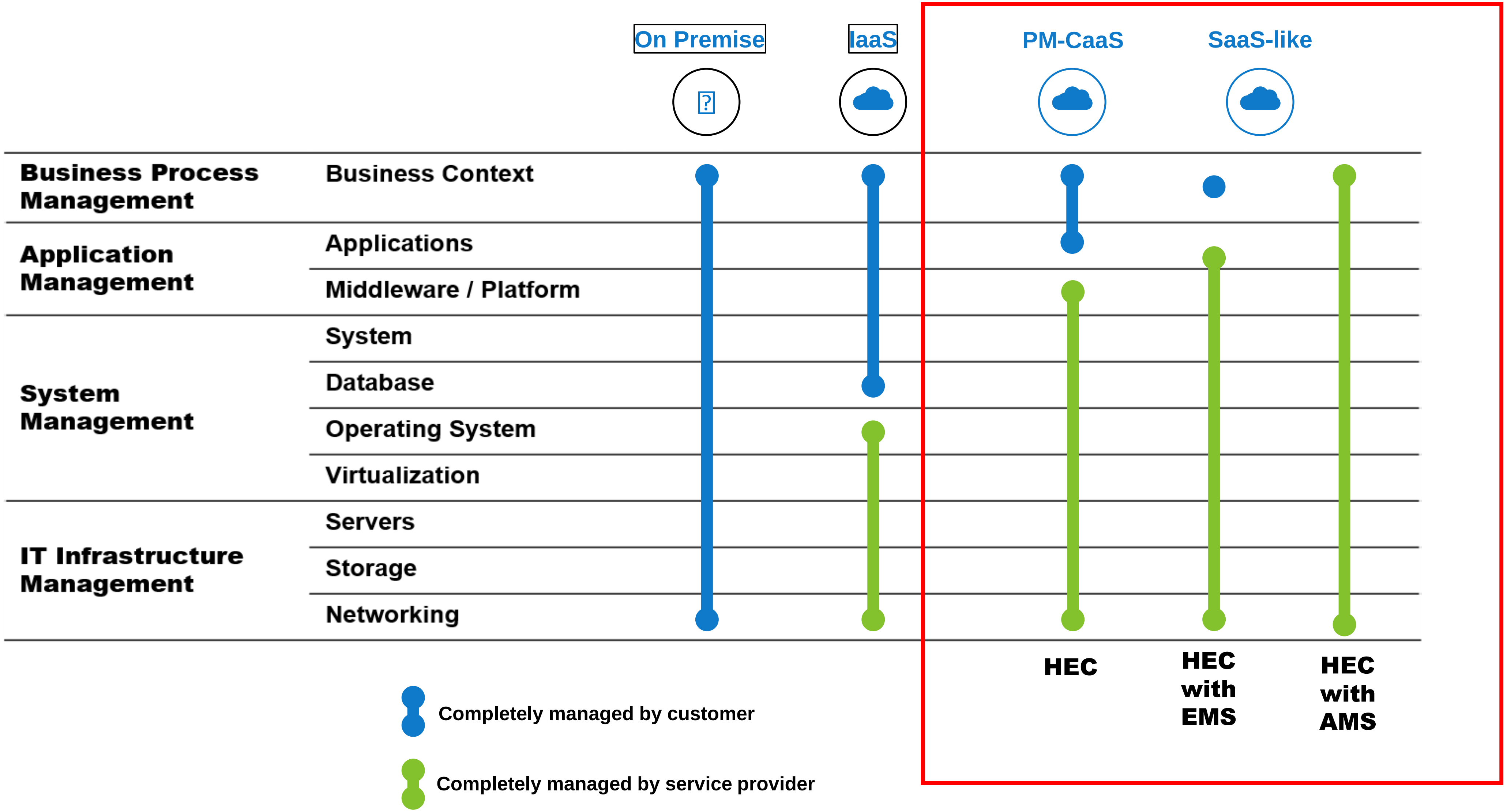
SAP EarlyWatch Alert Reports

↗ 9156 of 61897

Systems with Very Critical Status

Source: https://launchpad.support.sap.com/ewaworkspace

Framework for HEC for Security

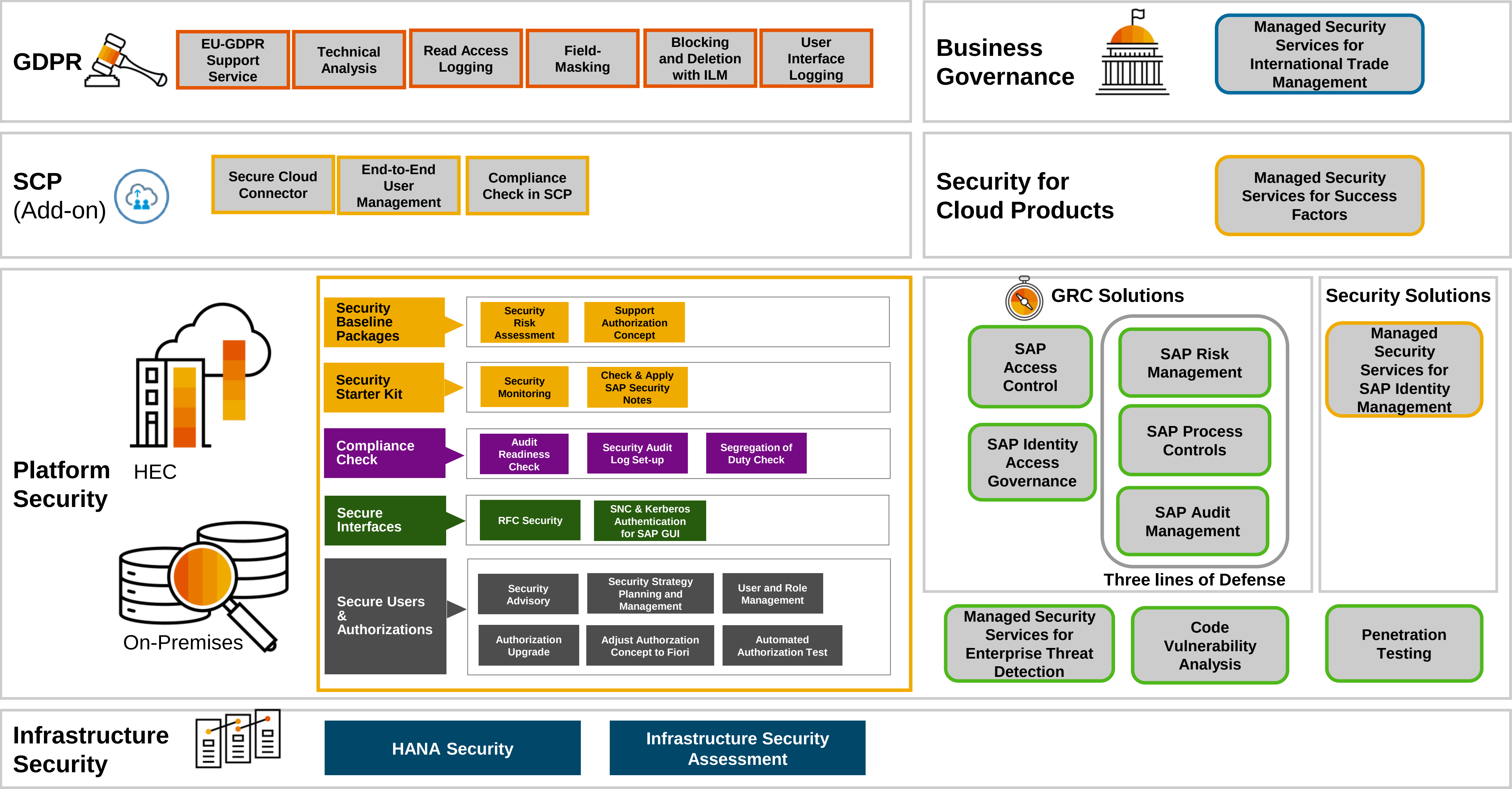


		On Premise	IaaS	PM-CaaS HEC	SaaS-like HEC with EMS	HEC with AMS
Business Process Management	Business Context	🟦	🟦	🟦	🟦	🟩
Application Management	Applications	🟦	🟦	🟦	🟩	🟩
	Middleware / Platform	🟦	🟦	🟩	🟩	🟩
System Management	System	🟦	🟦	🟩	🟩	🟩
	Database	🟦	🟦	🟩	🟩	🟩
	Operating System	🟦	🟩	🟩	🟩	🟩
	Virtualization	🟦	🟩	🟩	🟩	🟩
IT Infrastructure Management	Servers	🟦	🟩	🟩	🟩	🟩
	Storage	🟦	🟩	🟩	🟩	🟩
	Networking	🟦	🟩	🟩	🟩	🟩

🟦 Completely managed by customer

🟩 Completely managed by service provider

Managed Security Services Portfolio



GDPR

- EU-GDPR Support Service
- Technical Analysis
- Read Access Logging
- Field-Masking
- Blocking and Deletion with ILM
- User Interface Logging

Business Governance

- Managed Security Services for International Trade Management

SCP (Add-on)

- Secure Cloud Connector
- End-to-End User Management
- Compliance Check in SCP

Security for Cloud Products

- Managed Security Services for Success Factors

Platform Security

HEC

On-Premises

- **Security Baseline Packages**: Security Risk Assessment; Support Authorization Concept
- **Security Starter Kit**: Security Monitoring; Check & Apply SAP Security Notes
- **Compliance Check**: Audit Readiness Check; Security Audit Log Set-up; Segregation of Duty Check
- **Secure Interfaces**: RFC Security; SNC & Kerberos Authentication for SAP GUI
- **Secure Users & Authorizations**: Security Advisory; Security Strategy Planning and Management; User and Role Management; Authorization Upgrade; Adjust Authorzation Concept to Fiori; Automated Authorization Test

GRC Solutions

- SAP Access Control
- SAP Identity Access Governance

Three lines of Defense

- SAP Risk Management
- SAP Process Controls
- SAP Audit Management

Security Solutions

- Managed Security Services for SAP Identity Management

- Managed Security Services for Enterprise Threat Detection
- Code Vulnerability Analysis
- Penetration Testing

Infrastructure Security

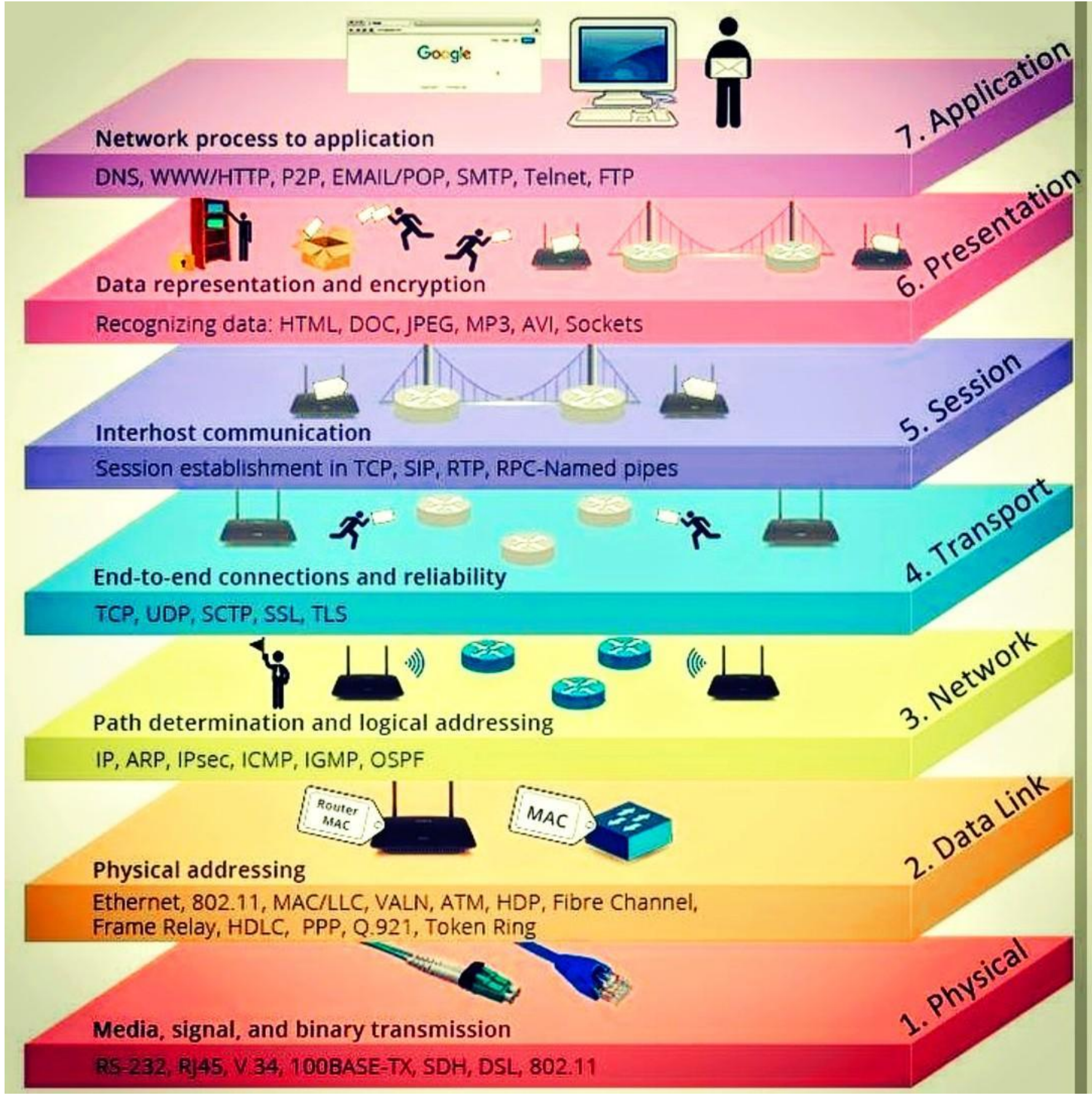
- HANA Security
- Infrastructure Security Assessment

Note: Portfolio Offerings with stand alone services and outcome based packages.

operations Risk Mgmt Compliance Governance

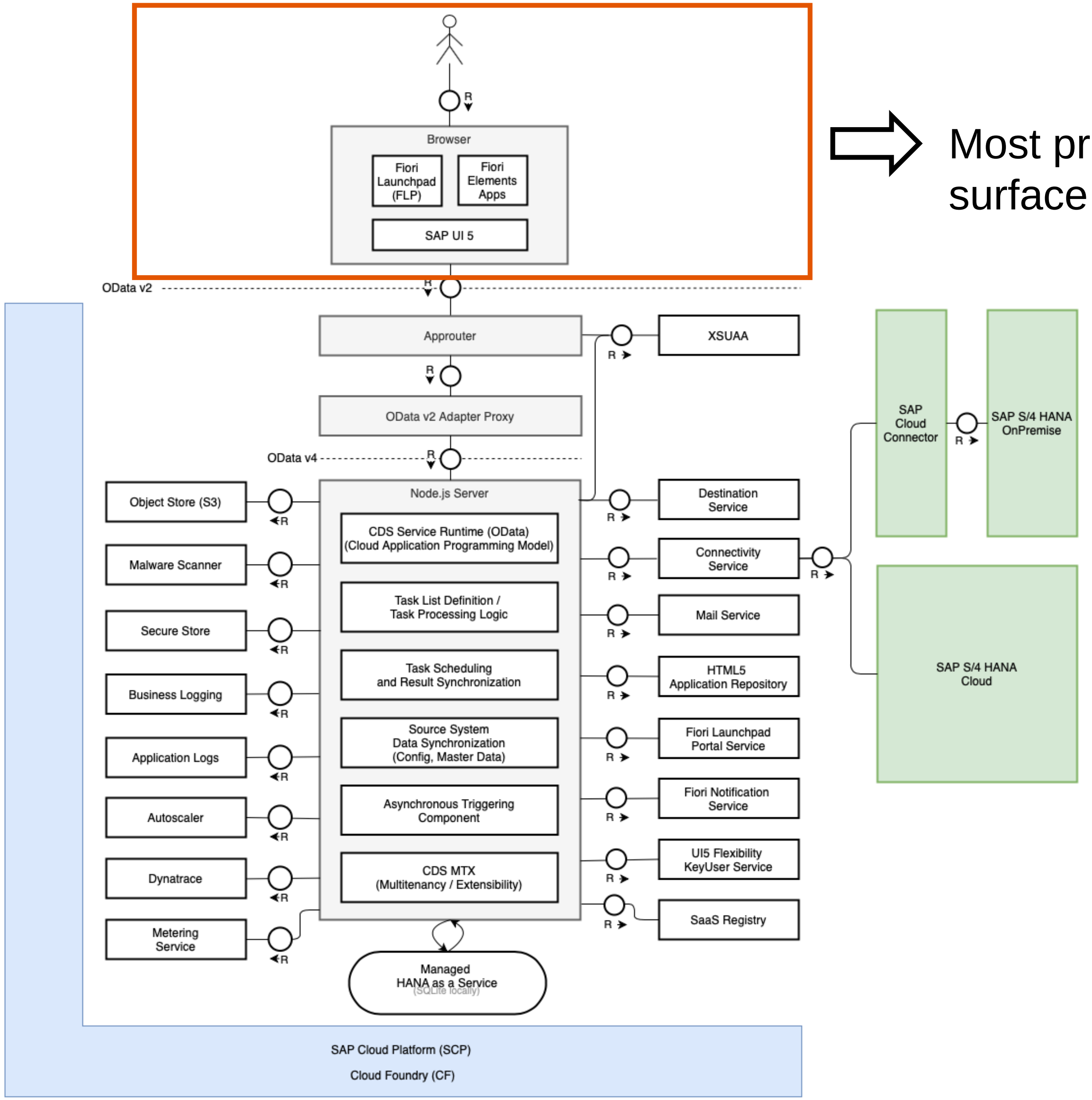
Threat intelligence

Security Layers


Google
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
2. Data Link
Router MAC
MAC
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel, Frame Relay, HDLC, PPP, Q.921, Token Ring
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

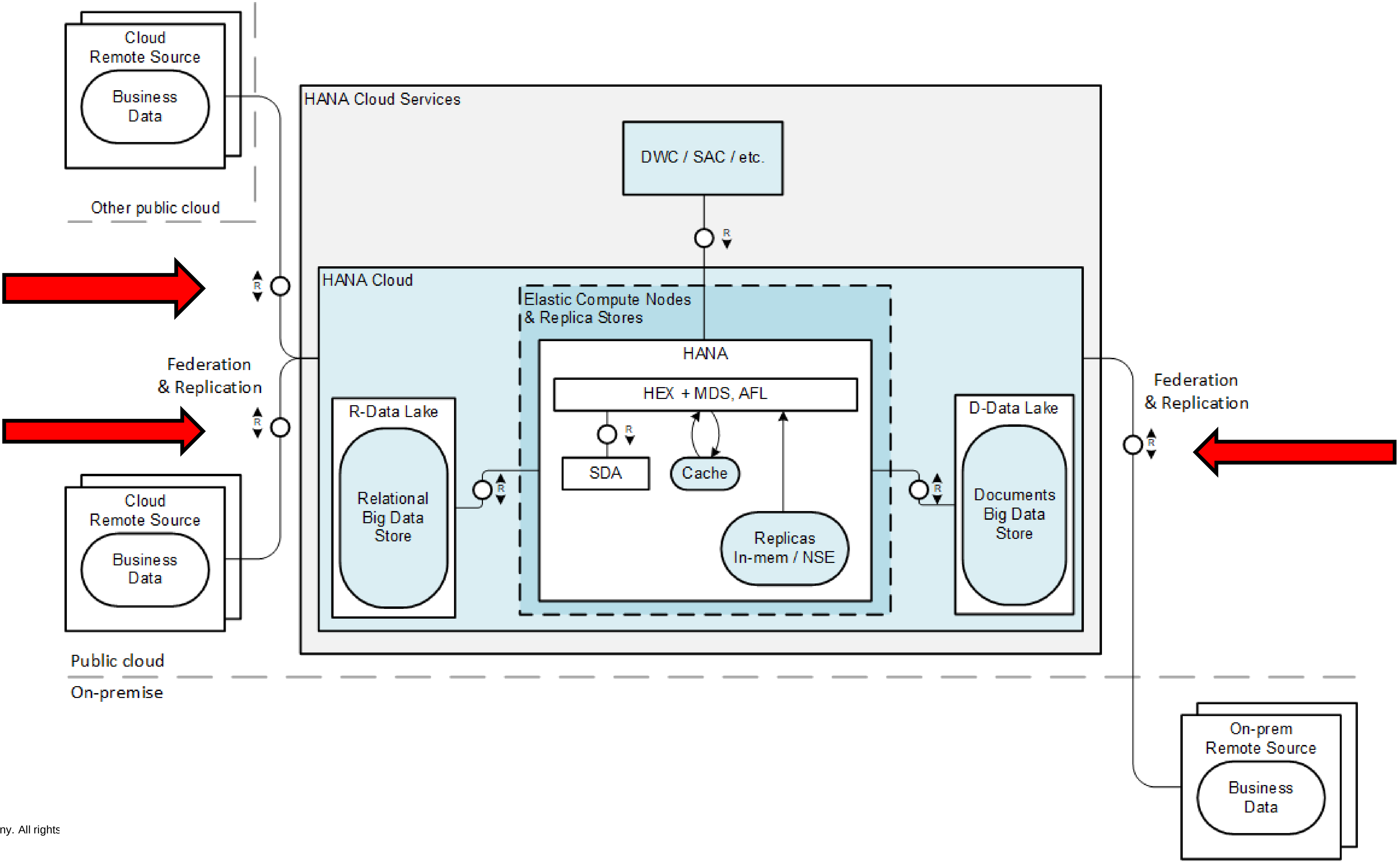
Possible attack vectors

High level Architecture SCP/HEC



Most preferred attack vector / surface

High level Architecture Hana Cloud



Where is the easiest way for hackers?

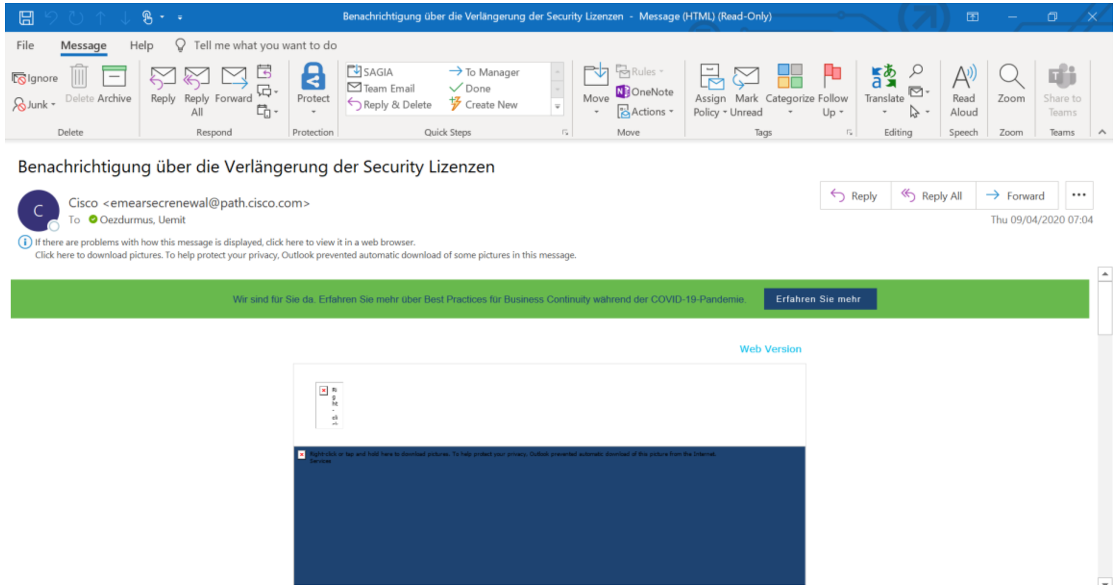
Commonly used target: User Phishing

Different ways to approach a user by using his/her attention by:

- Pharming (redirection to a bogus website)
- Smishing (using SMS as phishing tool)
- Vishing (Using Phone as phishing tool)
- Session hijacking (steal and misuse of user’s security token)
- Whaling (business email compromise, targeting C-level)
- Cloning (using malicious Website)
- Domain spoofing (URL of Website looks real, but isn’t)

➡ **Aiming to hijack or steal user credential**

Example



Benachrichtigung über die Verlängerung der Security Lizenzen

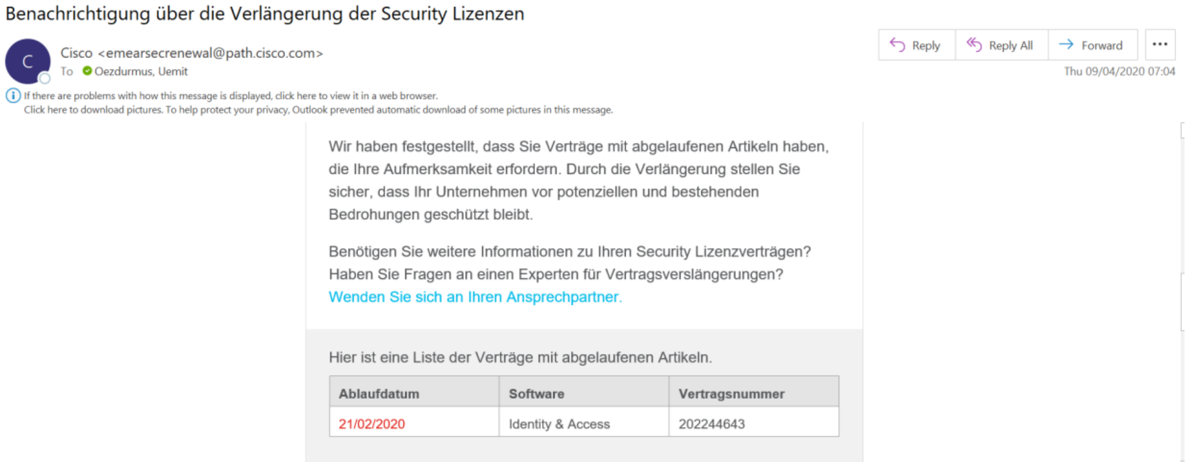
Cisco <emearsecrenewal@path.cisco.com>
To Oezdurmus, Uemit

Thu 09/04/2020 07:04

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Wir sind für Sie da. Erfahren Sie mehr über Best Practices für Business Continuity während der COVID-19-Pandemie.

Right-click or tap and hold here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.
Services



Benachrichtigung über die Verlängerung der Security Lizenzen

Cisco <emearsecrenewal@path.cisco.com>
To Oezdurmus, Uemit

Thu 09/04/2020 07:04

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

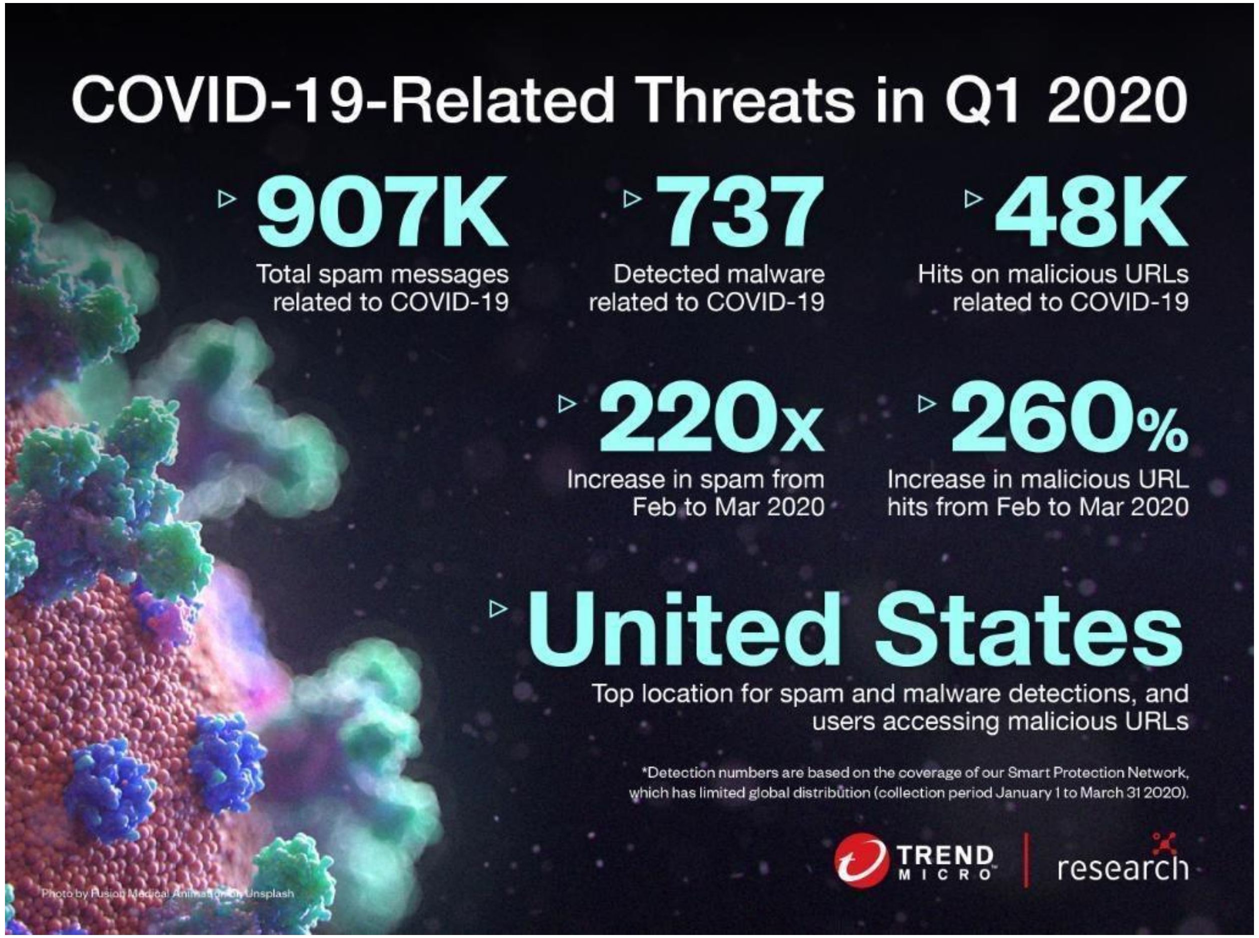
Wir haben festgestellt, dass Sie Verträge mit abgelaufenen Artikeln haben, die Ihre Aufmerksamkeit erfordern. Durch die Verlängerung stellen Sie sicher, dass Ihr Unternehmen vor potenziellen und bestehenden Bedrohungen geschützt bleibt.

Benötigen Sie weitere Informationen zu Ihren Security Lizenzverträgen? Haben Sie Fragen an einen Experten für Vertragsverslängerungen? Wenden Sie sich an Ihren Ansprechpartner.

Hier ist eine Liste der Verträge mit abgelaufenen Artikeln.

Ablaufdatum	Software	Vertragsnummer
21/02/2020	Identity & Access	202244643

2020 Actuals (source TrendMicro)



COVID-19-Related Threats in Q1 2020

▷ **907K**
Total spam messages related to COVID-19

▷ **737**
Detected malware related to COVID-19

▷ **48K**
Hits on malicious URLs related to COVID-19

▷ **220x**
Increase in spam from Feb to Mar 2020

▷ **260%**
Increase in malicious URL hits from Feb to Mar 2020

▷ **United States**
Top location for spam and malware detections, and users accessing malicious URLs

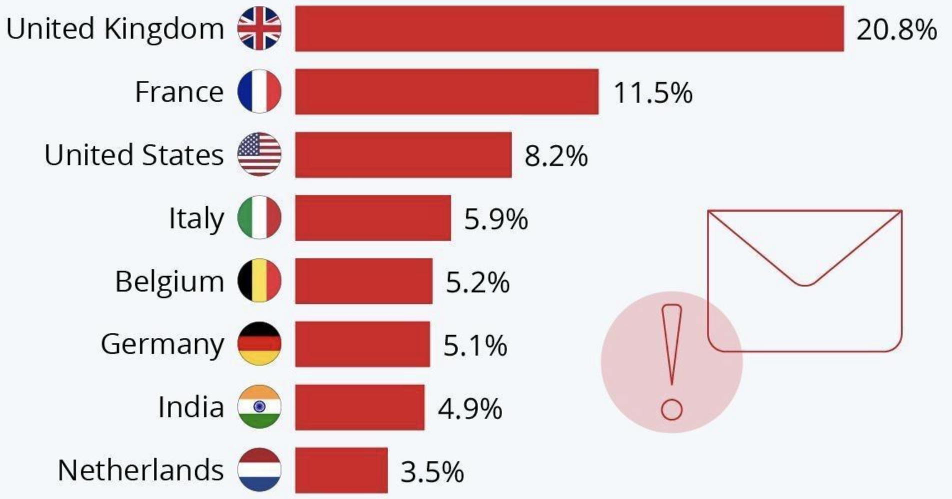
*Detection numbers are based on the coverage of our Smart Protection Network, which has limited global distribution (collection period January 1 to March 31 2020).

TREND MICRO | research

Photo by Fusion Medical Animation on Unsplash

The Countries Targeted Most by Malicious Coronavirus Spam

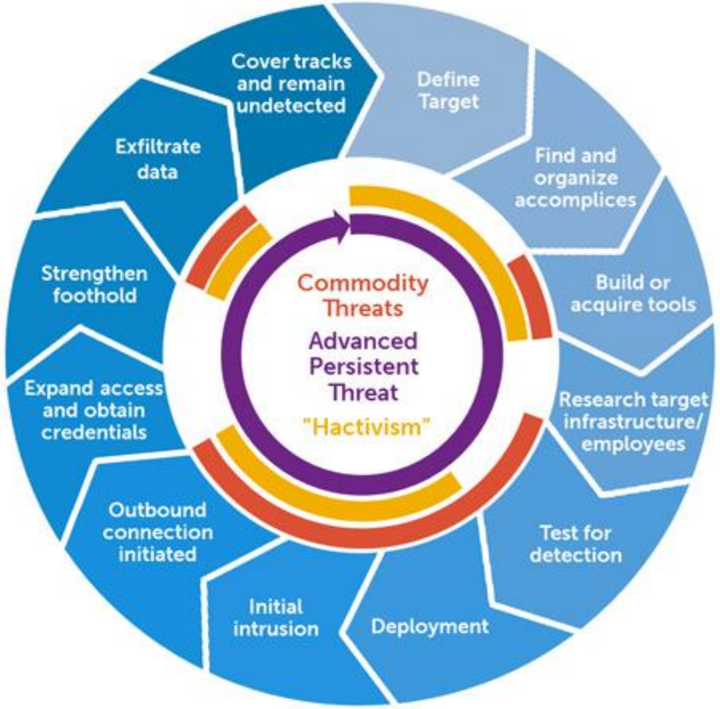
Countries targeted by largest share of global malicious spam emails with 'coronavirus' in the subject*



* January 1 to March 27, 2020.
Source: Trend Micro

Critical and hard to identify – Advanced Persistent Threat (Wikipedia)

An advanced persistent threat **(APT)** is a prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an period of time. The intention of an **APT attack** is usually to monitor network activity and steal data rather than to cause damage to the network or organization.



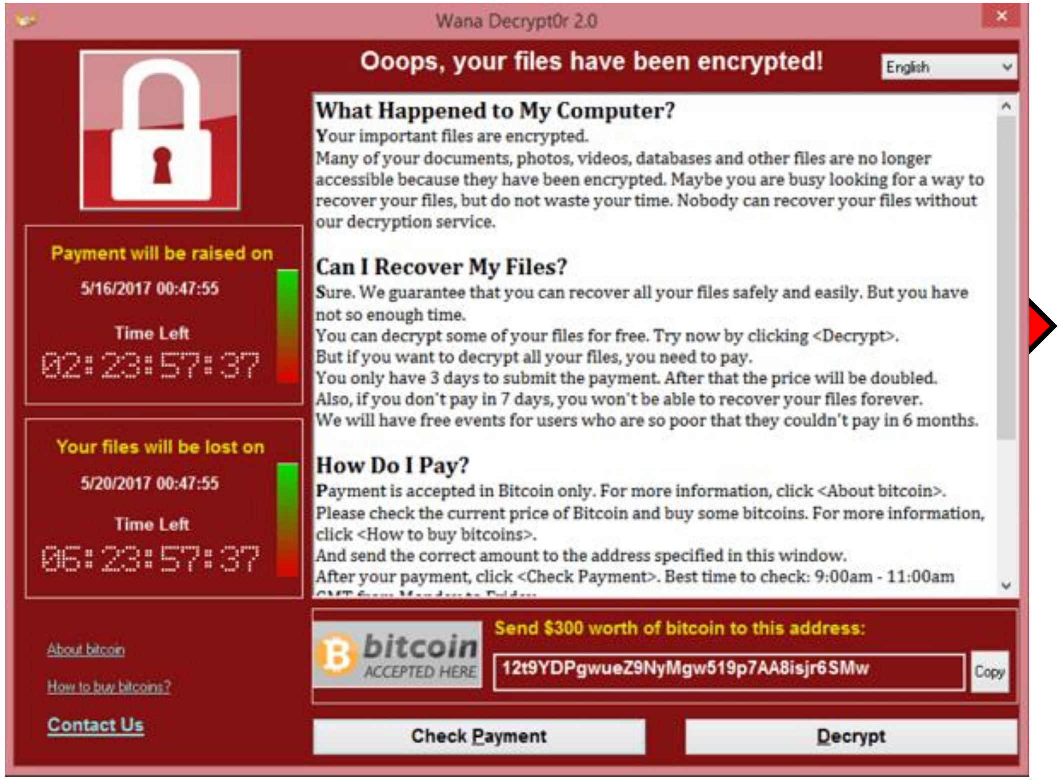
Cover tracks and remain undetected
Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Commodity Threats
Advanced Persistent Threat
"Hactivism"

Targeting business related systems of any kind, mainly used for:

- ❑ Steal Data
- ❑ Manipulate Data
- ❑ Manipulate systems
- ❑ Open backdoors for other hackers

Critical and hard to eliminate – Ransomware (Wikipedia)

Ransomware is a type of malware from cryptovirology that threatens to publish the victim’s data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Example: Wannacry

Targeting business related systems of any kind, mainly used for:

- Manipulate / encrypt Data
- Sabotage of systems DB systems
- Open backdoors for other hackers

What can we do to protect?

What to consider and protect – The end user

According to an independent survey of End Users:

80% would open suspicious emails and documents within their company’s network and devices, because they believed that those environments are much more protected than their private once.

To strengthen IT Security, the imperative is to educate and train the end user in parallel to setting up company security policies and guidelines.

What to consider and protect – end-to-end security

Processing Servers

Database Servers

Network FW/Switches
Gateways

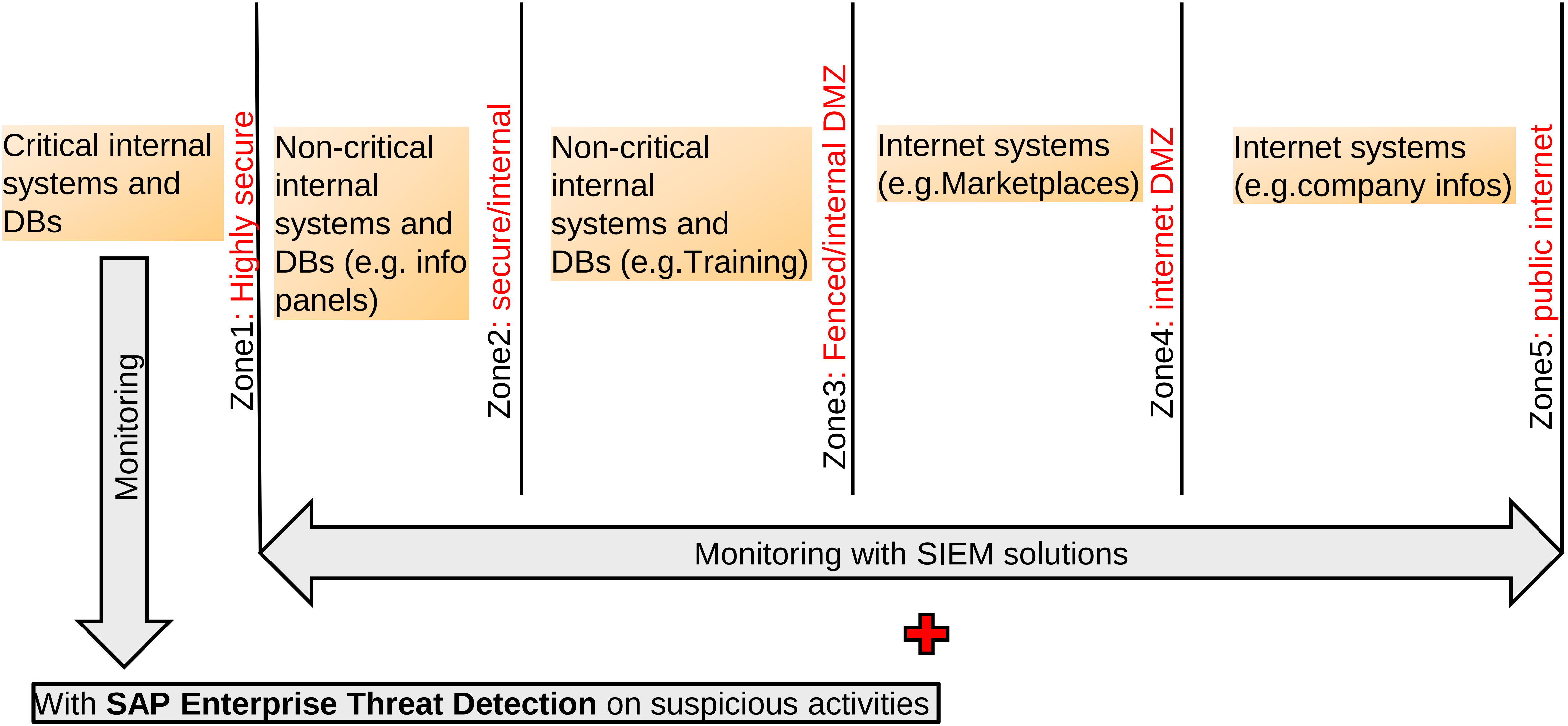
Email Servers / User accounts

Wifi Routers

User end devices

Mobile devices

What to consider and protect – network zones, segmentation and monitoring



Critical internal systems and DBs

Zone1: Highly secure

Non-critical internal systems and DBs (e.g. info panels)

Zone2: secure/internal

Non-critical internal systems and DBs (e.g.Training)

Zone3: Fenced/internal DMZ

Internet systems (e.g.Marketplaces)

Zone4: internet DMZ

Internet systems (e.g.company infos)

Zone5: public internet

Monitoring

Monitoring with SIEM solutions

With **SAP Enterprise Threat Detection** on suspicious activities

Managed Security Services Portfolio

GDPR

- EU-GDPR Support Service
- Technical Analysis
- Read Access Logging
- Field-Masking
- Blocking and Deletion with ILM
- User Interface Logging

Business Governance

- Managed Security Services for International Trade Management

SCP (Add-on)

- Secure Cloud Connector
- End-to-End User Management
- Compliance Check in SCP

Security for Cloud Products

- Managed Security Services for Success Factors

Platform Security

HEC

On-Premises

Security Baseline Packages
- Security Risk Assessment
- Support Authorization Concept

Security Starter Kit
- Security Monitoring
- Check & Apply SAP Security Notes

Compliance Check
- Audit Readiness Check
- Security Audit Log Set-up
- Segregation of Duty Check

Secure Interfaces
- RFC Security
- SNC & Kerberos Authentication for SAP GUI

Secure Users & Authorizations
- Security Advisory
- Security Strategy Planning and Management
- User and Role Management
- Authorization Upgrade
- Adjust Authorzation Concept to Fiori
- Automated Authorization Test

GRC Solutions

- SAP Access Control
- SAP Identity Access Governance

Three lines of Defense
- SAP Risk Management
- SAP Process Controls
- SAP Audit Management

Security Solutions

- Managed Security Services for SAP Identity Management

- Managed Security Services for Enterprise Threat Detection
- Code Vulnerability Analysis
- Penetration Testing

Infrastructure Security

- HANA Security
- Infrastructure Security Assessment

Note: Portfolio Offerings with stand alone services and outcome based packages.

operations Risk Mgmt Compliance Governance

Q & A

Thank you.

Contact information:

Uemit Oezdurmus
Global Head Managed Security Services

SAP Deutschland SE & Co.KG

T +49 175-2773725

E uemit.oezdurmus@sap.com

SAP® Cloud Application Services
We help The Best Run better

THE BEST RUN SAP®