FUJITSU

shaping tomorrow with you

Produkte im Umfeld der “Digitalen Souveränität”

FUJITSU Security Solution SURIENT

FUJITSU World Tour

10.05.2016 Congress Center Düsseldorf

Digitalisierte Welt benötigt hohe IT-Sicherheit

FUJITSU

Unsere vernetzte Welt, in der wir leben

Services, die dies ermöglichen bzw. erleichtern

Infrastrukturen auf denen dies basiert

Alles dreht sich um Daten (erfassen, speichern, auswerten)
Wo bleibt die IT-Sicherheit?

Fujitsu IT Security – 40 Jahre Erfahrung in Europa

Managed Security Services	Konsultierend und Unterstützend	Produkte

350+ Security Experten

Security Operations Centres arbeiten nach den höchsten nationalen Standards

F&E Möglichkeiten – Entwicklung/Integration Fujitsu Security Produkte, wie PalmSecure und SURIENT

Betrieb in öffentlichen und privaten Bereichen, und der Landesverteidigung

Nach den höchsten Standards ausgewählte Technologie Partner und Zertifizierungen

40+ Jahre Geschichte in Design, Integration Auslieferung von umfangreichen Cyber Security Services

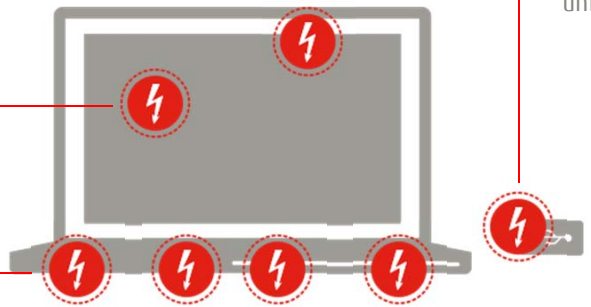
shaping tomorrow with you

Angriffspunkte gibt es reichlich
Endpunkt – Übertragung - Rechenzentrum

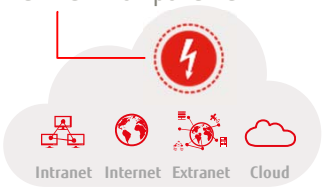
Webcam und Mikrofon (intern/extern)
können aktiviert und gesteuert werden (Raumüberwachung möglich)

Bildschirminhalte
können mitgelesen werden

Externe HDD, USB
können Viren und Backdoors unbemerkt installieren

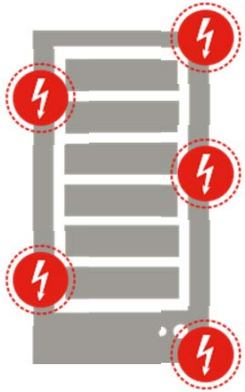


Kommunikation (Internet/LAN/WAN)
Backdoors in aktiven / passiven Netzwerk-Komponenten



Remote Zugriff
Übernahme und Steuerung der Systeme durch Fernzugriff

Zugriff auf kritische Daten
Admins können auf sensible Daten unbemerkt zugreifen



Daten werden abgefangen
Ausgehende Daten können abgefangen, mitgelesen und manipuliert werden

Hackerangriffe
Durch nicht durchgängiges Monitoring werden Hackerangriffe erleichtert; Logs können verfälscht werden

Hauptspeicher
speichert Daten unverschlüsselt

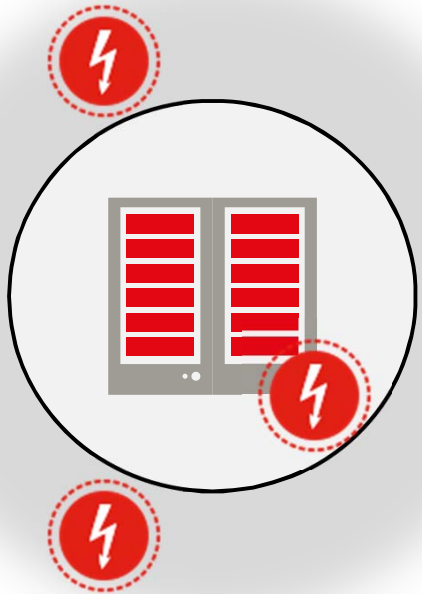
Maus- und Tastatureingaben
können mitgelesen werden

BIOS, OS, Treiber, Anwendung
Können Backdoors enthalten

Interne Datenträger (HDD, SSD, DVD)
sind trotz Verschlüsselung lesbar

Physikalischer Zugriff
auf Systeme durch unzureichend gesicherte Zugriffsprozesse

SURIENT – wenn es sicherer sein soll



- Angriffe kommen von außen und innen, deshalb:
  - Keine Angriffsfläche bieten (offene Ports, Zero Days)
  - Kapselung der Aufgaben und Anwendungen
  - Erzwungene Prozesse und n-Augen-Prinzip
  - Keine isolierten Zuständigkeiten
  - Verwendung anerkannter Methoden on offener SW
  - Keine “Security through Obscurity”

Probleme kann man niemals mit der gleichen Denkweise lösen, durch die sie entstanden sind.

Albert Einstein

Ende-zu-Ende Sicherheit
Endgerät – Übertragung – Rechenzentrum

Endgerät

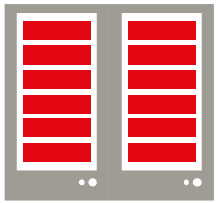
SURIENT Sealed Application Solution

- Sicherheitsoptimierte Endgeräte
- Gekapselte Anwendungen
- Permanente Überwachung des Sicherheitslevels
- Biometrische Authentifizierung mit PalmSecure

Übertragung

SURIENT Stealth Connect Solution

- Sichere und verschlüsselte VPN-Kommunikation mit einem Rechenzentrum
- VPN-Server ist nach außen nicht sichtbar (Stealth-Technologie)
- Verfügbar als Appliance und Software-Client



Rechenzentrum

SURIENT Managed Rack Solution

- Erhöhter Schutz der Server vor physischem Zugriff
- Biometrische Zugriffs-Autorisierung mit PalmSecure ID Match

SURIENT Sealed Rack Solution

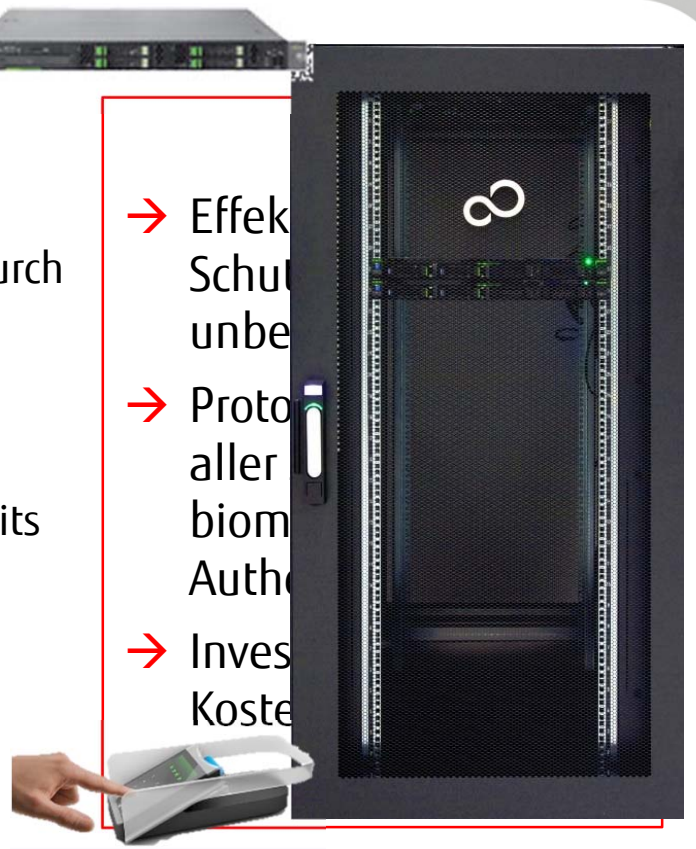
- Best-in-Class Schutz vor physischem Zugriff und Schutz vor elektronischen Angriffen

SURIENT Encrypted Boot Solution

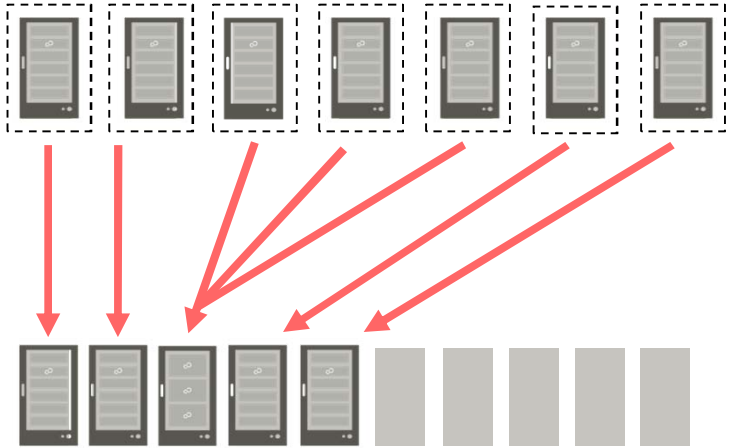
- Automatisches Booten von Servern mit verschlüsselten Platten

SURIENT Managed Rack Solution (MRS)

- Leicht integrierbare 19" Racks mit elektromechanischen Schlössern und Sensoren
- Durchgängiges Berechtigungskonzept für Racks und Cages
- Verhinderung der Weitergabe von Berechtigungen an Dritte durch biometrischen Methoden.
- Optionale Bestätigung des Zugriffs durch einen zweiten Berechtigten - auch von unterschiedlichen Orten aus
- Protokollierung aller Zugriffe und Zugriffsversuche z.B. für Audits
- Sorgenfreie Rundumlösung: Setup, Installation und Training werden an einem Tag beim Kunden vor Ort durchgeführt
- Kostenersparnis durch stark erhöhte Flexibilität und weniger Platzbedarf verglichen mit Einzäunungen

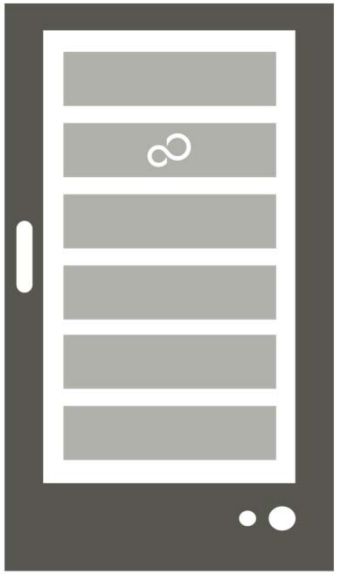


Caging im Rechenzentrum - ohne Zäune



Racks sind physisch durch Zäune gesichert

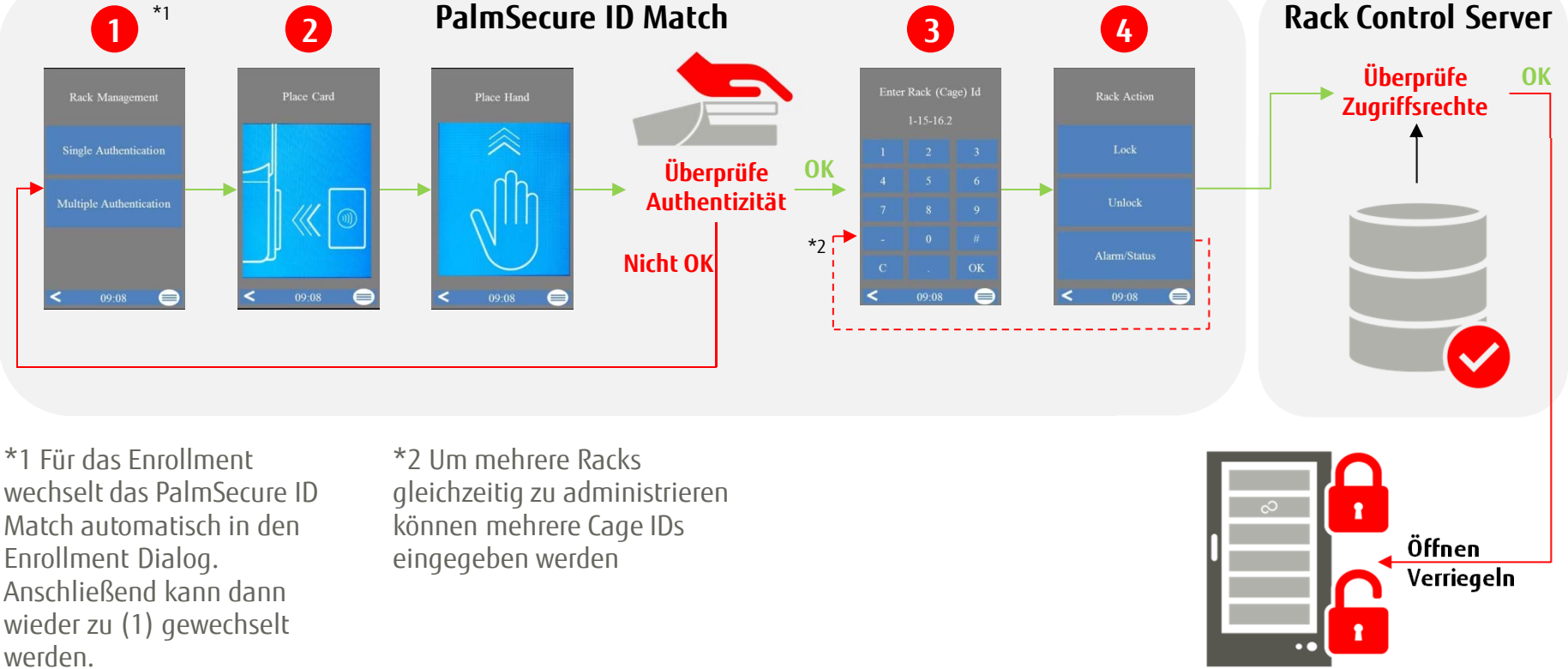
Racks sind durch SURIENT MRS gesichert



Vorteile:

- Geringer Platzbedarf und damit niedrigere Kosten
- Reduzierte Sicherheitsrisiken

Ablauf Öffnen/Verriegeln eines Racks



*1 Für das Enrollment wechselt das PalmSecure ID Match automatisch in den Enrollment Dialog. Anschließend kann dann wieder zu (1) gewechselt werden.

*2 Um mehrere Racks gleichzeitig zu administrieren können mehrere Cage IDs eingegeben werden

Biometrische Sicherheit mit PalmSecure supersicher und gleichzeitig benutzerfreundlich

Methode	FAR (%)	bei FRR (%)
Gesicht	~ 1.3	~ 2.6
Stimmmuster	~ 0.01	~ 0.3
Fingerabdruck	~ 0.001	~ 0.1
Fingervene	~ 0.0001	~ 0.01
Iris/Retina	~ 0.0001	~ 0.01
Fujitsu Palm Vein	**< 0.00008**	**~ 0.01**

FAR: False Acceptance Rate
FRR: False Rejection Rate

LIFEBOOK U904
Ultrabook
PalmSecure™

CELSIUS H730
Workstation
PalmSecure™

LIFEBOOK U745
Notebook
PalmSecure™

LIFEBOOK S936
Notebook
PalmSecure™

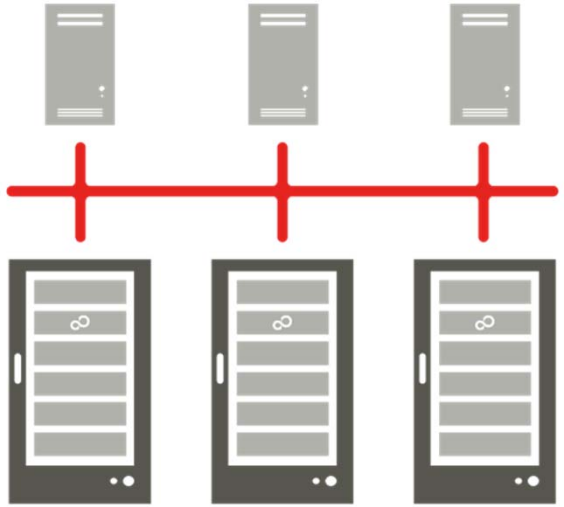
STYLISTIC Q775
Tablet
PalmSecure™

ESPRIMO Q956
Desktop
PalmSecure™

New!
From Q2/2016

SURIENT Encrypted Boot Solution (EBS)
Sichere Server sicher booten

- Schutz vor unerlaubtem Zugriff
  - Booten von vollverschlüsselten Servern ohne Benutzer- bzw. Admin-Interaktion
  - Hochsichere Boot-Server ohne offene Ports
  - Sichere Übertragung von verschlüsselten Geheimnissen
  - Passwort sicher im Tresor und sonst nirgendwo gespeichert
- Schutz vor Ausfällen oder Störungen
  - Hochverfügbare Boot-Server
- Schutz vor Manipulation
  - Automatische Integritätsprüfung der Hardware und Software
  - Kein “Single-point-of-attack” durch verteilte Boot-Server

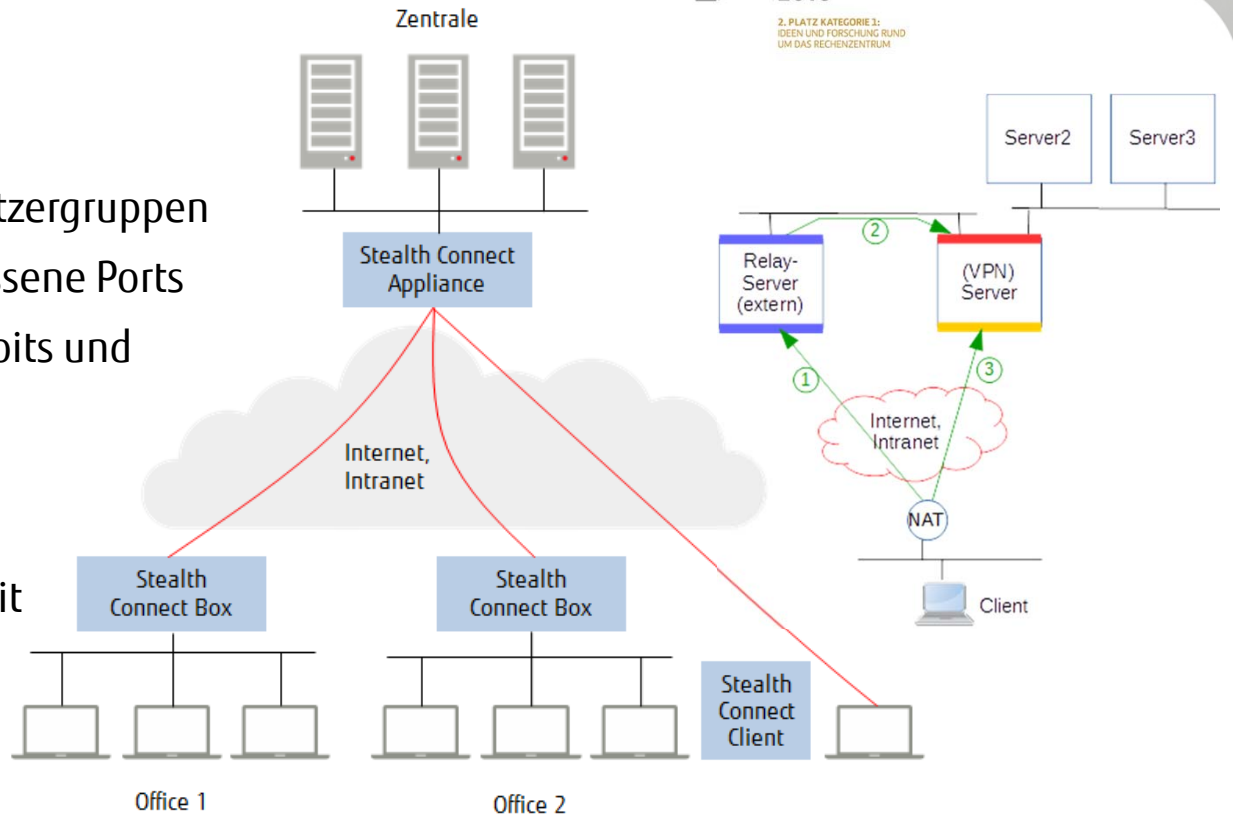


SURIENT Stealth Connect Solution (SCS)

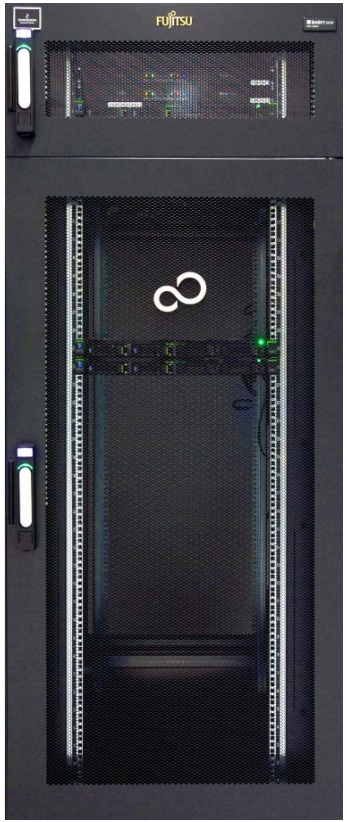
DEUTSCHER RECHENZENTRUMSPREIS 2016
2. PLATZ KATEGORIE 1: IDEEN UND FORSCHUNG RUND UM DAS RECHENZENTRUM

FUJITSU

- Sichere VPN-Kommunikation mit einem Rechenzentrum
  - Nutzbar für geschlossene Nutzergruppen
  - Angreifer sehen nur geschlossene Ports
  - Schützt gegen Zero Day Exploits und Man-in-the-Middle-Angriffe
- Optionen
  - Unterstützt Hochverfügbarkeit und Lastverteilung



Höchster Schutz durch SURIENT Sealed Rack Solution (SRS)



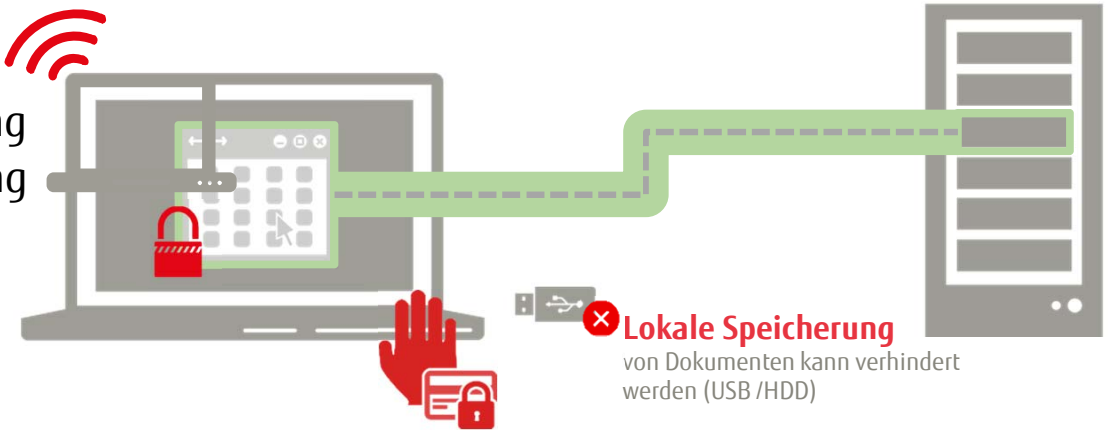
Kontroll-einheit 7HE

Server, etc. 34 HE

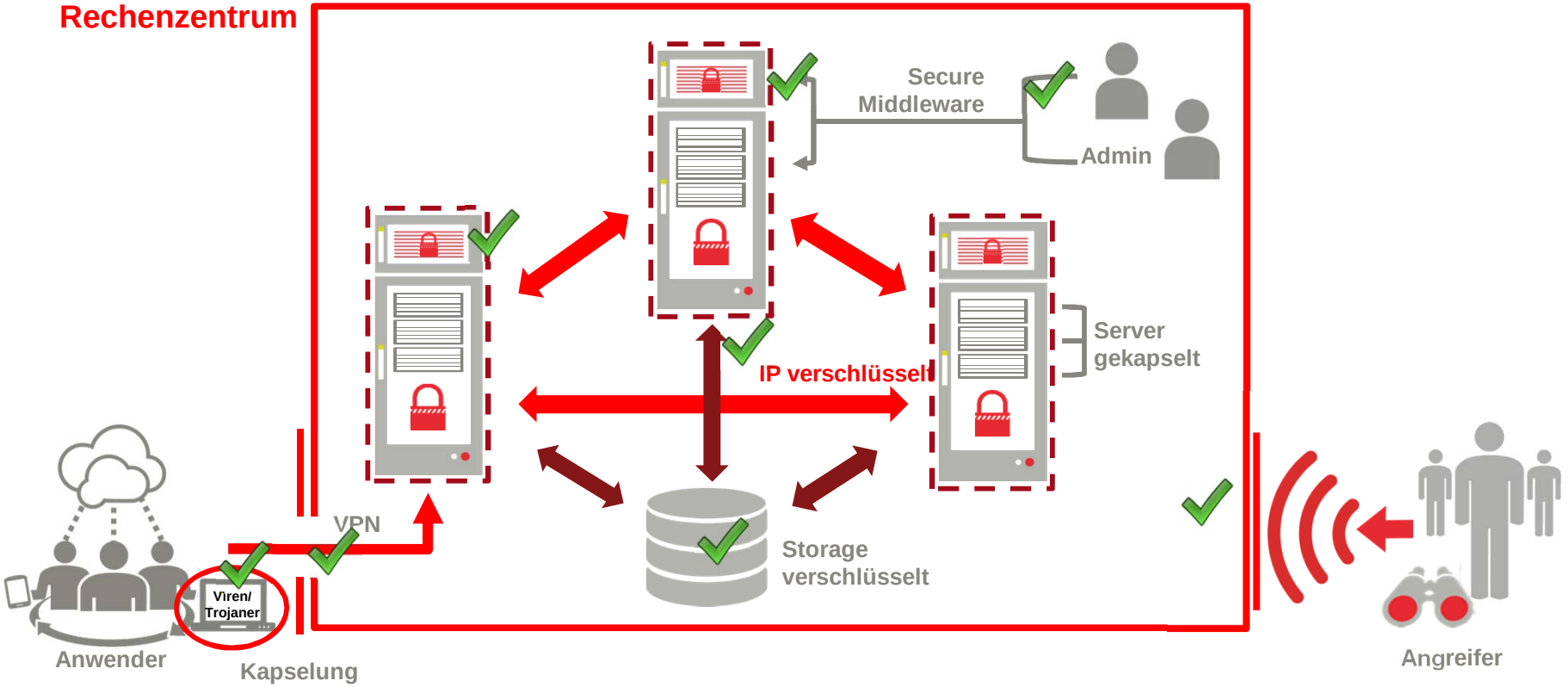
- Schutz vor physischem Zugriff
  - Verstärkte Hardware Cages („Server Safes“)
  - Biometrische Zugriffskontrolle per Handvenenscan
  - Ständige Überwachung durch Tür- und Schock-Sensoren
  - USV zum gepufferten Betrieb der Kontrolleinheit (ca. 2h)
  - Durchgriffssichere Mechanik
  - Vollständige Trennung der Kontrolleinheit und Nutzbereich
- Schutz vor elektronischen Angriffen
  - Keine offenen Ports nach Außen und somit keine erreichbaren Dienste („Stealth Data Center“)
  - Ende-zu-Ende-Verschlüsselung
- Investitionsschutz
  - Bereits vorhandene IT-Infrastruktur kann weiter im Sicherheitsrack verwendet werden

SURIENT Sealed Application Solution (SAS)

- Durchgängiger Ansatz, um Windows Client Produkte mit einer verbesserten Geräte- und hohen Ende-zu-Ende-Sicherheit zu liefern
- Starke und doppelte Verschlüsselung (TwoFish) für die Remote-Verbindung zwischen Client und Server-Anwendung mit Überwachung des Sicherheitskanals
- Verwendung speziell ausgestatteter und konfigurierter Clients



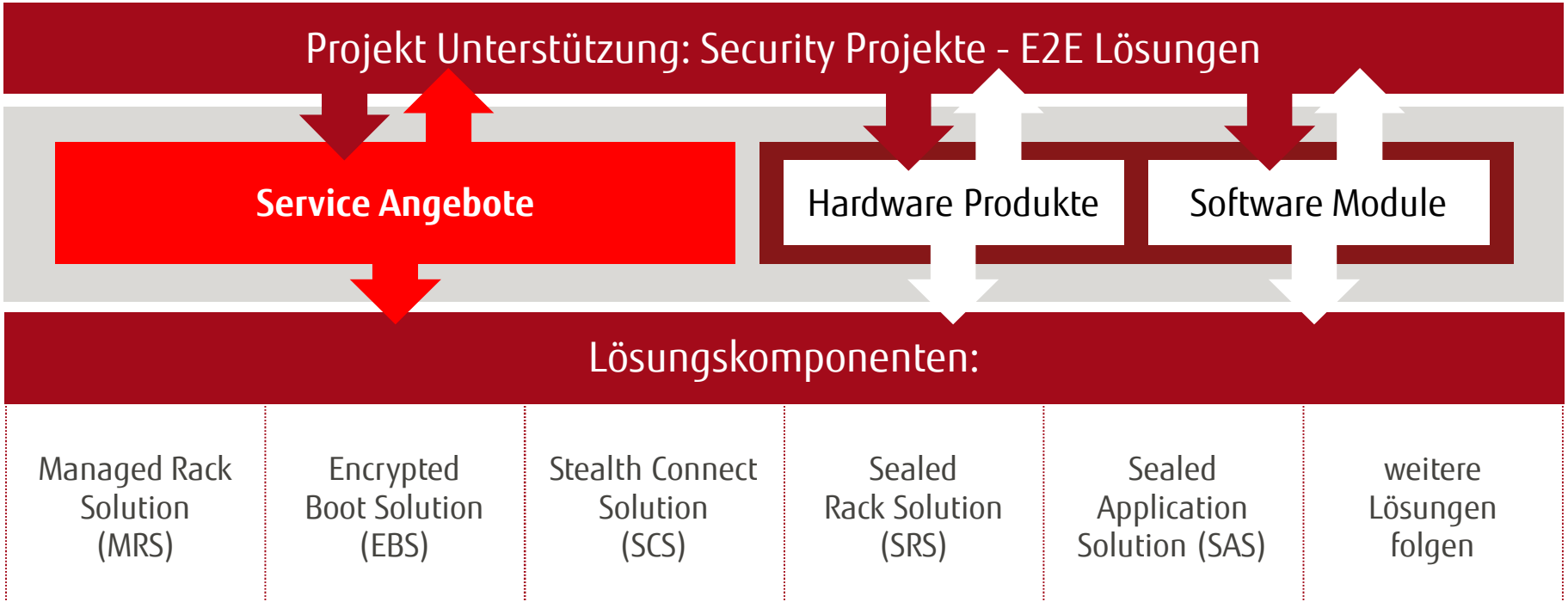
Stealth Data Center
So könnte am Ende ihr RZ abgesichert sein



Merkmale von Fujitsu SURIENT

- Stark erhöhte IT Sicherheit selbst gegenüber Zero Day Exploits
- Transparente und benutzerfreundliche Ende-zu-Ende Sicherheit vom Endgerät bis zum Rechenzentrum
- Hoher Investitionsschutz durch Verwendung vorhandener Infrastruktur
- Umfassender IT-Sicherheitsansatz durch neuartige technische und organisatorische Maßnahmen
- Modularer Aufbau der Lösungen - Module können einzeln oder kombiniert eingesetzt werden
- Mit vorhandenen Lösungsbausteinen können kundenspezifische Lösungen erstellt werden

Projektlösungen und Lösungskomponenten
Kombiniertes Angebot: Services, HW und SW Module



Wie ist der Weg zu einer projektbasierten Lösung?

FUJITSU

1. Durchführen von Schwachstellen-/Risikoanalyse (optional)
2. Identifizierung der gewünschten Lösungsmöglichkeiten
3. Erarbeiten einer kundenspezifischen E2E Lösung
4. Prototypisierung
5. Testbetrieb
6. Finalisierung und Übergabe
7. Pflege und Betrieb durch den Kunden oder Fujitsu

Informationen & Kontakt

Kontakt

Thomas Schkoda (Produkt Manager)
➔ thomas.schkoda@ts.fujitsu.com

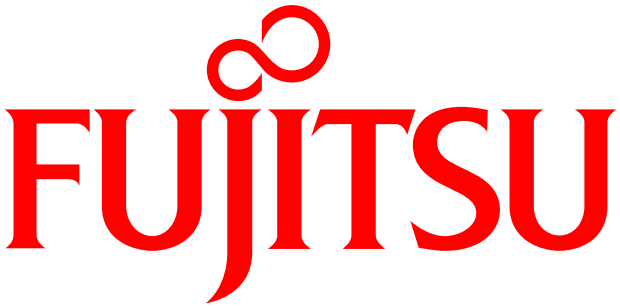
Harry Schäfle
➔ harry.schaefle@ts.fujitsu.com

Mailbox:
➔ SURIENT@ts.fujitsu.com

Informationen

Internet

➔ http://www.fujitsu.com/de/solutions/business-technology/security/surient/



shaping tomorrow with you

Reduktion der Angriffsflächen mit „Stealth“
Port Knocking++