IT-SA 2022

Access Management:

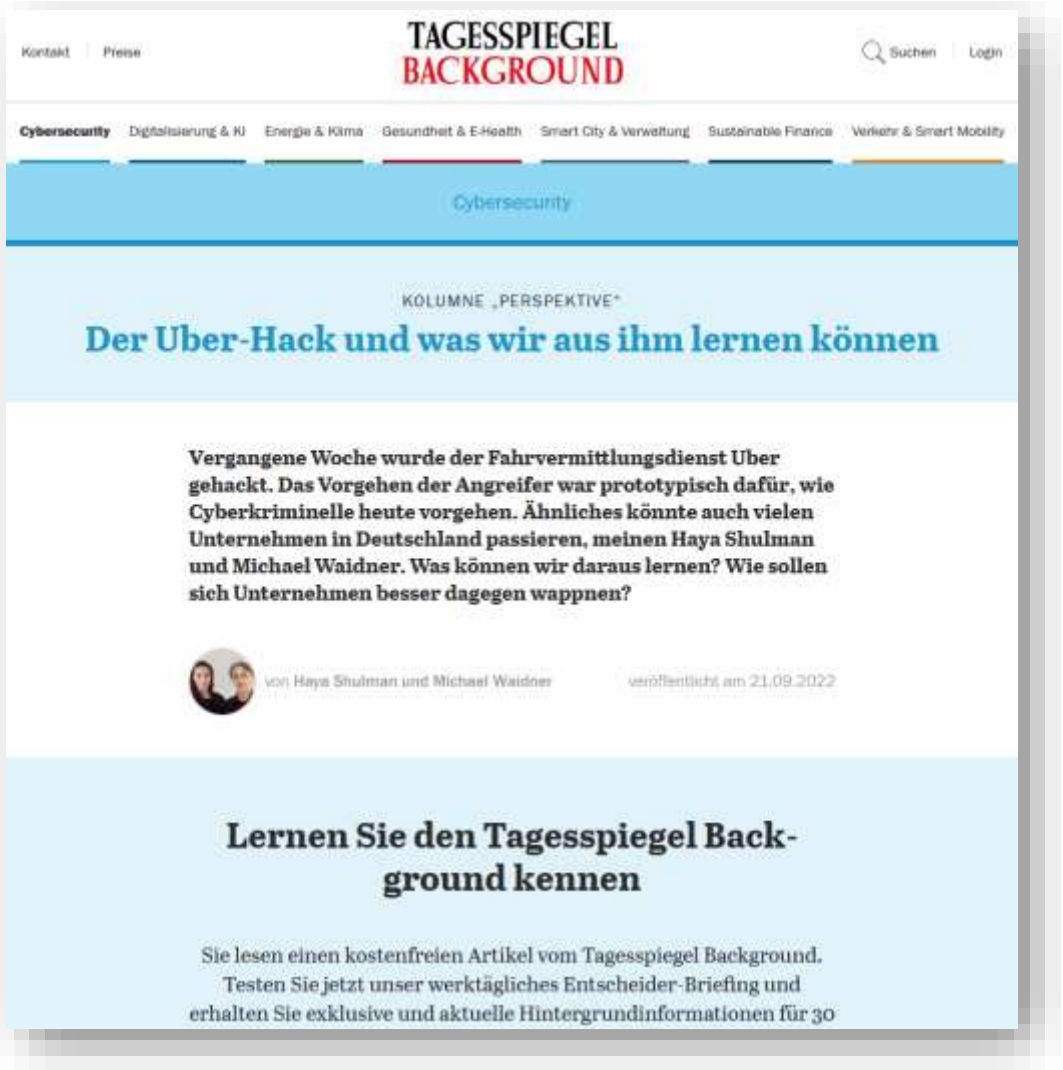
Transparenz, Kontrolle und Compliance für KRITIS und Industrie

Stefan Rabben | 26.10.2022

Business Case

	AUSGANGSLAGE	ANFORDERUNGEN	ZU SCHÜTZEN
CYBER SECURITY	Angespannte Bedrohungslage	Europäische Technologien	IDENDITÄTEN
	Herkömmliche Technologien nicht ausreichend	Zero Trust Architekturen	ZUGANGSDATEN
		Transparenz & Kontrolle	SYSTEMZUGRIFFE (Sitzungen)
COMPLIANCE & RISIKO MANAGEMENT	KRITIS	ISO27001, Anhang A B3S	ACCESS MANAGEMENT (BSI Risikomanagement Standard 200-3)
	INDUSTRIE	ISO27001, Anhang A TISAX, NIST, IEC62443	
	BETRIFFT	ANFORDERUNGEN	UMSETZUNG

Aus gegebenem Anlass: UBER Hack



Kontakt Preise

TAGESSPIEGEL BACKGROUND

Suchen Login

Cybersecurity Digitalisierung & KI Energie & Klima Gesundheit & E-Health Smart City & Verwaltung Sustainable Finance Verkehr & Smart Mobility

Cybersecurity

KOLUMNE „PERSPEKTIVE"

Der Uber-Hack und was wir aus ihm lernen können

Vergangene Woche wurde der Fahrvermittlungsdienst Uber gehackt. Das Vorgehen der Angreifer war prototypisch dafür, wie Cyberkriminelle heute vorgehen. Ähnliches könnte auch vielen Unternehmen in Deutschland passieren, meinen Haya Shulman und Michael Waidner. Was können wir daraus lernen? Wie sollen sich Unternehmen besser dagegen wappnen?

von Haya Shulman und Michael Waidner veröffentlicht am 21.09.2022

Lernen Sie den Tagesspiegel Background kennen

Sie lesen einen kostenfreien Artikel vom Tagesspiegel Background. Testen Sie jetzt unser werktägliches Entscheider-Briefing und erhalten Sie exklusive und aktuelle Hintergrundinformationen für 30

https://background.tagesspiegel.de/cybersecurity/der-uber-hack-und-was-wir-aus-ihm-lernen-koennen

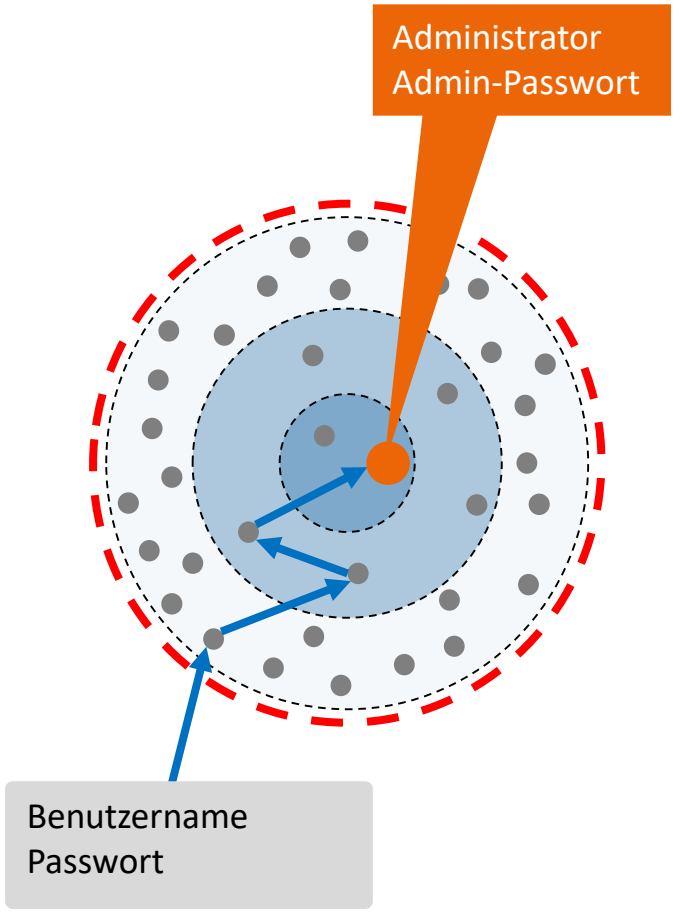
Was ist passiert?

1. **Social Engineering:**
   (Nicht-privilegierte) Zugangsdaten eines externen Beraters erhalten

2. **Passieren der Perimeter:**
   Über Fernzugriffsschnittstelle VPN-Zugang zum Intranet

3. **Scannen & Springen:**
   Scannen nach weiteren erreichbaren Systemen → „Hopping“

4. **Treffer gelandet:**
   Ungeschütztes Netzlaufwerk mit Powershell-Skript entdeckt:
   Inhalt: **Super-Administrator Zugangsdaten in Klartext**



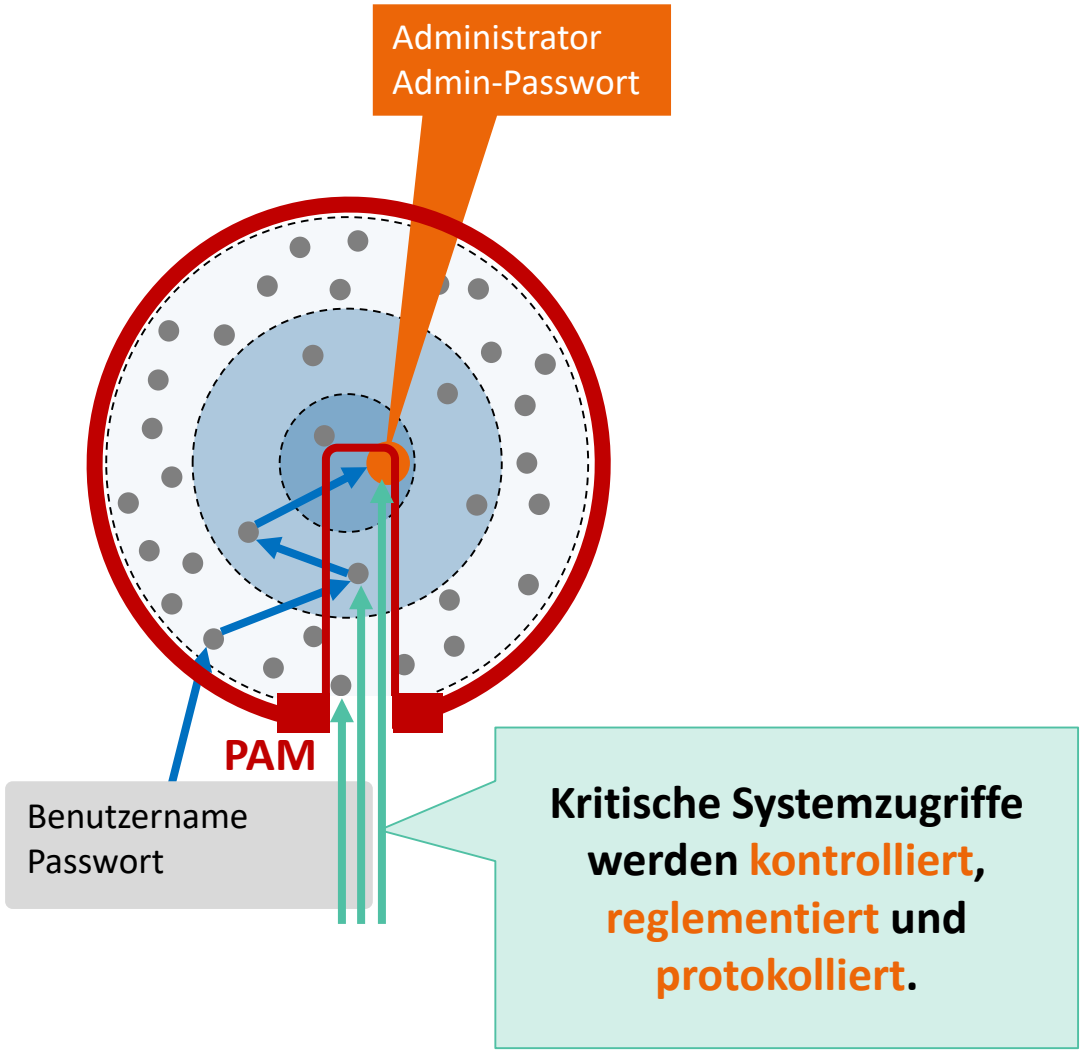
Wie schützt ACCESS MANAGEMENT?

1. **Keine Zugangsdaten im Klartext:**
   Zugangsdaten in Programmen und Skripten durch **API Calls** ersetzt

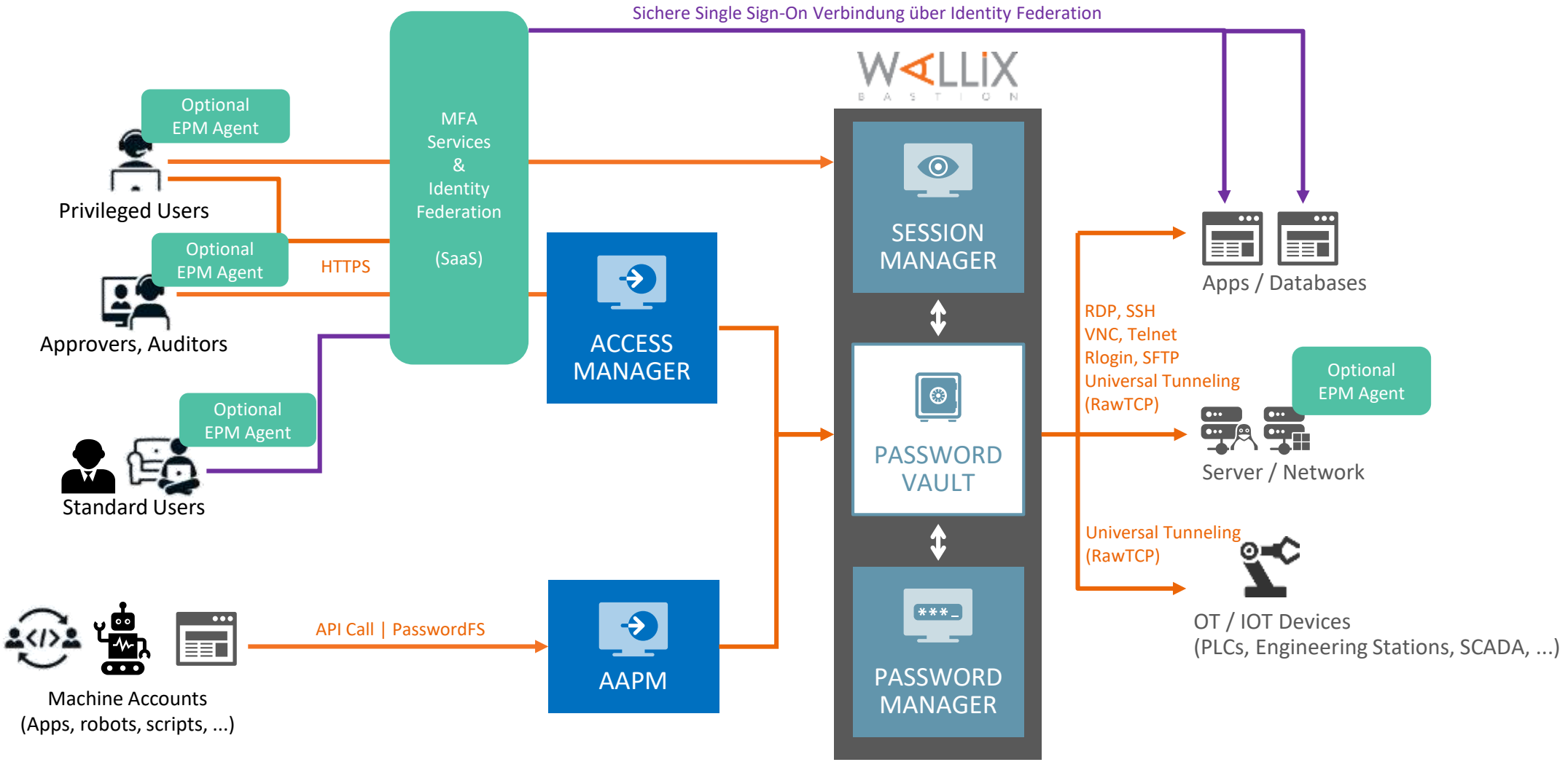
2. **Systemzugangsdaten unbekannt:**
   Benutzer **kennen keine Zugangsdaten** mehr (zentrale Password Vaults)

3. **„Hopping“ unterbunden:**
   Springen auf andere Systeme oder Subnetze nicht **mehr möglich**

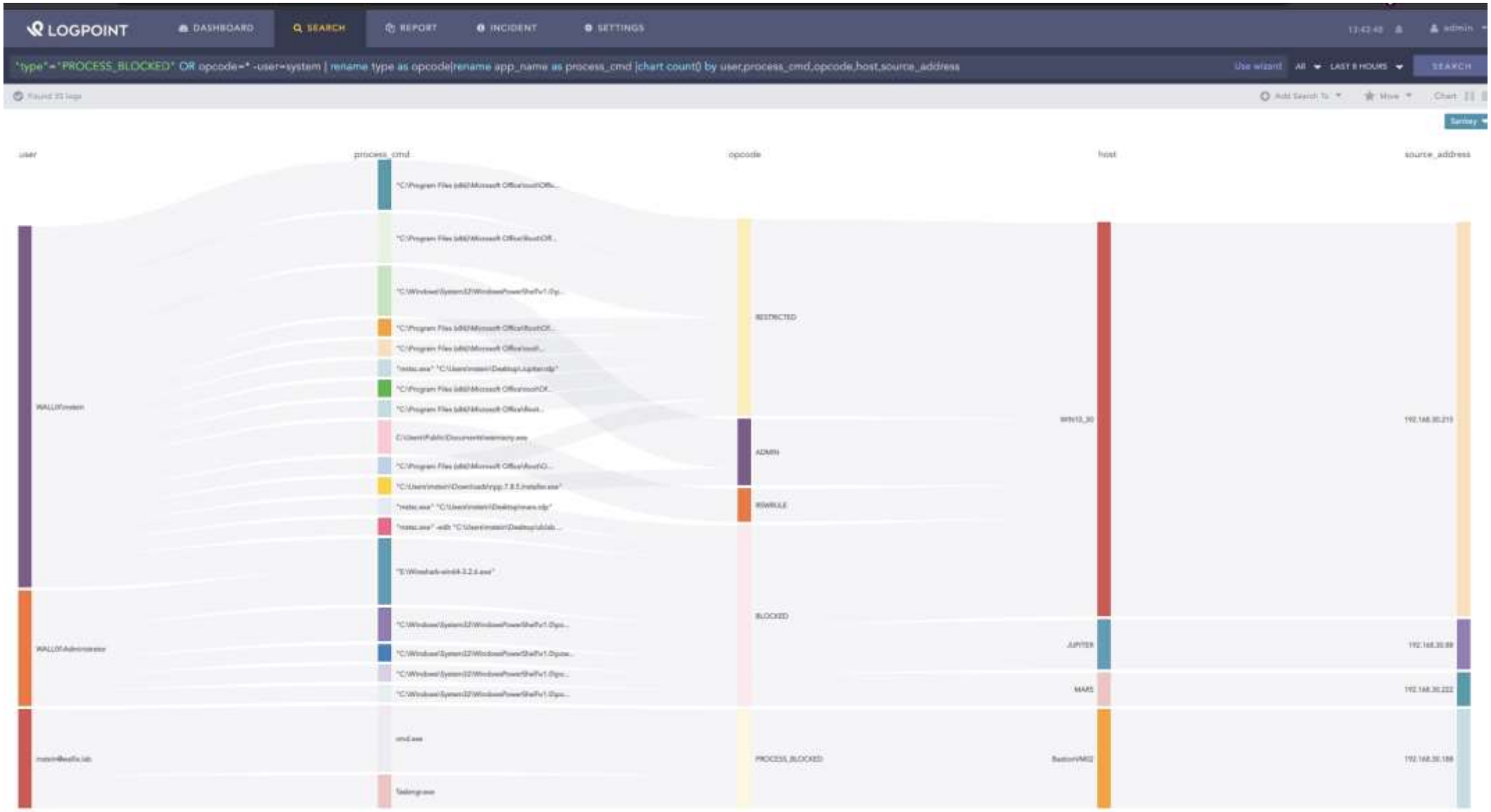
4. **Sicherung der Perimeter:**
   Fernzugriffsschnittstellen eliminiert, zentraler Zugang über PAM



Technologie & Architektur

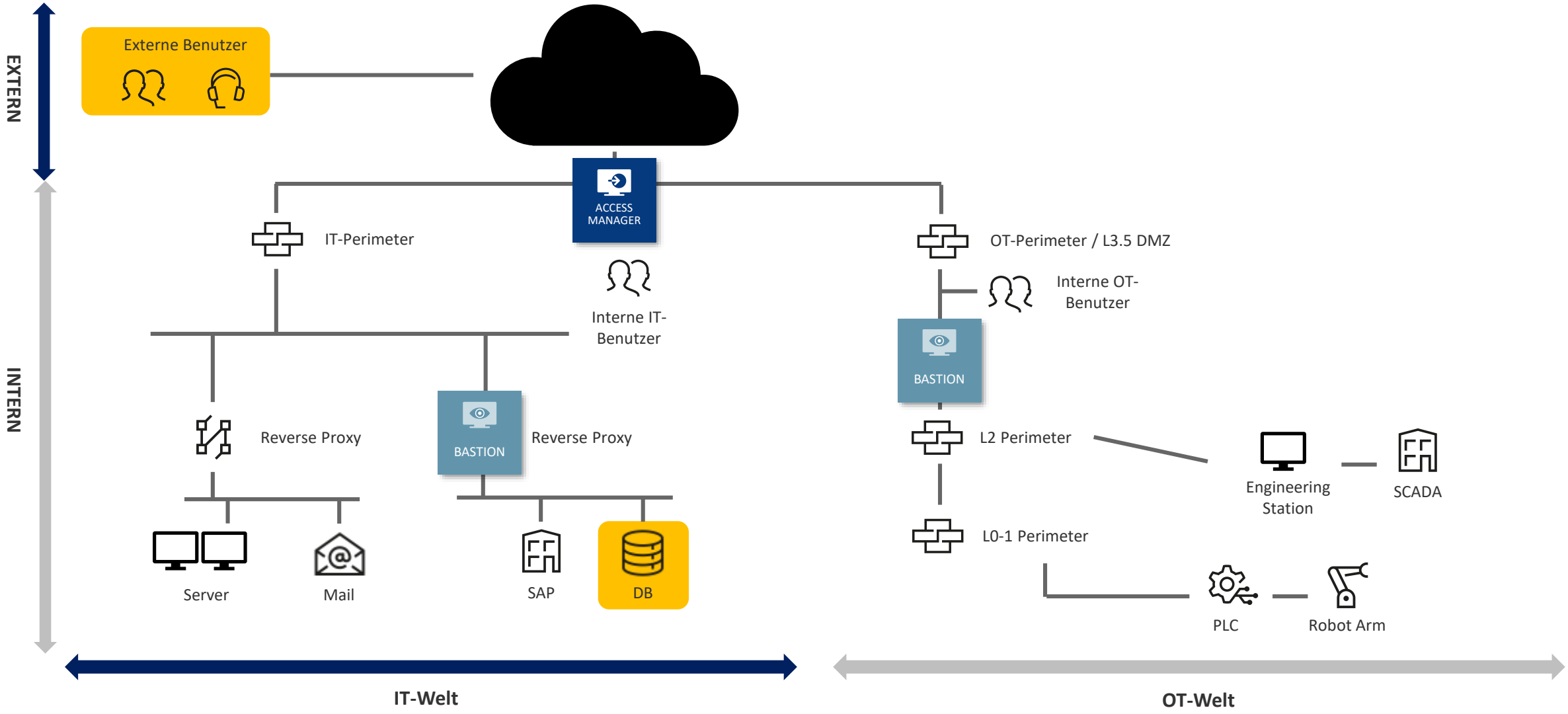


Anhang 2: SIEM Integration



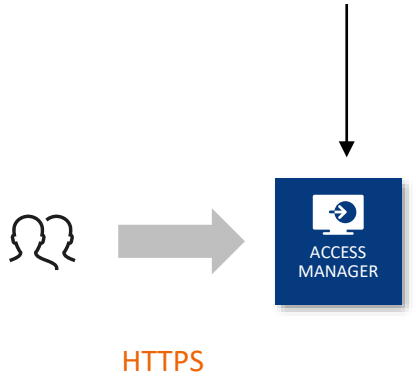
Benutzer | Applikation / Prozess | Security Event | Host | Quell-IP Adresse

Technologie & Architektur



Use Case 1: Sichere Verbindung zu einer Datenbank (IT)

IAM, LDAP oder lokale Benutzer-Datenbank



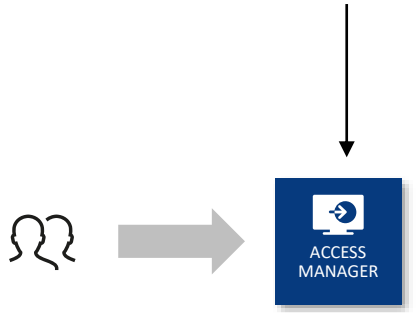
1

HTTPS-Verbindung über Webbrowser zum zentralen Zugangsportal (Access Manager).
(kein VPN, Remote-Client oder sichere Workstation erforderlich)

Benutzer authentifiziert sich mit seinem Benutzernamen.

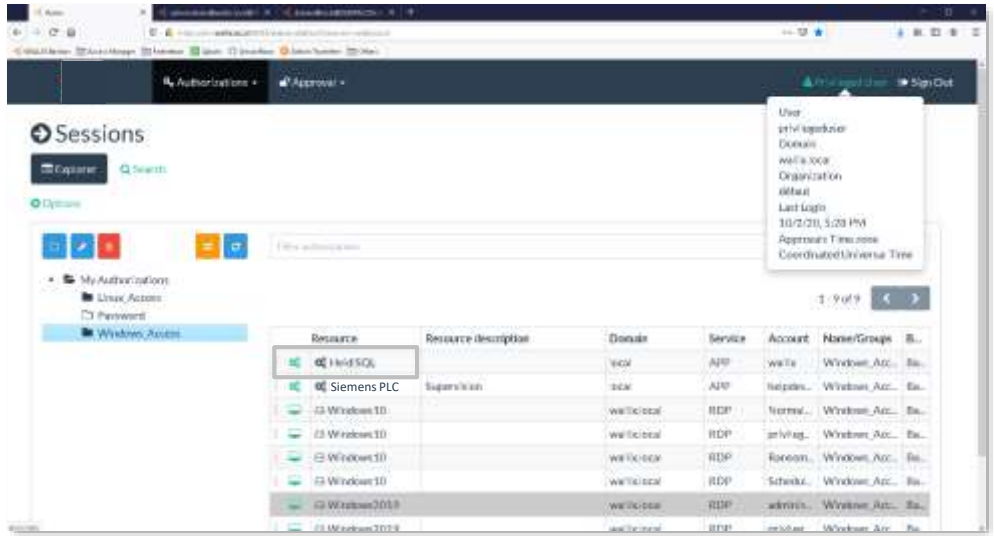
Use Case 1: Sichere Verbindung zu einer Datenbank (IT)

IAM, LDAP oder lokale Benutzer-Datenbank



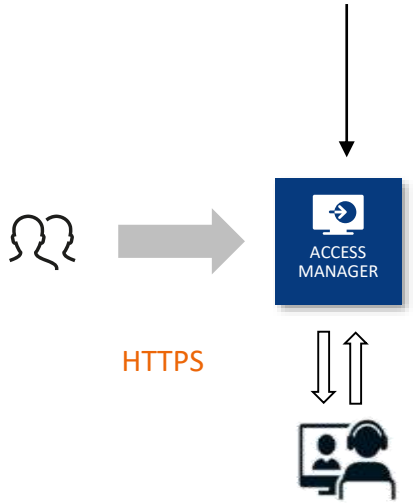
2

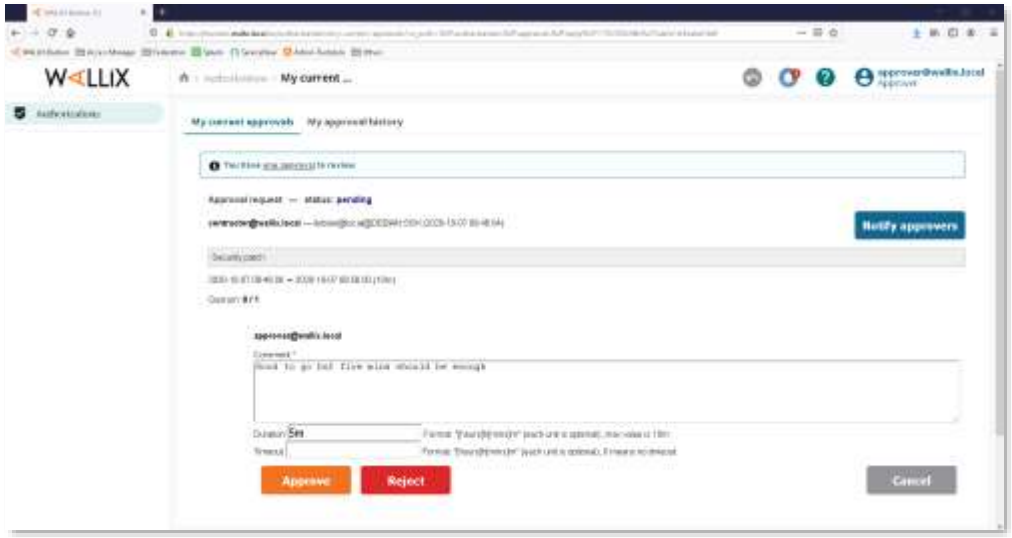
Zielsystem wird über Web-GUI ausgewählt
(hier: Datenbank)



Use Case 1: Sichere Verbindung zu einer Datenbank (IT)

IAM, LDAP oder lokale Benutzer-Datenbank

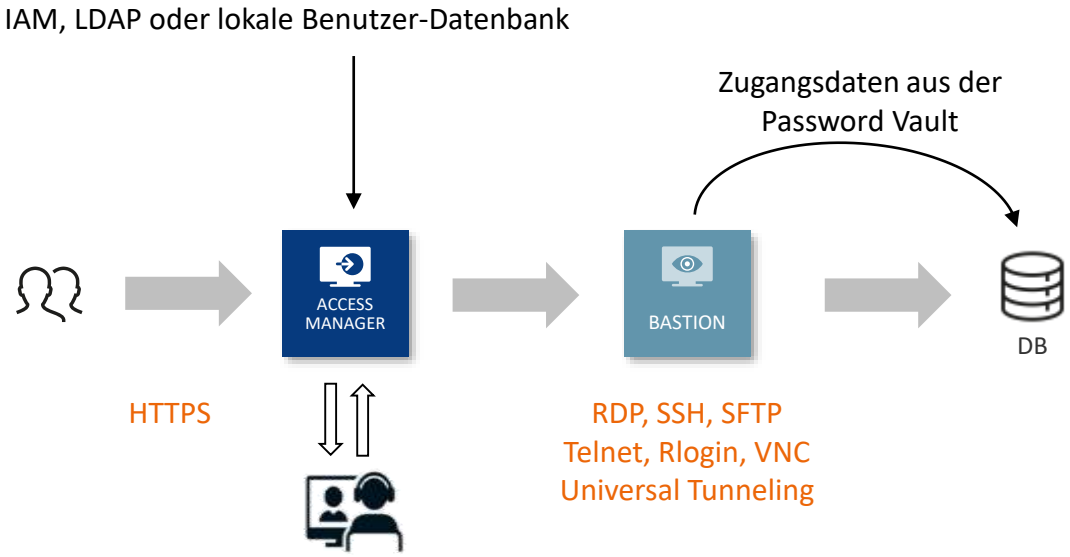


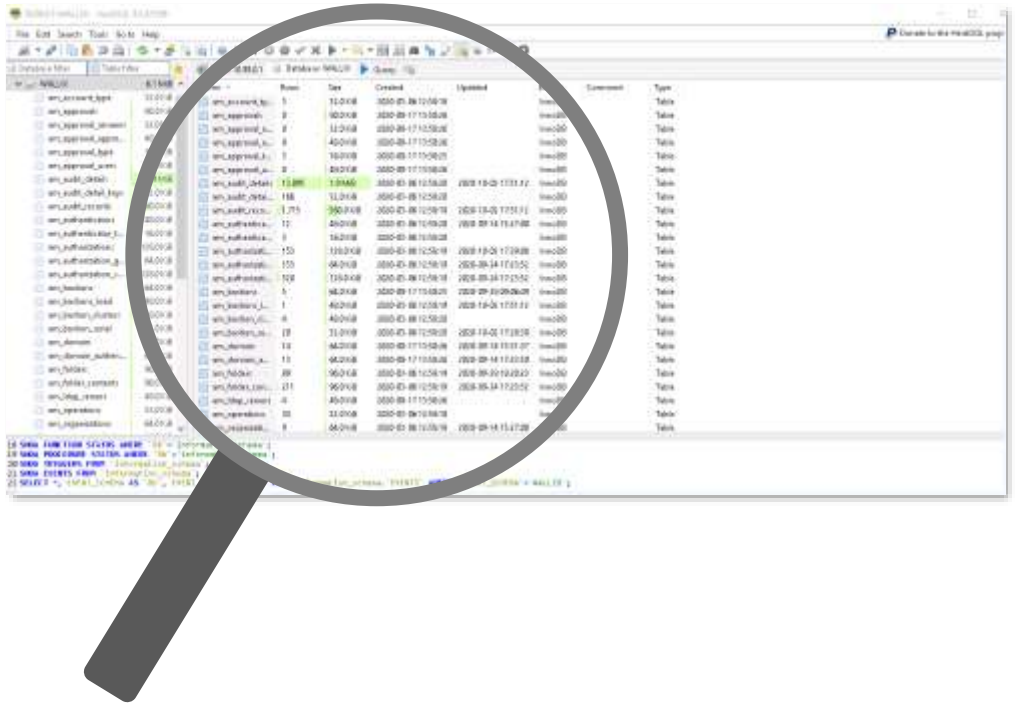


3

Genehmigungs-Workflow (sofern notwendig) wird eingeleitet

Use Case 1: Sichere Verbindung zu einer Datenbank (IT)

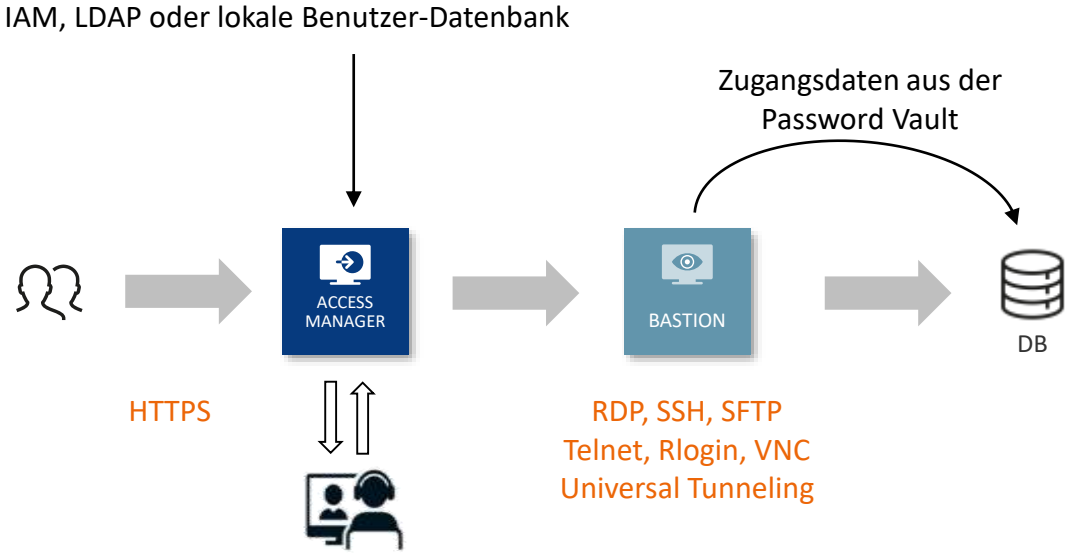


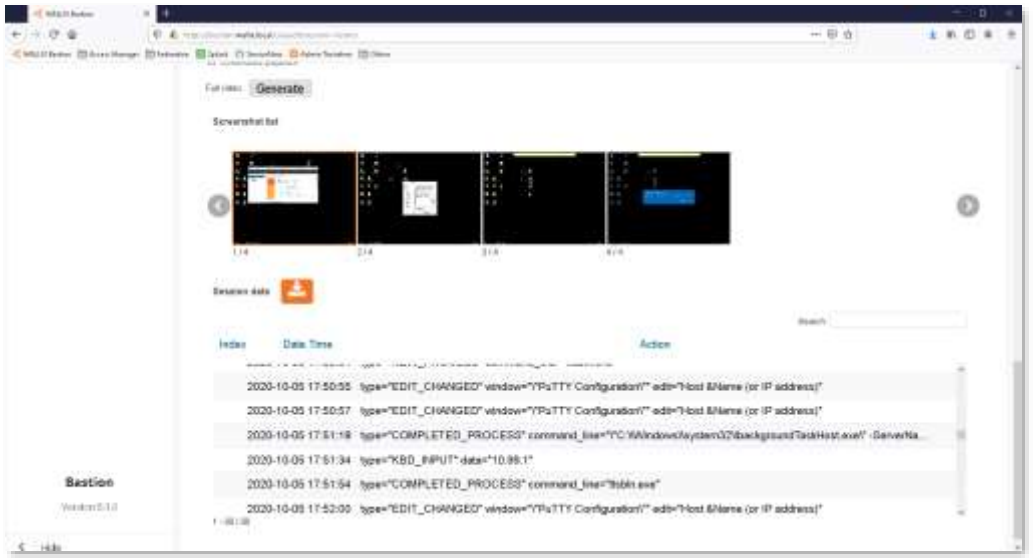


4

Agentenlose Verbindung zum Target wird herstellt.
Benutzer wird per SSO authentifiziert
Sitzungs-Policies werden etabliert

Use Case 1: Sichere Verbindung zu einer Datenbank (IT)





5

Sitzung wird aufgezeichnet (Video und Metadaten):

- Auditor kann sich aufschalten (4 Eyes, 4 Hands Principle)
- Audit Trails werden sicher abgelegt

Integrationen

Platforms	Identity IGA/IAM	Multifactor Authentication & SSO	Vault	SIEM	Vulnerability Mgt	DevOps	Antivirus / DLP	ITSM	Other	OT	Behavior Analytics
Microsoft Azure	OGITIX	gemalto	HashiCorp	LOGPOINT	Qualys.	ANSIBLE	FORCEPOINT	servicenow	Alleantia	fives	CYBER
amazon web services	Evidian	onelogin	HID	CYBERARK	IBM Security	Cyberwatch	Terraform	kaspersky	ConnectWise	bertin	
Google Cloud Platform	SailPoint	inwebo	okta	thycotic	splunk>	tenable	kubernetes	falcongaze	bmc	NUTANIX	
openstack	okta	Ping	DUO		BACKBOX	docker	McAfee				
Microsoft Hyper-v	Brainwave GRC	SecurEnvoy	yubico		blueprism						
vmware READY	Kleverware				beyond						

Standard Protocols				
{ REST-API }	Active Directory	SAML	SCIM	ICAP
	Radius	LDAP.com	syslog	KERBEROS

WALLIX PAM4ALL

Die Einführung von PRIVILEGED ACCESS MANAGEMENT ist das BINDEGLIED zwischen den meisten technischen Controls im Anhang A der ISO 27001 zu allen anderen technischen Lösungen im Cybersicherheitsspektrum.

Fragen und Demos bei uns am Stand

Digital Trust:
Virtueller Fallschirmsprung am Stand

WALLIX Stand: Halle 6, Stand 322

Vielen Dank

Stefan Rabben
M: 0162 – 283 6973
E: srabben@wallix.com