



Skillplan
GmbH

ZERO TRUST NETWORK ACCESS MIT SPSA



Skillplan Secure Access SPSA

Die **On-Premises-Lösung für Zero Trust Network Access mit rdp, ssh oder vnc.**

SPSA ermöglicht **Zero Trust Microsegmentierung**, erweiterte Zugriffskontrolle und **Unterstützung für Multi Faktor Authentisierung.**

Strikte Protokolltrennung erhöht zusätzlich die **Sicherheit vor "lateral movment"** Angriffen.

Versionen

SPSA Foundation

Die Basisversion für den schnellen Einsatz bei Ransomware Attacken bzw. für kleinere Umgebungen.

SPSA Pro

Die Komplettlösung für erhöhte Sicherheitsanforderung mit bis zu 4 zusätzlichen & eigenständigen Proxies.

Einsatzmöglichkeiten

- ✓ Disaster Recovery
- ✓ Remote Maintenance
- ✓ Microsegmentierung
- ✓ Legacy Isolierung
- ✓ PAM Lösung
- ✓ Ablösung JumpHosts



Appliance

Als Hardware Appliance oder VM für Hyper-V oder ESX.



MFA

MFA für lokale Appliance-Benutzer oder mit Active Directory-Integration erhöht die NIS2-Konformität.



Session-Protokolle

Unterstützt Zugriffe via rdp, ssh oder vnc. Je nach Protokoll auch für Altsysteme.



Europäisches Produkt

Keine Cloud-Daten, Patch-Infrastruktur aus EU-Rechenzentren (GDPR-konform).



Sitzungs-Aufzeichnungen (Pro)

NIS2-konforme Verwaltung privilegierter Sitzungen.



Externe IDPs (Pro)

Unterstützt EntraID oder Cisco DUO als Identityprovider zur User Authentisierung.

**Vertriebs-
partner EU**

just network services GmbH
sales@junese.de
+49 89 124 1386-50



Kleinmatt 5,
CH-6402 Merlischachen



<https://www.skill-plan.com>



info@skill-plan.com



Skillplan
GmbH

DISASTER RECOVERY MIT SPSA



Executive Summary

Skillplan Secure Access bietet eine leistungsstarke und sichere **Lösung für Disaster Recovery nach Cyberattacken**. Die Möglichkeit der **Installation ohne Internetzugang, die Absicherung von „roten“ Zonen und die schnelle Inbetriebnahme** machen SPSA zu einer essenziellen Komponente für widerstandsfähige IT-Umgebungen.

Herausforderung:

Cyberattacken wie Ransomware, Datenmanipulation und unautorisierte Zugriffe können Unternehmen innerhalb von Minuten lahmlegen.

In kritischen Situationen zählt jede Sekunde – eine schnelle, sichere Wiederherstellung ist essenziell, um Betriebsunterbrechungen zu minimieren. Doch herkömmliche Recovery-Prozesse sind oft zu langsam, zu komplex und auf Internetverbindungen angewiesen, die im Notfall nicht immer verfügbar sind.

Lösung:

Skillplan Secure Access (SPSA) bietet eine isolierte, hochsichere Umgebung für den schnellen und sicheren Systemzugriff – auch ohne Internetverbindung. Speziell entwickelt für den Schutz sensibler („roter“) Zonen, ermöglicht SPSA eine zuverlässige Wiederherstellung, selbst unter extremen Bedingungen.



Inbetriebnahme

- Sofortige Bereitstellung durch vorkonfigurierte Appliance oder VM.
- Ohne Internetzugang möglich.



Gesicherter Zugriffe

- Geschützte Recovery-Umgebung für kompromittierte IT-Systeme.
- Zugriffskontrolle mit Zero-Trust-Prinzipien zur Verhinderung erneuter Infektionen.



Messbare Ergebnisse

- Wiederherstellung betroffener Systeme in kürzester Zeit.
- Schutz vor erneuten Angriffen durch gesicherte Zugriffsmechanismen.



Kosteneinsparungen

Reduzierung des finanziellen Schadens durch schnelle Reaktionsfähigkeit.



Risikominimierung

- Schnelle Wiederherstellung kritischer Systeme durch sichere Backup-Zugänge.
- Verhinderung von Ausbreitungseffekten durch isolierte Recovery-Prozesse.





Skillplan
GmbH

REMOTE MAINTENANCE MIT SPSA

Executive Summary

Skillplan Secure Access (SPSA) bietet eine sichere und benutzerfreundliche Lösung für Remote Maintenance

Mit zeitgesteuerten Wartungsfenstern, vollständiger Protokollierung und MFA-geschützten Accounts wird ein höchstes Maß an Sicherheit und Kontrolle gewährleistet – ohne VPN-Client.

Herausforderung:

Unternehmen sind zunehmend auf **Fernwartung** angewiesen, um Systeme effizient zu warten und zu aktualisieren. Gleichzeitig stellen **ungesicherte Remote-Zugänge ein erhebliches Sicherheitsrisiko** dar. VPN-Lösungen sind oft umständlich, schwer zu verwalten und bieten keine feingranulare Kontrolle über externe Zugriffe.

Lösung:

Skillplan Secure Access (**SPSA**) ermöglicht eine **sichere, protokollierte und kontrollierte Remote Maintenance**, ohne dass ein VPN-Client erforderlich ist.

Mit **zeitgesteuerten Wartungsfenstern, MFA-geschützten Accounts und einem zentralen Zugriffspunkt** wird **höchste Sicherheit bei minimalem Verwaltungsaufwand** gewährleistet.



Aufzeichnung der Zugriffe

- Detaillierte Protokollierung aller Wartungssitzungen für vollständige Nachvollziehbarkeit.
- Schutz vor Missbrauch und unautorisierten Änderungen.



MFA

- Multi-Faktor-Authentifizierung für alle administrativen Remote-Zugänge.
- Schutz vor unbefugtem Zugriff und Account-Übernahmen.



Messbare Ergebnisse

- Sicherer, nachvollziehbarer Fernzugriff auf IT- und OT-Systeme.
- Reduktion von Fehlkonfigurationen und unkontrollierten Zugriffsversuchen.



Single point of control

- Zentrale Steuerung aller Remote-Zugriffe über eine gesicherte Plattform.
- Reduzierung der Angriffsfläche durch einheitliches Zugriffs-konzept.



Kein VPN-Client notwendig

Direkter, sicherer Zugriff ohne komplexe VPN-Infrastrukturen.





Skillplan
GmbH

ISOLIERUNG VON LEGACY-SYSTEMEN MIT SPSA

Executive Summary

Skillplan Secure Access ermöglicht eine **kontrollierte und sichere Isolierung von Legacy-Systemen**, die weiterhin betrieben werden müssen.

Die Zero-Trust-Architektur stellt sicher, dass nur **autorisierte Benutzer und Anwendungen Zugriff** erhalten, während **alle anderen Verbindungen blockiert oder überwacht werden**.

Herausforderung:

Legacy-Systeme, die nicht mehr gepatcht werden können, sind ein bevorzugtes Ziel für Cyberangriffe. Ungeschlossene Sicherheitslücken wirken wie ein Katalysator für Attacken und setzen Unternehmen hohen Risiken aus.

Lösung:

Skillplan Secure Access (SPSA) bietet eine **zentrale Sicherheitslösung für Legacy-Systeme durch Isolierung und Mikrosegmentierung**. SPSA verhindert direkte Netzwerkverbindungen zu anfälligen Systemen, minimiert so die Angriffsfläche erheblich und ermöglicht gleichzeitig einen **sicheren, effizienten administrativen Zugriff**.



Appliance

Als Hardware Appliance oder VM für Hyper-V oder ESX verfügbar.



Multi-Faktor-Authentifizierung (MFA)

MFA für lokale Appliance-Benutzer oder mit Active Directory-Integration zur Erhöhung der NIS2-Konformität.



Feine Steuerung des Datenflusses

- Regelbasierte Filterung von eingehenden und ausgehenden Verbindungen.
- Einschränkung des Datenverkehrs auf autorisierte Anwendungen und Benutzer.
- Vollständige Protokollierung aller Interaktionen mit dem Legacy-System.



Messbare Ergebnisse

- Sichere Weiterführung kritischer Legacy-Systeme trotz fehlender Sicherheitsupdates.
- Transparente Kontrolle über alle Zugriffe und Datenflüsse.



Kosteneinsparungen

- Kein überhasteter Ersatz alter Systeme erforderlich.
- Reduzierung der Risiken und Kosten durch mögliche Cyberangriffe.



Risikominimierung

- Eliminierung direkter Netzwerkverbindungen zu Legacy-Systemen.
- Schutz vor Malware und Ransomware durch isolierte Zugriffsmechanismen.





Skillplan
GmbH

JUMP HOST ERSATZ MIT SPSA



Executive Summary

Skillplan Secure Access bietet eine moderne und effiziente Alternative zu klassischen Jumphosts.

Durch **Zero-Trust Network Access (ZTNA)**, **zentrale Steuerung** und eine **vereinfachte Topologie** ermöglicht SPSA eine **sichere, kosteneffiziente** und leicht verwaltbare **Lösung** für den **Schutz privilegierter Zugriffe**.

Herausforderung:

Jumphosts sind eine etablierte Methode zur Absicherung administrativer Zugriffe, doch sie bringen hohe Kosten, komplexe Infrastrukturen und Sicherheitsrisiken mit sich. Sie benötigen kontinuierliche Wartung, erfordern zusätzliche Lizenzen und bieten oft keine granulare Zugriffskontrolle. Eine moderne, effiziente Alternative ist notwendig.

Lösung :

Skillplan Secure Access (**SPSA**) ersetzt **klassische Jumphosts durch eine Zero-Trust Network Access (ZTNA)-Lösung**.

Dadurch wird die Topologie vereinfacht, die Verwaltung zentralisiert und Lizenzkosten reduziert, während gleichzeitig ein höchstes Maß an Sicherheit und Kontrolle gewährleistet wird.



Vereinfachte Topologie

- Keine separate Jumphost-Infrastruktur erforderlich.
- Reduzierung der Angriffsfläche durch eine schlanke, moderne Architektur.



Single Point of Control

- Zentrale Steuerung aller Zugriffe.
- Detaillierte Zugriffskontrolle mit vollständiger Protokollierung.



Messbare Ergebnisse

- Reduzierung der Komplexität und des Verwaltungsaufwands.
- Erhöhung der Sicherheit durch Zero-Trust-Architektur.



Kosteneinsparungen

- Eliminierung von Lizenzkosten und Administrationsaufwand für Jumphosts.
- Effizientere Nutzung bestehender IT-Ressourcen.



Risikominimierung

- Reduzierung des RDP-Verkehrs auf ein Minimum.
- Granulare Steuerung der Zugriffe auf Endsysteme.





Skillplan
GmbH

RDP-ABSICHERUNG MIT SPSA



Executive Summary

Skillplan Secure Access (SPSA) ermöglicht eine sichere, zentralisierte Verwaltung privilegierter RDP-Zugriffe mit Zero-Trust-Architektur. Die Lösung ist speziell für mittelständische Unternehmen entwickelt und unterstützt die Erfüllung aktueller Compliance-Anforderungen.

Herausforderung:

Remote-Desktop-Protokoll (RDP) ist ein bevorzugtes Ziel für Cyberangriffe. Offene RDP-Zugänge erhöhen das Risiko von Ransomware-Attacken und unautorisierten Zugriffen. Traditionelle Sicherheitslösungen sind oft zu komplex um schnell auf Bedrohungen zu reagieren.

Lösung:

Skillplan Secure Access (SPSA) bietet eine zentrale Sicherheitslösung für RDP-Server durch Isolierung und Mikrosegmentierung.

Die Lösung verhindert direkte Netzwerkverbindungen zu RDP-Servern und reduziert so die Angriffsfläche erheblich, während der administrative Zugriff sicher und effizient bleibt.



Appliance

Als Hardware Appliance oder VM für Hyper-V oder ESX verfügbar.



MFA

- MFA für lokale Appliance-Benutzer oder
- mit Active Directory-Integration zur Erhöhung der NIS2-Konformität.



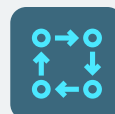
Messbare Ergebnisse

Vollständige Transparenz aller administrativen RDP-Zugriffe.



Kosteneinsparungen

- Wegfall separater Admin-Arbeitsplätze.
- Reduzierter Verwaltungsaufwand.
- Erhöhung des Sicherheitsniveaus.



Risikominimierung

- Erhöhter Schutz vor Ransomware-Angriffen durch isolierte RDP-Systeme.
- Minimierung von Ausfallzeiten durch schnelle Reaktionsfähigkeit.





Skillplan
GmbH

ACTIVE DIRECTORY ABSICHERUNG MIT SPSA



Executive Summary

SPSA bietet eine **effiziente Absicherung von Active Directory-Umgebungen** durch die Implementierung eines **Zero-Trust-Zugangsmodells für administrative Zugriffe**.

Die Lösung ist **speziell auf die Bedürfnisse mittelständischer Unternehmen zugeschnitten** und **ermöglicht eine zentrale, sichere Verwaltung privilegierter Zugriffe** bei gleichzeitig **überschaubarem Implementierungsaufwand**.

Herausforderung:

Auch kleinere Active Directory-Umgebungen sind zunehmend Ziel von Cyberangriffen, wobei besonders administrative Zugänge im Fokus stehen. Traditionelle Sicherheitslösungen sind oft zu komplex und kostenintensiv für mittelständische Unternehmen.

Lösung:

SPSA stellt ein zentrales Zugangsportal bereit, das administrative Zugriffe effektiv absichert und überwacht, ohne dabei die gewohnten Arbeitsabläufe zu beeinträchtigen.

- ✓ **Sofortige Erhöhung des Sicherheitsniveaus durch Zero-Trust-Architektur**
- ✓ **Vereinfachte Verwaltung privilegierter Zugriffe**
- ✓ **Unterstützung bei der Erfüllung aktueller Compliance-Anforderungen**



Appliance

Als Hardware Appliance oder VM für Hyper-V oder ESX.



MFA

MFA für lokale Appliance-Benutzer oder mit Active Directory-Integration erhöht die NIS2-Konformität.



Messbare Ergebnisse

Vollständige Transparenz aller administrativen Zugriffe.



Kosteneinsparungen

- Wegfall separater Admin-Arbeitsplätze.
- Reduzierter Verwaltungsaufwand.
- Erhöhung Sicherheitsniveau.



Risikominimierung

- Erhöhter Schutz vor Ransomware-Angriffen durch isolierte Zugriffe.
- Minimierung von Ausfallzeiten durch schnelle Reaktionsfähigkeit.



Kleinmatt 5,
CH-6402 Merlischachen



<https://www.skill-plan.com>



info@skill-plan.com