



Alexander Schwemberger
BearingPoint AT
+43 664 88 31 85 03
alexander.schwemberger@bearingpoint.com



Guido Erroi
Cyolo D-A-CH
+41 78 238 1212
guido@cyolo.io

Remote PAM

Wie ZTNA, IAM und SRA zusammenwachsen

06.06.2024



Warum Remote PAM?

Unsichere Fernzugriffe gefährden IT und OT.

- Unzureichend gesicherter Fernzugriff auf OT und IT-Ressourcen ist ein häufiges Einfallstor für Cyberattacken
- Ausnutzen von Schwachstellen, Diebstahl von Zugangsdaten, Supply Chain Attacken, Kompromittierte Endpunkte, ...
- Herkömmliche Fernzugriffslösungen, z.B. VPNs, bieten eine direkte Verbindung zwischen potenziell nicht vertrauenswürdigen Endpunkten, kritischen Systemen und Infrastrukturen
- Ziel sollte es sein, gesicherte und verifizierte Identitäten mit Applikationen zu verbinden, und die Kontrolle über Daten und Zugriffe alleinig dem System Owner zu überlassen

Warum Remote PAM?

Gartner: „...reduce attack exposure and provide secure remote privileged access“

“RPAM tools improve administrative efficiency and reduce the security risks of poorly managed remote privileged access.

Security and risk management leaders responsible for identity and access management should deploy these tools to reduce attack exposure and provide secure remote privileged access.”

Securing Remote Privileged Access Management
Through RPAM Tools – December 2023

Gartner[®]

Warum Remote PAM?

Regulatorik, Normen und andere Treiber

KRITIS	NIS	CRA
IEC 62443	Insurance	ISO 27001
CIS Controls	EU 2023/1230	Kosten



Was ist IAM, ZTNA und SRA?

Identity (and Access) Management

Zentrale Systeme zur Erstellung, der Verwaltung und dem Schutz von Identitäten, und teilweise Zugriffen

Funktionen

1. Identitätsmanagement
2. Zugriff (Login)
3. Service (personalisierter Zugriff)
4. Federation (auth. ohne Passwort)
5. Audit

Zero Trust Network Access

Systeme, die logische Zugriffsgrenzen schaffen und Anwendungen vor der Entdeckung verbergen und den Zugriff auf eine Reihe von Entitäten beschränken

Prinzipien

1. Misstrauen
2. Minimale Rechte
3. Kontinuierliche Überprüfung
4. Mikrosegmentierung
5. Zero Trust Access

Secure Remote Access

Eigentlich Marketingbegriff, der Technologien und Methoden zur Erhöhung der Sicherheit von Fernzugriffen umfasst

Typische Funktionen

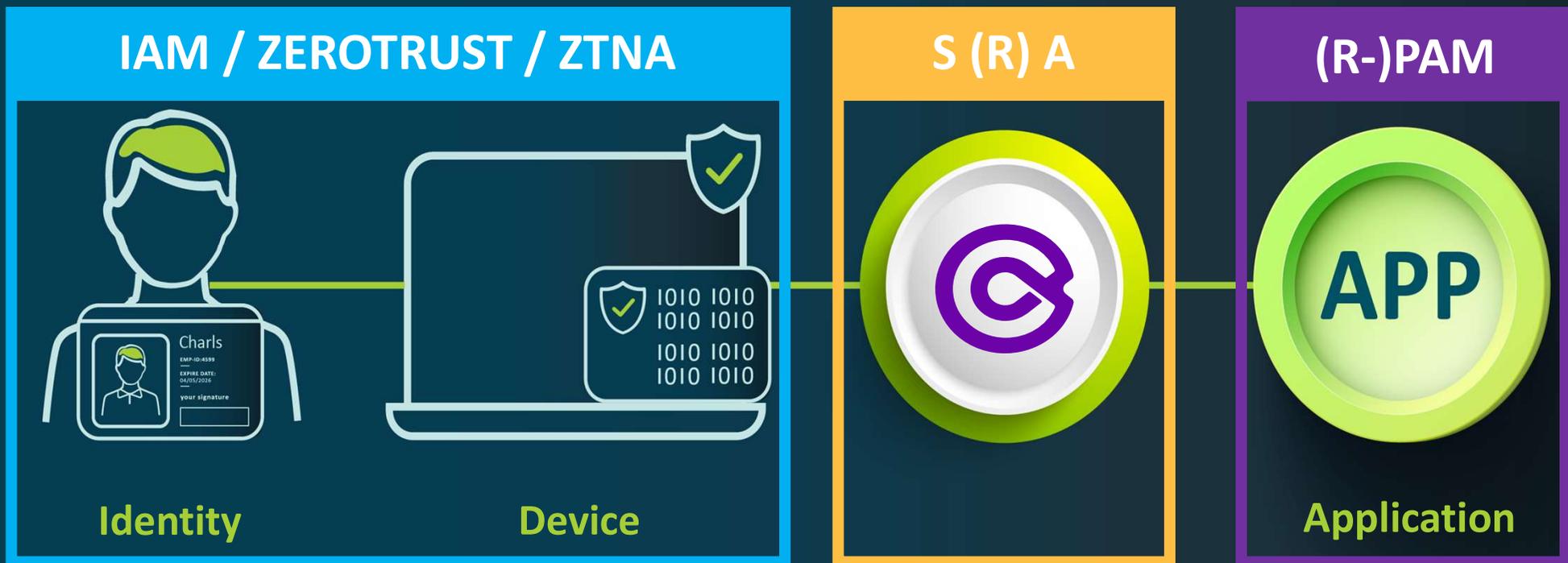
1. Reverse Connections
2. IAM Funktionen
3. Überprüfung von Devices
4. MFA
5. Monitoring und Auditing

Was zeichnet RPAM Lösungen aus?



Cyolo vereint das Beste aus 3 Welten

Praxis orientiert | einfache Installation & Betrieb | Bezahlbar



Wie setzt Cyolo RPAM um?

Zero Trust

Integrierter Vault
Application Security
Zero Trust für User
Access & Action Management

Identity

Internes IDP/SSO/MFA (auch legacy)
Device Zero Trust
Kontextbasiert (Gerät, Ort, Zeit, Security...)
Lokale Datenhaltung (keine Cloud)

SRA

Keine eingehenden Verbindungen
Ende-zu-Ende verschlüsselt
Geringe Latenz
Just-In-Time Access

Privileged

Session Audit & Recording
Supervised Access
Forensics
Lokales Approval



BearingPoint®

Together we are more than business

BearingPoint ist ein unabhängiges Management- und Technologieberatungsunternehmen mit europäischen Wurzeln und globaler Reichweite.

Wir unterhalten Niederlassungen an mehr als 40 Standorten und entwickeln mit 6.000 Mitarbeitern innovative Strategien für neue und bestehende Geschäftsmodelle und konzipieren und implementieren digitale Lösungen und Services für führende Unternehmen und öffentliche Institutionen.

Mit unseren Kompetenzen in den Bereichen Managementberatung, agile Transformation, technologiebasierte Business Services und smarte BearingPoint-Softwarelösungen setzen wir uns gemeinsam mit unseren Kunden und Partnern aktiv für messbaren und nachhaltigen Geschäftserfolg ein.

In Österreich unterstützen wir mit 350 Mitarbeitern führende Unternehmen und Organisationen. Das globale BearingPoint-Netzwerk mit mehr als 10.000 Mitarbeitern betreut Kunden in über 75 Ländern.



Alexander Schwemberger
BearingPoint AT
+43 664 88 31 85 03
alexander.schwemberger@bearingpoint.com

**Think digital.
Act agile.
Manage innovation.**

Cyolo

Privileged Remote Operations



Guido Erroi
Cyolo D-A-CH
+41 78 238 1212
guido@cyolo.io

cyolo.io