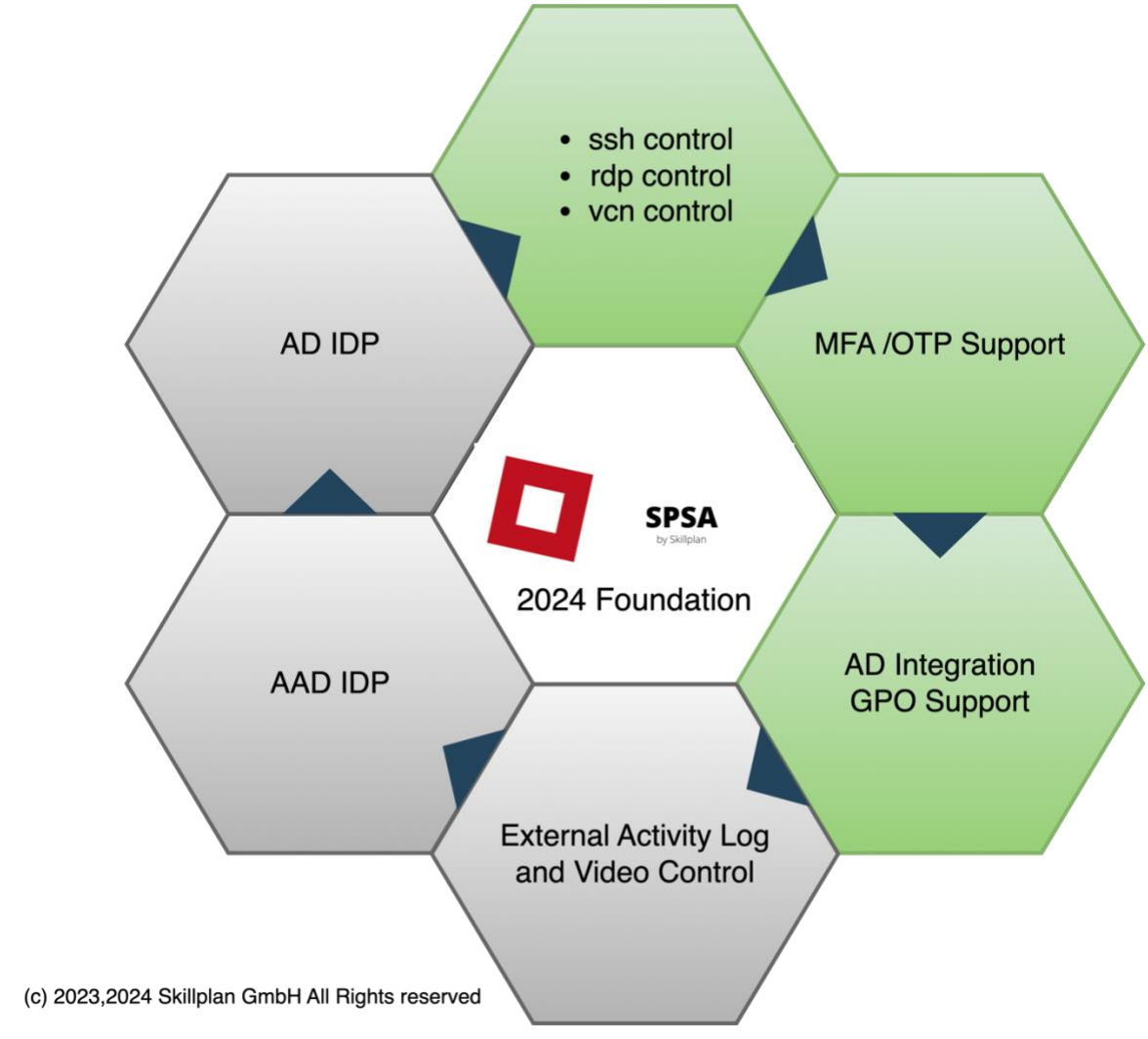
SPSA Foundation
Skillplan Secure Access

VERSION 02/2024

Überblick

SPSA die Zero Trust Access Lösung für RDP-Umgebungen, SSH-Zugriffe sowie zur Isolierung unsicherer Legacy Systeme via RDP oder VNC-Verbindungen.



Schnelle Umsetzung durch **On-Premises Lösungen "out of the box"**. SPSA kann rasch und kostengünstig als **virtuelle Appliance auf VMware ESX-i** installiert werden oder auch als **physikalische Appliance** auf einem dedizierten System. Ergänzt wird die Zero Trust Lösung durch eine **abgesicherte Patch-Infrastruktur** der Skillplan GmbH für **Appliance, Betriebssystem** und **SPSA**.

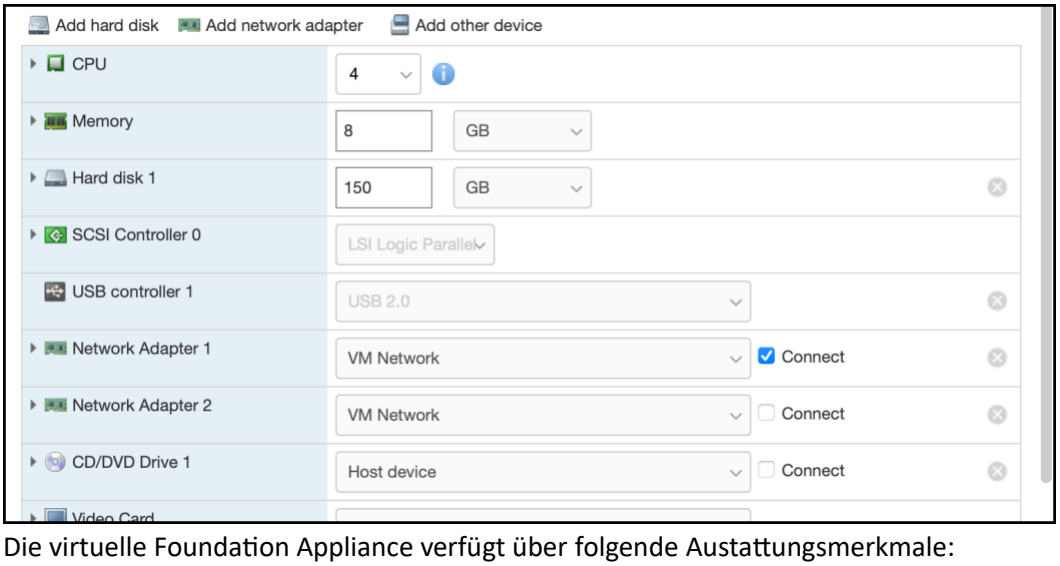
Physische Appliance (z Zt. Erhältlich in der Schweiz und in der EU)

Die Foundation Appliance verfügt über folgende Austattungsmerkmale:

- 4 Core CPU
- 32 GByte RAM
- 1 TB SSD
- 2 x NIC

Die Appliance unterstütz bis zu 25 Sessions gleichzeitig.

Virtuelle Appliance für VMWARE ab Version 7.0



Die virtuelle Foundation Appliance verfügt über folgende Austattungsmerkmale:

- 4 Core CPU
- 8 GByte RAM
- 150 GB Storage
- 2 x NIC

Die Appliance unterstütz bis zu 10 Sessions gleichzeitig.

Abkürzung	Bedeutung
rdp	Remote Desktop Protocol für Remote Zugriffe auf Windows Systeme
ssh	Secure Shell für remote Zugriffe auf Linux/Unix System, Appliances und Netzwerkkomponenten
SPSA Portal	User- und Administrations-portal der SPSA-Umgebung
SPSA-Proxy	Proxy Komponente zur Protokollumsetzung für SPSA

SPSA im Einsatz

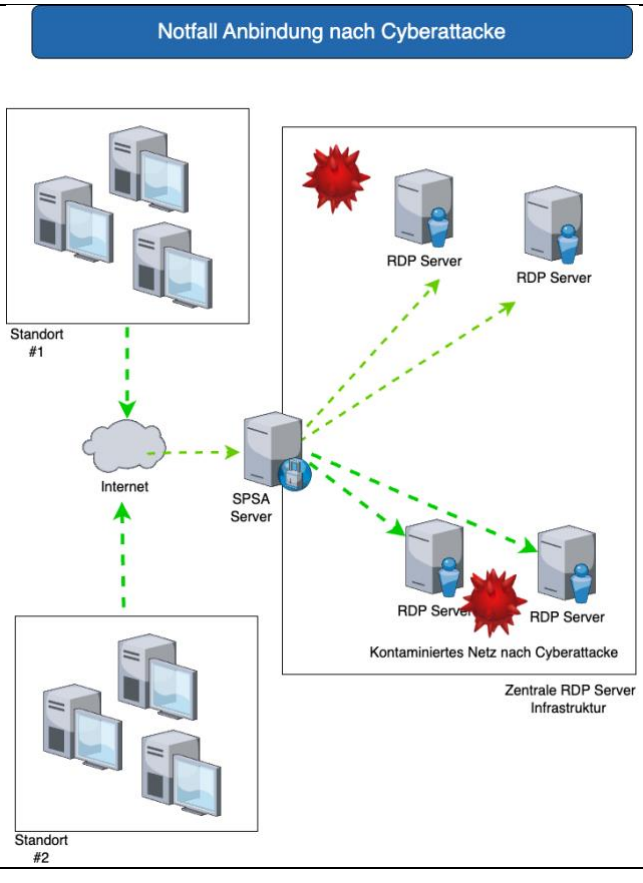
Zugriffe auf kompromittiertes Netzwerk nach einer Cyberattacke

Sie benötigen

Gesicherte Zugriffe auf kompromittierte Netzwerke aus einem "sicheren" Netzwerk. Die Zugriffe sollen ermöglicht werden, um die produktionsrelevante IT so früh wie möglich wieder einsetzen zu können. Beispiele, Produktionssteuerung oder ERP Systeme.

Die Lösung mit SPSA

SPSA ermöglicht Zugriffe auf Produktionssystem in kontaminierten Netzen, ohne den fort-laufenden Neuaufbau der IT-Infrastruktur des Unternehmens zu gefährden.



Gesicherter Zugriff auf Legacy Systeme

Sie benötigen

Den Betrieb isolierter Legacy Systeme auch bei bekannten Zero Day Lücken, ohne diese Systeme zu exponieren.

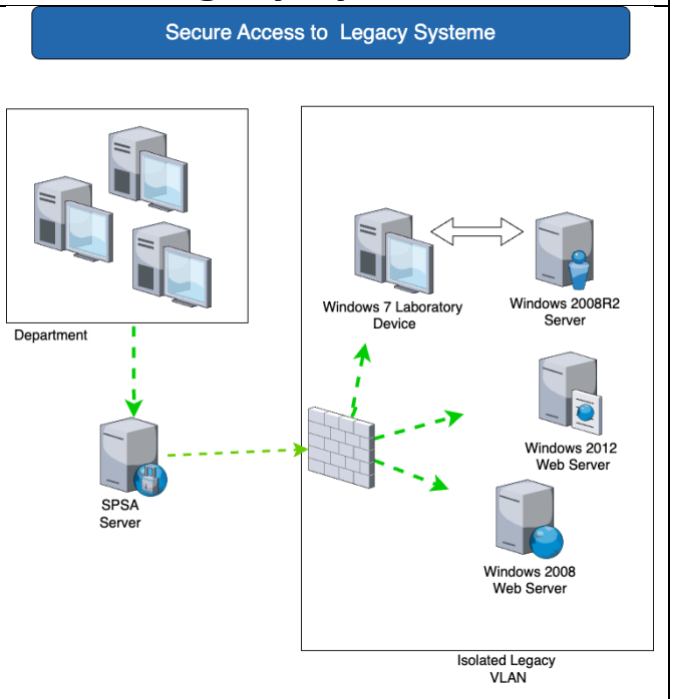
Risikominimierung bei nicht behebbaren Sicherheitslücken.

Die Lösung mit SPSA

Nicht mehr patchbare Systeme und Systeme mit bekannten Sicherheitslücken, können vom restlichen Netz isoliert und doch weiterhin zugegriffen werden, ohne das gesamte Netzwerk zu exponieren.

Funktionen, wie Cut & Paste oder Dateitransfer können auf System- und Userbasis granular geregelt werden bis hin zu einem reine Display Sharing ohne Zugriffe auf das System.

Beispiele sind: RDP-Verbindungen zu Windows Server 2008 Applikationen oder Windows 7 Applikation, die derzeit noch nicht ersetzt werden können.



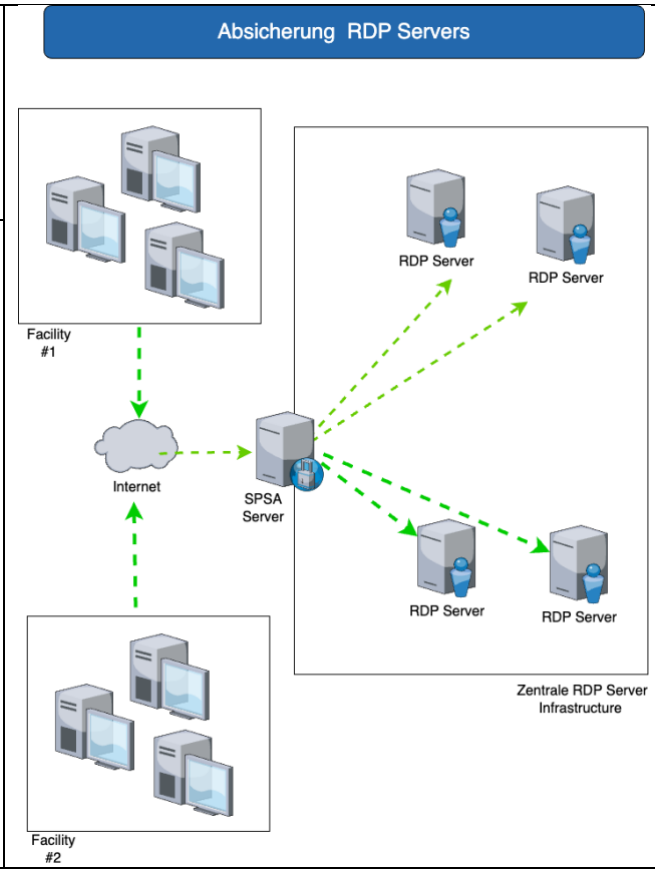
Absicherung von RDP-Servern

Sie benötigen

Die bestehenden RDP-Installationen sollen abgesichert werden, um das Risiko durch die Ausnutzung von RDP-Servern im Netzwerk zu minimieren.

Die Lösung mit SPSA

SPSA unterbindet „Lateral Movement“ durch ein zentrales Zugriffsportal für Server Zugriffe über RDP. Hiermit ermöglich SPSA die Bereitstellung abgesicherter Zugriffe auf RDP-Server für sowohl interne als auch für externe Zugriffe.



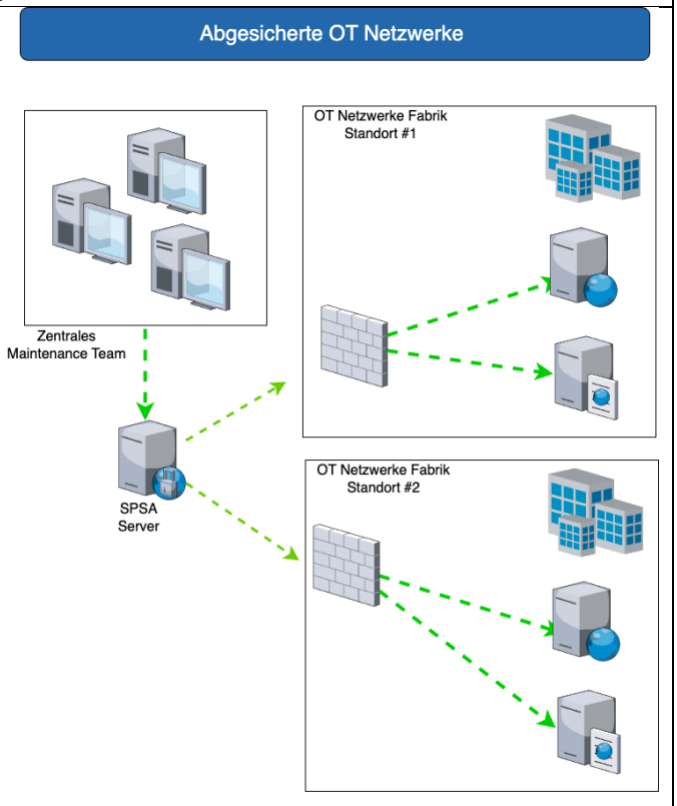
Zugriff auf segmentierte OT-Netze

Sie benötigen

Gesicherte Zugriffe bei Segmentierung von Produktionsnetzwerken, Labornetzten und OT-Netzwerken soll aus Office-Netzwerken ermöglicht werden (ohne die Segmentierung aufzuheben).

Die Lösung mit SPSA

Sollen OT und IT-Netzwerke voneinander getrennt betrieben werden (Microsegmentierung), so ermöglicht der Einsatz von SPA gesicherte Zugriffe aus dem IT-Netz auf Systeme in OT-Netzwerken über ein zentrales Zugriffsportal.



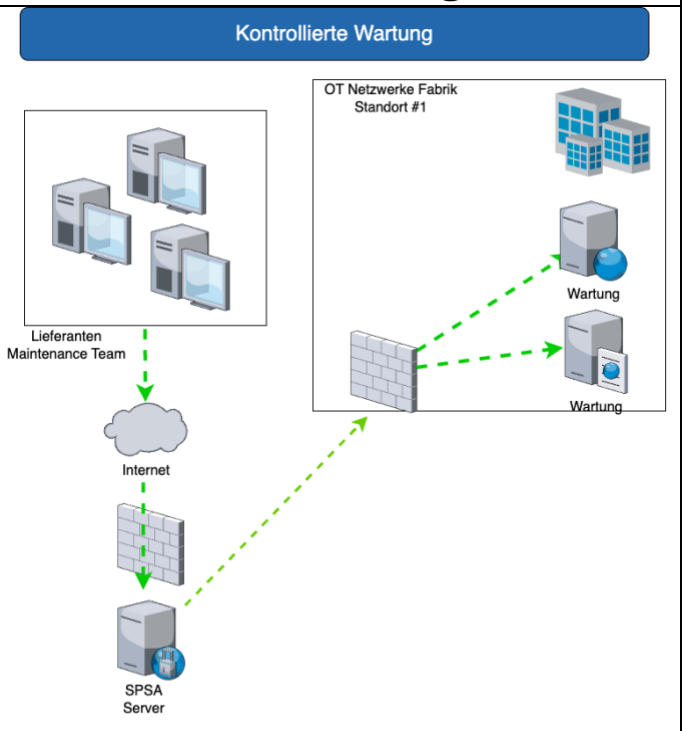
Kontrollierte Remote-Maintenance Zugriffe

Sie benötigen

Zu Wartungszwecken müssen Support Techniker über das Internet auf interne Systeme zugreifen können.
Hierbei werden RDP, ssh oder Telnet Verbindungen verwendet. Einzelne Mitarbeiter akquirierter Firmen sollen schnell über das Internet Zugriffe auf ausgewählte Systeme erhalten können, um den Integrationsprozess zu beschleunigen

Die Lösung mit SPSA

Ermöglicht zeitgesteuerte Zugriffe von Lieferanten auf Systeme zu Wartungszwecken ohne Installation von zusätzlicher Software bei den Lieferanten für Zugriffe über ssh, RDP und VNC. SPSA ermöglicht Managed Remote Maintenance Gateway für Lieferanten Zugriffe auf Serversysteme oder für Mitarbeiter von Firmen, die nicht im Firmen Netzwerk angeschlossen sind.



Zentrale Verwaltungs-Instanz zur Administration von MS Servern

Sie benötigen

Im Rahmen der Absicherung des Active Directories und unternehmenskritischer Applikationen auf MS Windows Basis, soll die Administration zentralisiert und abgesichert werden.

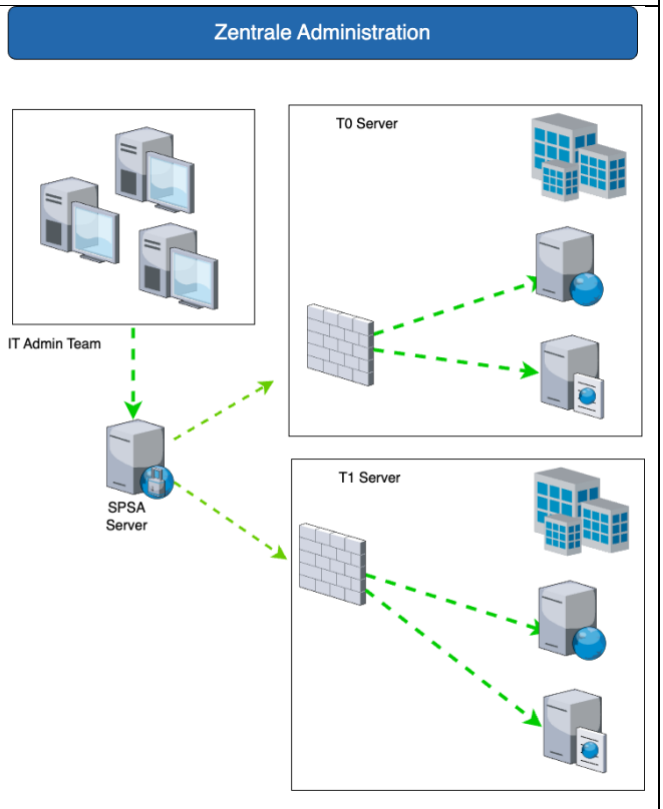
Darüber hinaus sollen Active Directories, die nach dem MS Tiering Modell gesichert sind, durch zentrale Administrationsportale zusätzlich abgesichert werden.

Die Lösung mit SPSA

Zur Absicherung administrativer Verbindungen bei der Verwaltung von Tier0, Tier1 und Tier2 Systeme bei Einführung des Microsoft Tiering Modells (zentrale Bereitstellung der PAW-Infrastruktur).

SPSA ermöglicht die zentrale Verwaltung von administrativen Zugriffen auf kritische Infrastruktur- Komponenten. Diese kann mit dem MS-Tiering Modell kombiniert werden.

Darüber hinaus ermöglicht SPA ein zentrales Logging privilegierter Zugriffe auf kritische Infrastruktur-Server via RDP oder ssh.



SPSA-Features

Sichere & bewährte Software

auf Basis von Apache Guacamole™

- Ein abgesichertes System mit Lowest Privileged Access
- Eine gesicherte Update- und Patching Infrastruktur, welche ihre Aplliance up-to-date hält
- Einfaches Admin Interfaces zur Verwaltung der Appliance
- Integrierte Möglichkeit Backups der kritischen Daten zu erstellen und auszulagern
- Integriertes Performance Monitoring mit der Möglichkeit die Monitoring Daten zur Auswertung zur Skillplan GmbH hochzuladen
- Unterstützung für RDP, SSH, telnet und VNC-Verbindungen
- Integrierte User Datenbank mit MFA-Support für Standard Authentication Apps wie Microsoft oder Google Authenticator
- Die Möglichkeit Benutzeranmeldungen zeitlich zu limitieren
- Active Directory Single Sign on (Pro Version)
- Azure Active Directory (SAML) Single Sign on
  mit Integration von Conditional Access (Pro Version)
- Portal mit bis zu 4 separaten SPSA Proxies an bis zu vier Standorten (Pro Version
- Aufzeichnung und Replay von RDP und SSH-Sessions via Videoaufzeichnung (Pro Version)

SPSA Next Steps

Sie hätten gerne eine SPSA-Vorstellung?
Dann wenden Sie sich bitte an sales@skill-plan.com zur Abstimmung eines Demo Termins.

Sie wollen SPSA während einer 30-tägigen Teststellung ausprobieren?
Dann wenden Sie sich bitte an sales@skill-plan.com zur Registrierung für eine Teststellung

Sie haben weitere Fragen und brauchen individuelle Antworten?

Beschreiben Sie uns Ihre Fragen an sales@skill-plan.com, damit wir einen Termin via Teams oder Zoom finden und vereinbaren können.