CYBER-ATTACKEN MACHEN DIE NETZWERKSICHERHEIT ZUR HERAUSFORDERUNG

IoT/OT-Security – damit Cyber-Attacken keine Chance haben

InfoGuard
SWISS CYBER SECURITY

AKTUELLE BEDROHUNGSLAGE SCHWEIZ

Inside IT

Schoggifabrikant Läderach von Ransomware-Attacke ...

Die Produktion, Logistik und Administration des Chocolatiers sollen vom Cyberangriff betroffen sein. Der Verkauf in den Filialen funktioniert...

06.09.2022

Watson

Autohändler Emil Frey ist von Cyberattacke betroffen: Website offline

Die Emil-Frey-Gruppe ist das neuste Opfer einer Cyberattacke. Laut dem Schweizer Unternehmen mit rund 22'000 Angestellten sind mehrere...

12.01.2022

Inside Paradeplatz

V-Zug wehrt Cyber-Attacke ab

V-Zug wehrt Cyber-Attacke ab ... Vor Jahresfrist war bereits mit der Stadler Rail von Unternehmer Peter Spuhler ein Betrieb aus dem...

28.07.2021

Inside IT

Ransomware-Angriff auf die Brugg Group betrifft weltweite ...

September 2020, wurde bei der Brugg Group eine Cyberattacke festgestellt. Dabei hätten die Täter vereinzelt Daten auf einigen IT-Systemen...

17.09.2020

Luzerner Zeitung

Nach Cyberattacke bei CPH-Gruppe: Papiermaschinen stehen still

Es bleibt unklar, was genau in der Nacht auf den 7. Januar am Hauptsitz der börsenkotierten CPH-Gruppe in Perlen passiert ist.

Luzerner Zeitung

Cyber-Attacke: Comparis wird von Hackern erpresst

Der grösste Vergleichsdienst der Schweiz ist Opfer einer Attacke von kriminellen Cyber-Hackern geworden. Lösegeld will das Unternehmen keines...

08.07.2021

Aargauer Zeitung

Siegfried Zofingen: Cyber-Attacke hat Folgen für Mitarbeiter

Der Cyber-Angriff auf das IT-Netzwerk des Pharma-Unternehmens Siegfried Gruppe mit Hauptsitz in Zofingen hat Folgen für die Mitarbeiter. 15.06.

15.06.2021

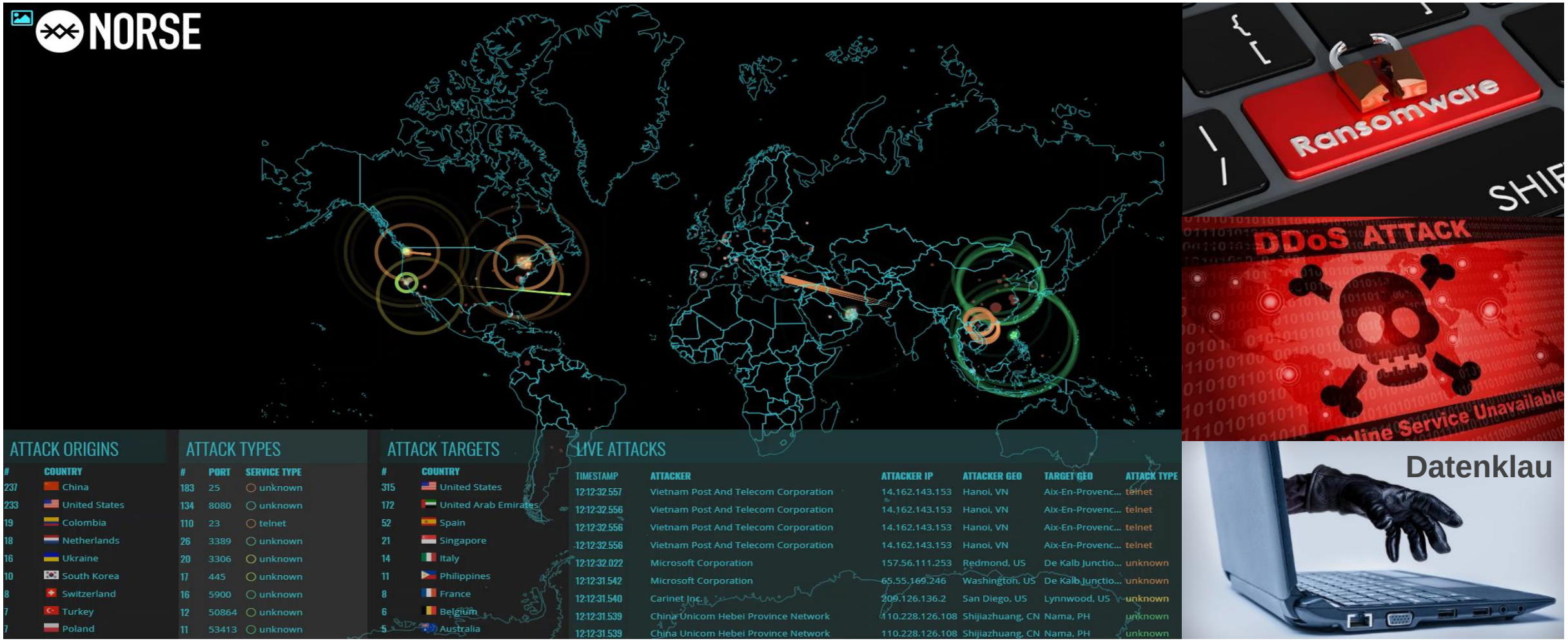
St. Galler Tagblatt

Lösegeld - Nach Cyber-Angriff: Erpresser erhöhen Druck auf Peter Spuhlers Stadler Rail

Nach Cyber-Angriff: Erpresser erhöhen Druck auf Peter Spuhlers Stadler Rail. Die Cyberkriminellen, die Anfang Mai ins IT-Netzwerk des...

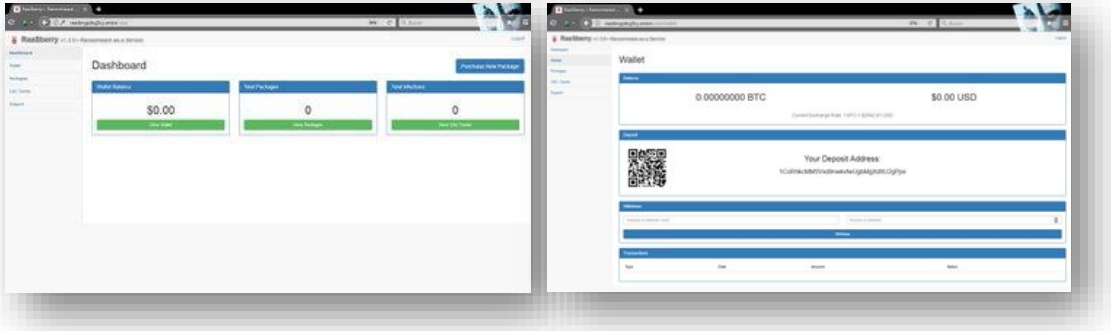
06.07.2020

CYBER KRIMINALITÄT ALS TOP RISIKO



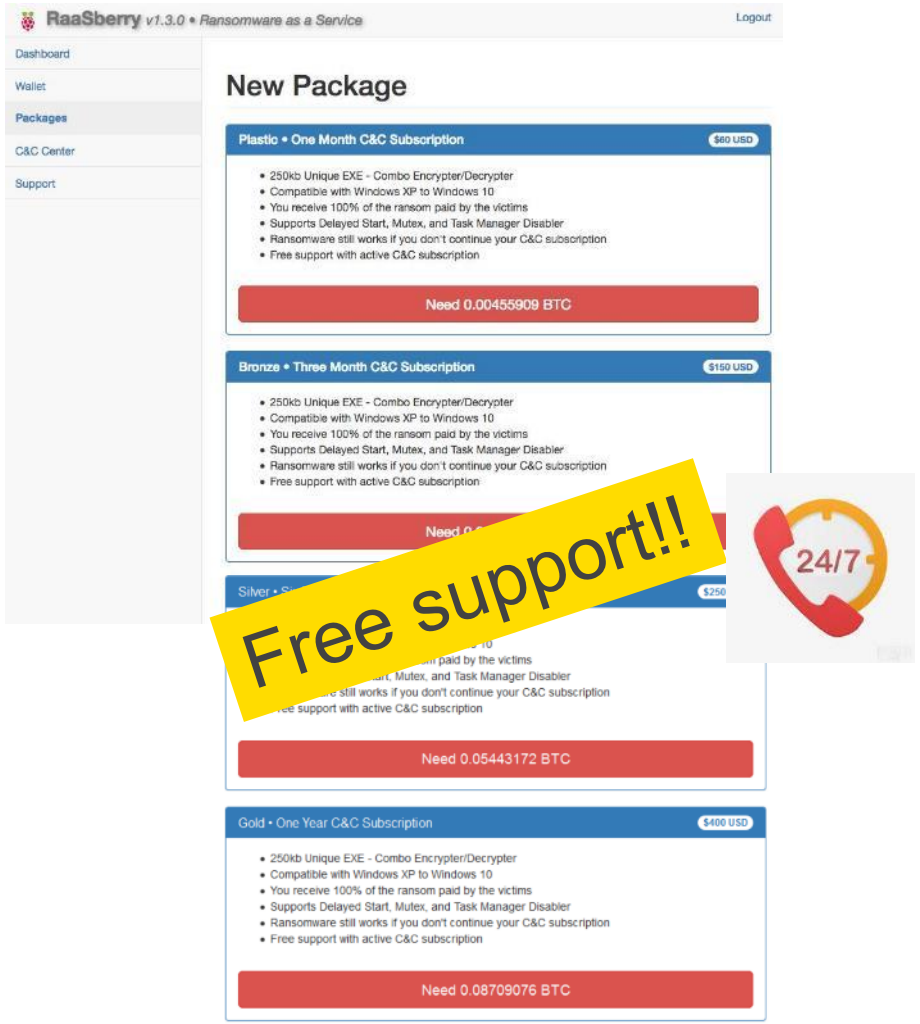
CYBER CRIME IST BIG BUSINESS
RANSOMWARE AS A SERVICE (RAAS) IM DARKWEB

- Beispiel:
  RaaSberry bietet massgeschneiderte Ransomware-Pakete, die zur Verteilung bereit sind.
  Die Plattform bietet übersichtliche Dashboards um den «Erfolg» der Kampagnen in Real-time zu verfolgen.



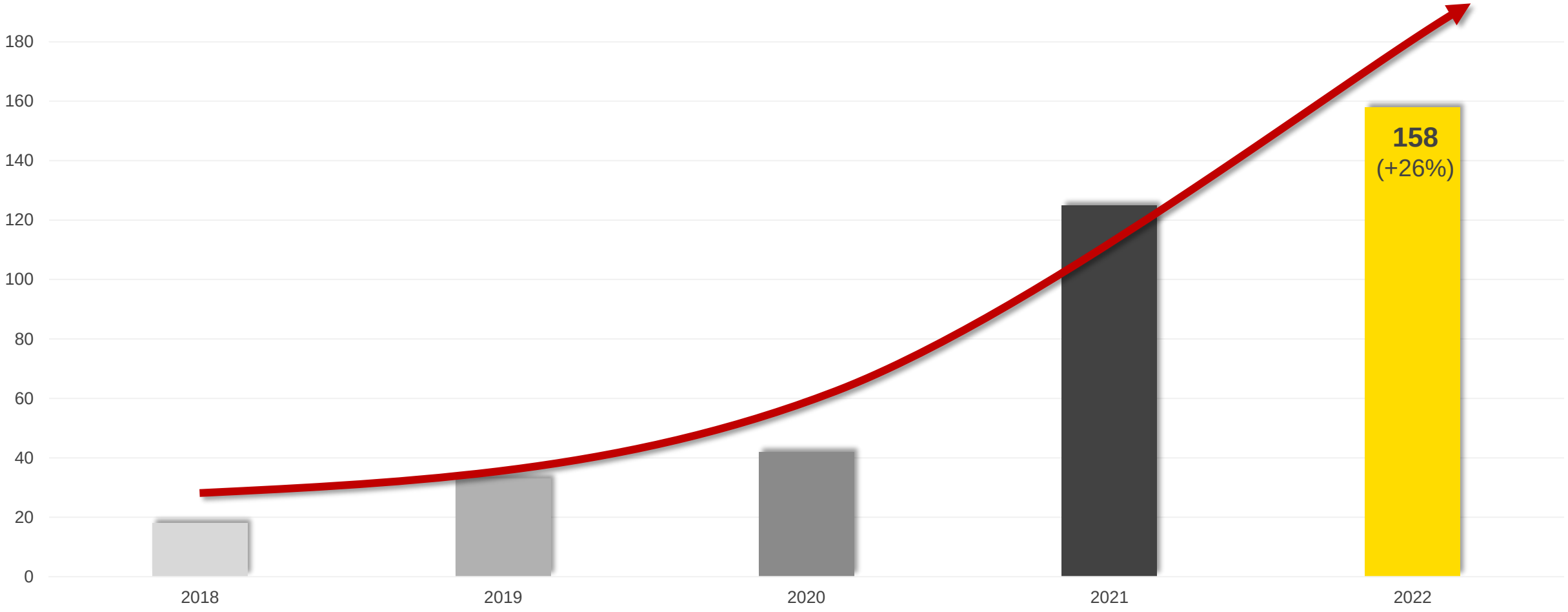
Service-Packages:

- Plastic — Abo 1 Monat für COMMAND AND CONTROL - $60
- Bronze — Abo 3 Monate für COMMAND AND CONTROL - $150
- Silver — Abo 6 Monate für COMMAND AND CONTROL - $250
- Gold — Abo 1 Jahr für COMMAND AND CONTROL - $400
- Platinum — Abo 4 Jahre für COMMAND AND CONTROL - $650



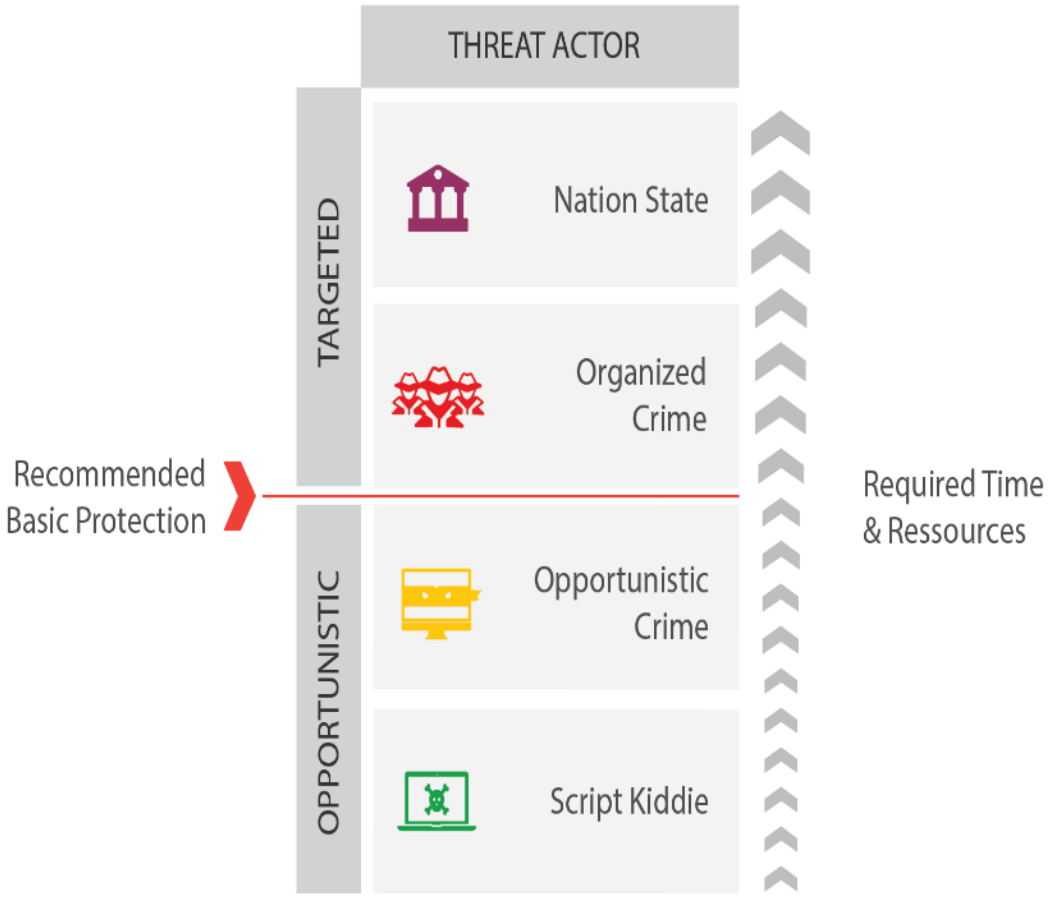
Quelle: https://resources.infosecinstitute.com/zlab-malware-analysis-report-ransomware-service-platforms/

CYBER CRIME IST BIG BUSINESS – BEARBEITETE SICHERHEITSVORFÄLLE DURCH INFOGUARD



Quelle: InfoGuard CSIRT

CYBER CRIME IST BIG BUSINESS – THREAT ACTOR MODEL



ZIELE	RESSOURCEN	VORGEHEN
• Information • Spionage • Sabotage	• Unlimitierte finanzielle Ressourcen • Zielorientiert	• Erwerb und Aufbau von Wissen • Persistente und versteckte Angriffe • Kompromittierung von Lieferanten
• Schaden • Spionage • Fear, Uncertainty and Doubt	• Grosse finanzielle Ressourcen • Möglicherweise von mehreren Firmen unterstützt	• Kauf von Wissen auf dem Schwarzmarkt • Physische Angriffe
• Finanzieller Gewinn über einen längeren Zeitraum	• Geschäftsorientiert • Agieren ähnlich wie ein KMU	• Existierende Gruppe mit einzelnen Spezialisten • Erpressung
• Ruhm • Reputation	• Minimale finanzielle Ressourcen	• Verwendung von öffentlich verfügbaren Tools

CYBER CRIME IST BIG BUSINESS – TOP THREATS

Quelle: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

PARADIGMENWECHSEL AUCH PRODUKTION

- Von einer Perimeter basierten zu einem Daten, Geräte und Benutzer basierten Fokus
- Kontrolle des Zugang zu Unternehmensressourcen
- Unabhängig vom Standort: Benutzer, Systeme und Anwendungen sind überall.

Original phrase was coined by an Forrester analyst, John Kindervag, in 2010.
Jericho Forum released a whitepaper about network de-perimeterisation in Feb 2005.

OT / IOT - VULNERABILITY

- Aufweichung / Verwässerung der NW-Architektur
  - Wireless Access: falsch konfigurierte drahtlosen Zugangspunkt/OT (WLAN, 4G-6G),
  - Neue Interfaces (non cable based; probably unknown once)
  - Interconnection zwischen Netzwerken: OT- und IT-Konvergenz
- Supply Chain und MSP Chain Attacks
- Human Errors / Menschliches Versagen and Social Engineering: Mangelndes Bewusstsein
- Malware via Internet & Intranet, USB, etc.
- Kompromittierung von Cloud-Komponenten
- Schwachstellen von Teilkomponenten
- Unzureichende Sichtbarkeit
- Schwache Passwörter
- Veraltete Komponenten (fehlende Produkte-Sicherheit)

Threats

Malware
Insider Attack
DoS / DDoS
Third Party Threats
Malfunction
Hackers

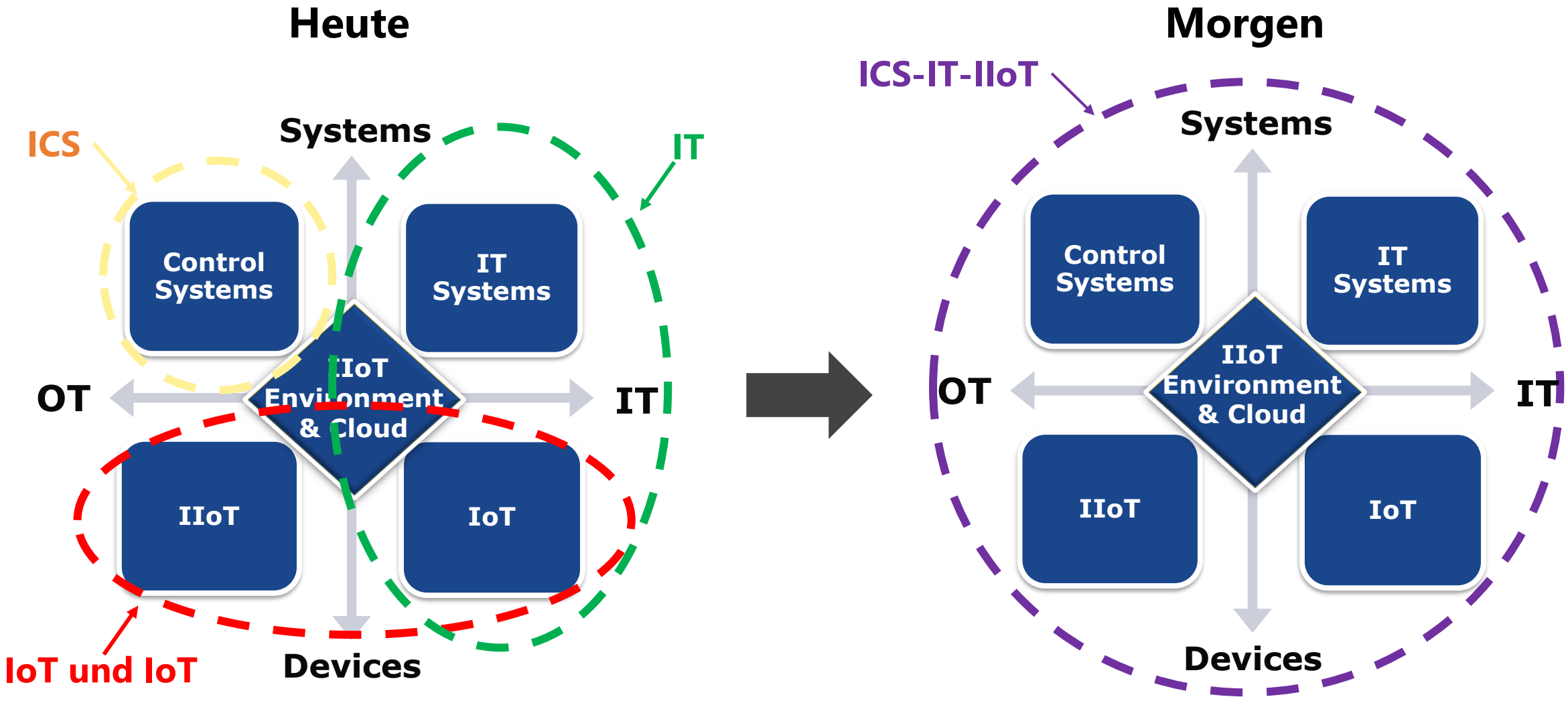
OT SECURITY – SAME, SAME, BUT DIFFERENT

IT-Security-Konzepte können nicht alle 1:1 auf OT übertragen werden, aber die Grundprinzipien sind die selben:

- OT Security ist «Security for Safety».
- «Security & Privacy by Design & Default» mit Langzeitperspektive hat hohen Stellenwert wegen langer Lebensdauer und geringer Veränderbarkeit der Systeme.
- Deterministischen Netzwerkverkehr als Vorteil für Firewalling und «Zero Trust» nutzen. «Virtual Patching» durch Kapselung und vorgelagerte Filterung des Netzwerkverkehrs.
- Visibilität, Monitoring und Alarmierung in Echtzeit noch wichtiger als für IT.
- Bei fehlgeschlagenem Update raschen (und automatischen) Fallback auf Vorgänger-Version sicherstellen.
- Ausfallsicherheit durch Redundanz erhöhen.
- Security entlang der gesamten Lieferkette sicherstellen und Lieferanten in alle Massnahmen integrieren.
- Beherrschung der Risiken soll ein ISMS eingerichtet und instandgehalten werden. Die Konformität mit ISO 27001 und wo relevant mit IEC 62443 "Industrial communication networks - IT security for networks and systems" ist anzustreben.

UNTERNEHMEN BRAUCHEN INTEGRIERTE CYBERSICHERHEITSSTRATEGIEN

InfoGuard
SWISS CYBER SECURITY



CYBERSICHERHEITSSTRATEGIE – ZERO TRUST

Die grundlegendsten Konzepte

«Never Trust, Always Verify»

- Konzept für Netzwerksicherheit
- Jedes Gerät und jeder Dienst im Netzwerk wird als potenziell unsicher angesehen
- Nicht vertrauen, sondern überprüfen

- Daten sind die neue Grenze
- Secure by Design der integrierten Komponenten (Product Security)

Zero Trust ist kein Produkt oder Dienstleistung, sondern eine Sicherheitsstrategie

SEVEN TENANTS OF ZERO TRUST (NIST) SPECIAL PUBLICATION (SP) 800-207

InfoGuard
SWISS CYBER SECURITY

1. Alle Data Sources und Compute Services werden als Ressourcen betrachtet.
2. Die gesamte Kommunikation ist unabhängig vom Standort des Netzes gesichert.
3. Der Zugriff auf einzelne Unternehmensressourcen wird per Session gewährt.
4. Der Zugriff auf Ressourcen wird durch dynamische Richtlinien bestimmt.
5. Das Unternehmen überwacht und misst die Integrität und die Sicherheitslage aller eigenen und zugehörigen Ressourcen.
6. Alle Ressourcenauthentifizierungen und -autorisierungen sind dynamisch und werden streng durchgesetzt, bevor der Zugriff erlaubt wird.
7. Das Unternehmen sammelt so viele Informationen wie möglich über den aktuellen Zustand der Anlagen, der Netzwerkinfrastruktur und der Kommunikation und nutzt diese, um seine Sicherheitslage zu verbessern.

OT VERFOLGT ZERO TRUST – EINSCHRÄNKUNGEN VON ZERO TRUST IN ICS

- Fähigkeit zur Anwendung von Mikro-Segmentierung auf Legacy-Systeme (keine Offline-Zeiten)
- Alte Protokolle (proprietär und herstellerspezifisch, insbesondere für Automatisierung und speicherprogrammierbare Steuerungen)
- Peer-to-Peer-Technologien und Mesh-Netzwerke funktionieren völlig entgegengesetzt zu Zero-Trust-Modellen, da sie von einem gemeinsamen Zugang ausgehen.
- Ein rollenbasierter Zugang und Mikroperimeter-Kontrollen sind in dieser Umgebung möglicherweise nicht möglich.
- Wenn ein ICS-Netzwerk stark auf Mesh-Technologien angewiesen ist, könnte die Einführung von Zero Trust eine Überarbeitung der Architektur erfordern.
- Ggf. sind in ICS grundlegende Änderungen an der Architektur und den Systemen erforderlich, um die Sicherheit in den Mittelpunkt ihres Designs zu stellen.

Purdue Model

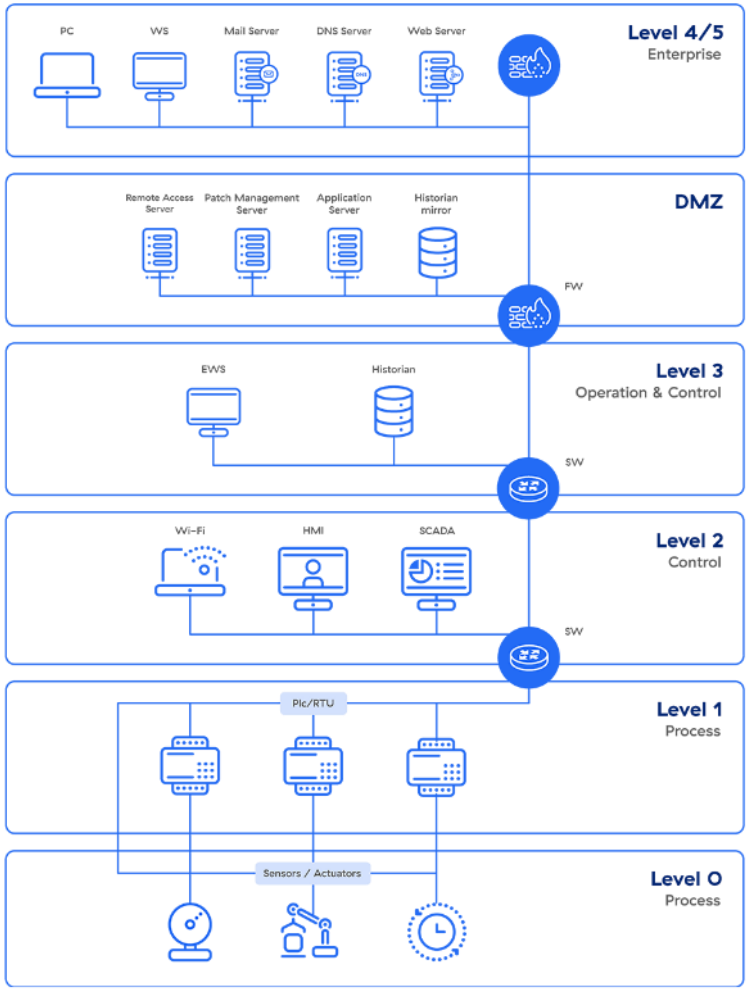


Bild Quelle: https://www.zscaler.com/

OT VERFOLGT ZERO TRUST – ABER LEIDER…

- Es gibt keine einheitliche ZTA-Lösung
- Mangel an Zeit und Ressourcen, um herauszufinden, welche Kombination von ZTA-Technologien am besten funktionieren würde
- ZTA erfordert
  - Ressourcen zu identifizieren und Prioritäten zu setzen
  - Explizite Richtlinien zu entwickeln, um die Bedingungen festzulegen, die erfüllt sein müssen, damit einem Subjekt der Zugang zu jeder Ressource gewährt wird:
    - Traditionell: Identität und Rolle der Person;
    - ZT: Standort des Subjekts und der Ressource, Tageszeit und das verwendete Gerät, sein Gesundheitszustand.
- Es fehlt ein vollständiges Inventar der Ressourcen und ein klares Verständnis der Kritikalität ihrer Daten
- Fehlender Überblick über die Transaktionen, die zwischen Subjekten, Ressourcen, Anwendungen und Diensten stattfinden
- Hohe Investitionen und ein grosser Fussabdruck in Legacy-Unternehmens- und Cloud-Technologien
- Interoperabilitätsprobleme können auftreten und zusätzliche Fähigkeiten und Schulungen erfordern

CONSLUSION

Das Purdue-Modells versucht:

Das OT-Netz zu schützen, indem es durch die DMZ vom (mit dem Internet verbundenen) IT-Netz getrennt wird.

- Angreifer haben jedoch bewiesen, dass sie in der Lage sind, diese Barriere zu durchbrechen.
- Mit der zunehmenden Konnektivität in IIoT und Industrie 4.0 wird die Notwendigkeit deutlich, die Cybersicherheit in ICS zu erweitern.

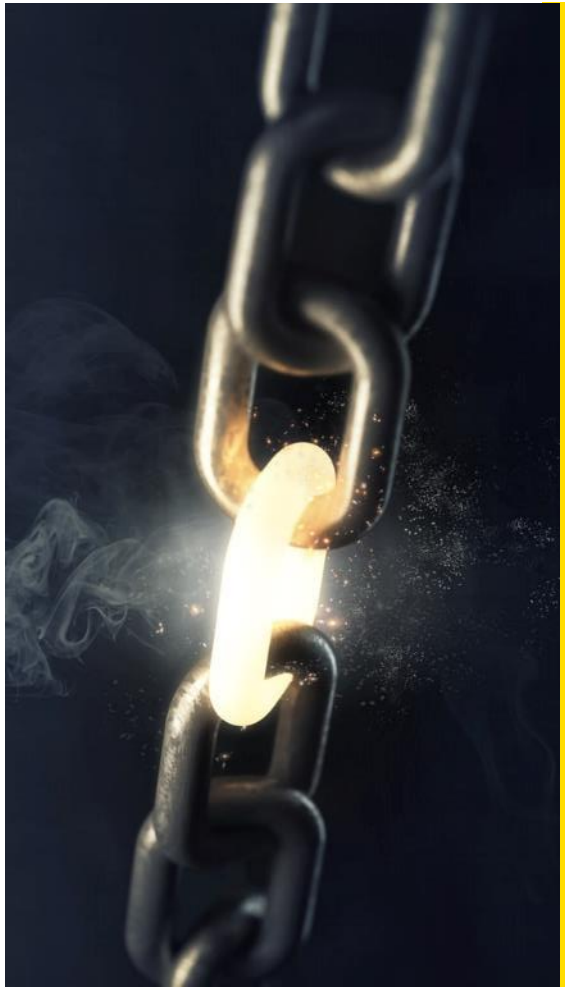
Unsere Erfahrung zeigt:

«Nur die Implementierung eines aktiveren Sicherheitsansatzes mit einem gelebten Asset-Management, granularer Zugriffskontrolle, Protokollierung und Bedrohungserkennung sowie einer proaktiven Produkte-Sicherheit verbessert die Sicherheit der kritischen Systeme nachhaltig.»


Tipps &
Tricks

SICHERHEITSMASSNAHMEN FÜR UNTERNEHMEN MIT FOKUS OT / IOT SECURITY

InfoGuard
SWISS CYBER SECURITY



- **Security Monitoring / Security Operation Center** - zentralisierte Protokollierung/zentralisierte Überwachung
- Sicherer Zugang / **Sichere Remote Zugänge** für MA, Partner und Lieferanten inkl. Multi-Faktor-Authentifizierung
- **Asset Inventarisierung**, Transparenz in der Architektur und Datenflüsse
- Kontinuierliche **Analyse und Priorisierung der Software- und Konfigurations-Schwachstellen** (Softwareversionen, Updates, Kompatibilität mit den OT-Systemen etc.).
- **Patch Management** (SW-Update, Konfiguration Anpassungen; Hardening, Segmentation, SW-Patching, etc.)
- **Netzwerksegmentierung (Micro-Segmentation)**, klare Abgrenzung zwischen nicht miteinander verbundenen Netzwerken
- Backup-Management, **Datensicherungen** sind der effektivste Weg, sich von Datenverlusten zu erholen
- Durchführen von **Recovery Tests**

DARÜBER HINAUS… – BEWÄHRTE ORGANISATORISCHE MASSNAHMEN

Cyberangriffe verhindern oder die Auswirkungen der Angriffe eindämmen.

1. Etablieren Sie eine Sicherheitsorganisation (**CISO Rolle**).
2. Stellen Sie sicher, dass das **Krisenmanagement** im Falle einer Krise **funktionsfähig** ist. Erstellen Sie dazu Aufgabenlisten, Kontaktadressen der wichtigsten Entscheidungsträger und Hilfsmittel sowie ein **Kommunikationskonzept**.
3. Stellen Sie sicher, dass ein schneller **Notbetrieb möglich** ist. Dazu müssen Sie die **zeitkritischen Prozesse kennen** und ggf. Workarounds definieren.
4. **Überprüfen** Sie regelmässig Ihre Pläne, Abläufe, Hilfsmittel und verantwortlichen Personen, beispielsweise mit Table-Top-Übungen oder jährlichen Reviews.
5. **Schulen Sie Ihre Mitarbeitende** regelmässig in Security-Awareness-Trainings.
6. Stellen Sie sicher, dass Sie Ihre **IT** möglichst **schnell wiederherstellen** können bspw. mit einem funktionierenden **Backup-Konzept** (Offline).
7. Ziehen Sie den Abschluss einer **Cyber-Versicherung** in Erwägung.
8. Richten Sie ein **Wallet für Kryptowährungen** ein.

WAS TUN BEI EINEM CYBERANGRIFF?
8-PUNKTE-PLAN FÜR DEN NOTFALL

1. Bleiben Sie **ruhig** und gehen Sie **strukturiert** an die Lösung der Probleme.
2. Alarmieren Sie die für die Bewältigung notwendigen Mitarbeitenden und etablieren Sie einen **Krisenstab**, der die Aktivitäten steuert.
3. Holen Sie sich für die Bewältigung von Sicherheitsvorfälle **externe Unterstützung** (Sicherheitsunternehmen, Versicherungen, KAPO, NCSC).
4. Bestimmen Sie gemeinsam mit Experten, welche **Sofortmassnahmen** eingeleitet werden müssen.
5. Sorgen Sie dafür, dass Ihre **wichtigsten Prozesse weiterbetrieben** werden können – manchmal sind diese auch ohne IT betreibbar (inklusive Zahlungsverkehr).
6. **Kommunizieren** Sie **regelmässig**, z.B. an Kunden, Partner, Mitarbeitende, Öffentlichkeit, Regulatoren.
7. Nach Analyse und Eindämmung des Vorfalls, stellen Sie sicher, dass der **Angreifer nachhaltig entfernt** wird.
8. Bereinigen Sie Ihre IT-Systeme schrittweise und stellen Sie Ihre **Handlungsfähigkeit** wieder her.

HABEN SIE EINEN CYBERANGRIFF? KONTAKTIEREN SIE UNS

InfoGuard
SWISS CYBER SECURITY

CSIRT

7x24 Hotline: +41 41 749 19 99
E-Mail: investigations@infoguard.ch

Please note, that in urgent cases and out of office hours the hotline has to be called.

IOT, hybride Arbeitsmodelle und Mobilität machen die Netzwerksicherheit zur Herausforderung

HPE Aruba Networking Edge-to-Cloud Security

Markus Limacher, Head of Security Consulting, InfoGuard AG
Beat Sommerhalder, Country Manager, HPE Aruba Networking Switzerland

27.02.2023

Accelerating adoption of new models can be challenging

Zero Trust

- Eliminates implicit trust
- Provides least-privilege access to resources
- Requires continuous monitoring

Secure Access Service Edge (SASE)

- Builds on Zero Trust security services with WAN capabilities
- Delivers security services via the cloud

New models can be difficult to implement

- 60% of organizations will embrace Zero Trust, yet most will fail to realize the benefits[1]
- Challenge: Access controls enabled via several platforms that are not integrated
- Headless IoT devices cannot support agents for cloud-delivered security[2]

1. Gartner, May 2022
2. Forrester, Jan. 2022

HPE aruba networking

IoT Security

New models require new capabilities

Identity-based controls

Authoritative NIST Zero Trust Architecture and Gartner SASE frameworks specify **identity as a key component**

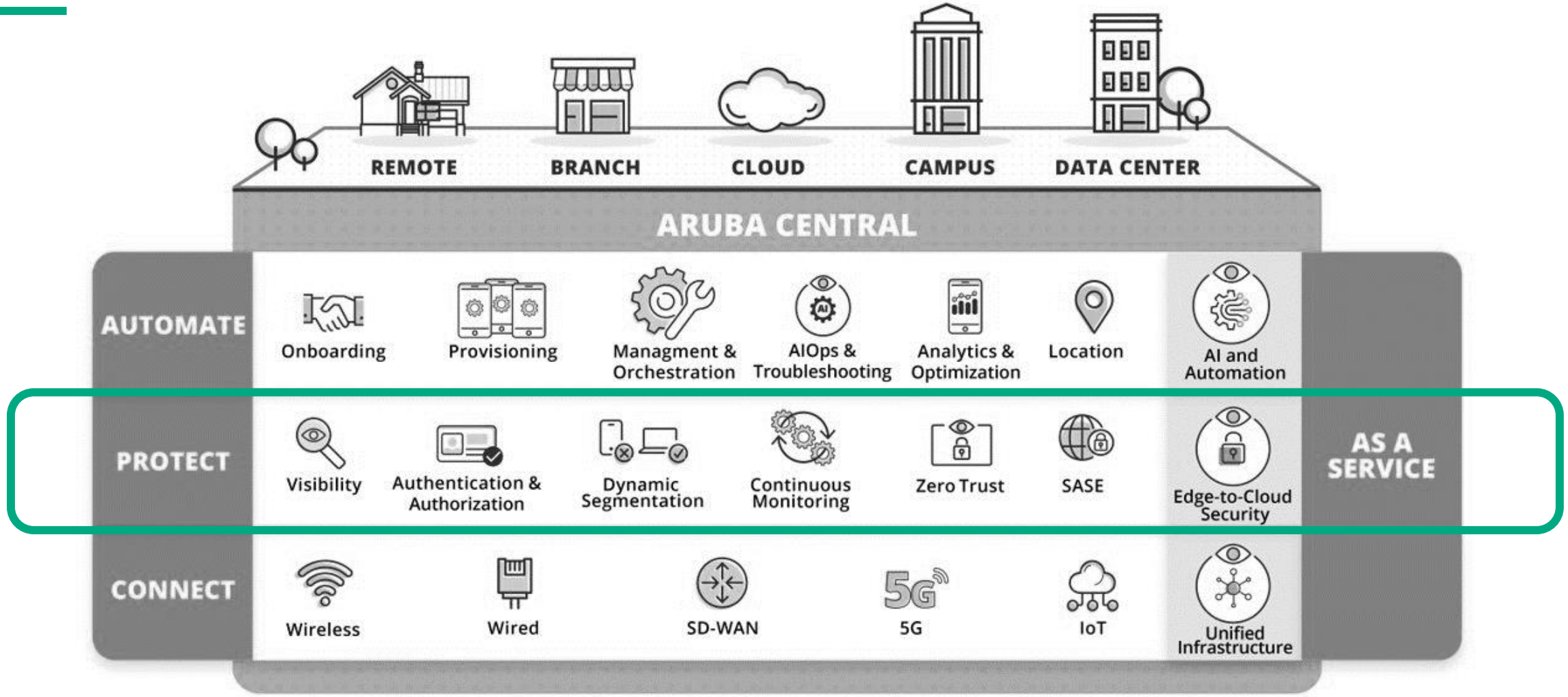
Integration

Addresses operational complexity that can slow implementation and lead to security issues

HPE aruba networking

IoT Security

HPE Aruba Networking Edge Services Platform (ESP) architecture



Built-in support for Zero Trust and SASE security frameworks
that increases protection while simplifying operations

HPE aruba networking

IoT Security

HPE Aruba Networking Zero Trust security foundation

ClearPass Policy Manager

Client Insights
ClearPass Device Insight

Policy Enforcement Firewall
SD-WAN
Unified Threat Management/IDS/IPS
360 Security Exchange

Cloud Auth
ClearPass Policy Manager

Dynamic Segmentation

Centralized Overlay

- ClearPass Policy Manager
- Policy Enforcement Firewall

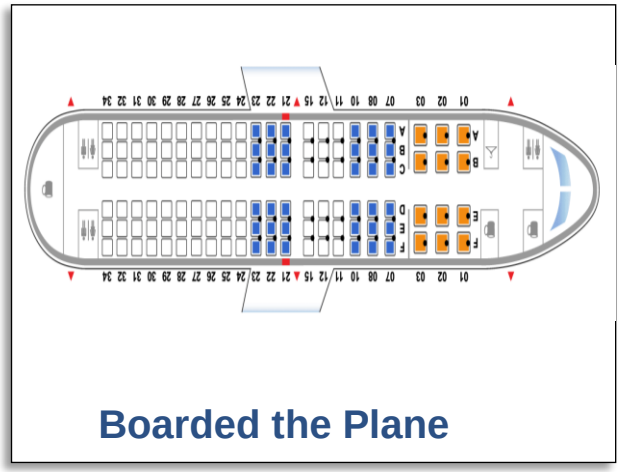
Distributed Overlay w/ Central NetConductor

- Policy Manager, Flexible NAC
- Inline Enforcement via Switches & Gateways

HPE aruba networking

IoT Security

Need to Secure Your Edge? Let's look at Airport Security



HPE aruba networking

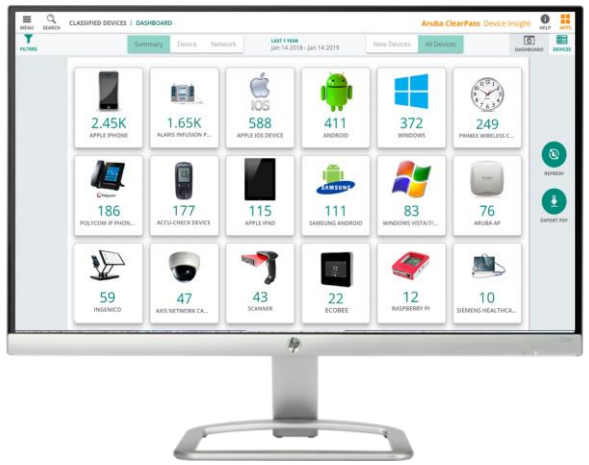
IoT Security

WHO? Is Boarding into the Network

AT THE AIRPORT

VISIBILITY INTO THE OVERALL ENVIRONMENT IS A FIRST IMPORTANT STEP.

AT THE EDGE



CLEARPASS DEVICE INSIGHT

- What's connected to your network (Wired & Wireless) - regardless of location
- AI-powered visibility
- Embrace IoT without security worries
- Ensures Secure Access for every connected device
- 24/7 Visibility and Control

HPE aruba networking

IoT Security

Identify Yourself with proper AUTHENTICITY

AT THE AIRPORT

BOARDING PASS & PASSPORT SCANS

The goal of this layer of inspection is to reduce the attack surface by minimizing the movement of people into places where they are not supposed to go.

AT THE EDGE

- Robust Authentication for Users | Devices | IoT. On Wired, Wireless and Remote Access
- Secure Authorization (User & Device Role & Auth Method)
- Automated BYOD provisioning
- Guest access that's simple and fast

HPE aruba networking

IoT Security

Complete SCAN before Accessing the Resources

AT THE AIRPORT

FULL BODY AND LUGGAGE SCANNERS

The goal of this layer is to ensure that people heading toward departing airplanes are not carrying anything dangerous

AT THE EDGE

Distributed Stateful Segmentation,

DPI ENGINE

TPM CHIP

HPE aruba networking

IoT Security

IDENTITY-BASED Access Privileges

AT THE AIRPORT

MICRO SEGMENTATION

Access control that reduces the attack surface by minimizing allowed connections between workloads.

AT THE EDGE

DYNAMIC
SEGMENTATION

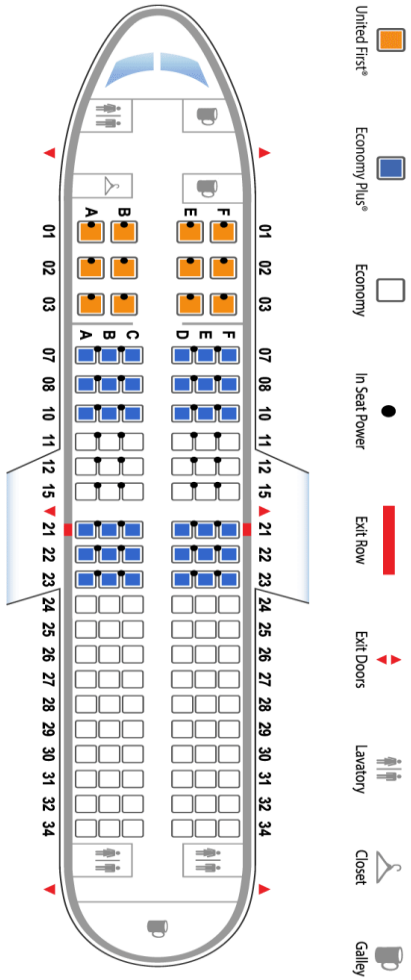
CENTRAL
NETCONDUCTOR
ROLE-BASED SECURITY

- Micro-Segmentation
- Simplified Security Operations
- Easy Management of User Policy and Access to right Applications

HPE aruba networking

IoT Security

Better User Experience with Continuous Monitoring



IN THE PLANE

MONITORING

Monitoring and Assisting Passengers on the Plane with different services to cater the needs and insights

AT THE EDGE

CONTINUOUS MONITORING
Aruba Threat Defense

ARUBA SECURITY EXCHANGE

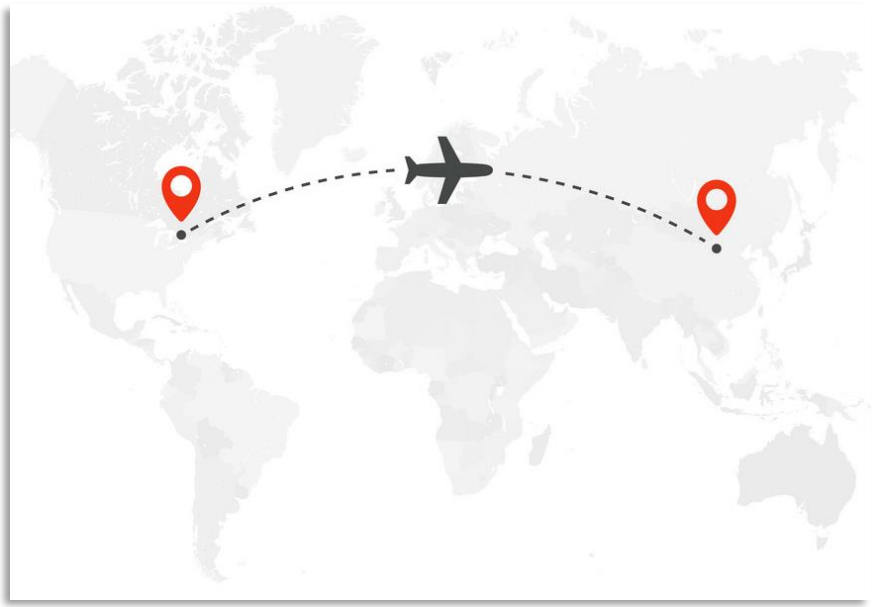
ENFORCEMENT AND RESPONSE
Attack Response
Event-triggered actions

Continuously Monitoring of every Users / Devices on the Network and take appropriate actions when needed.

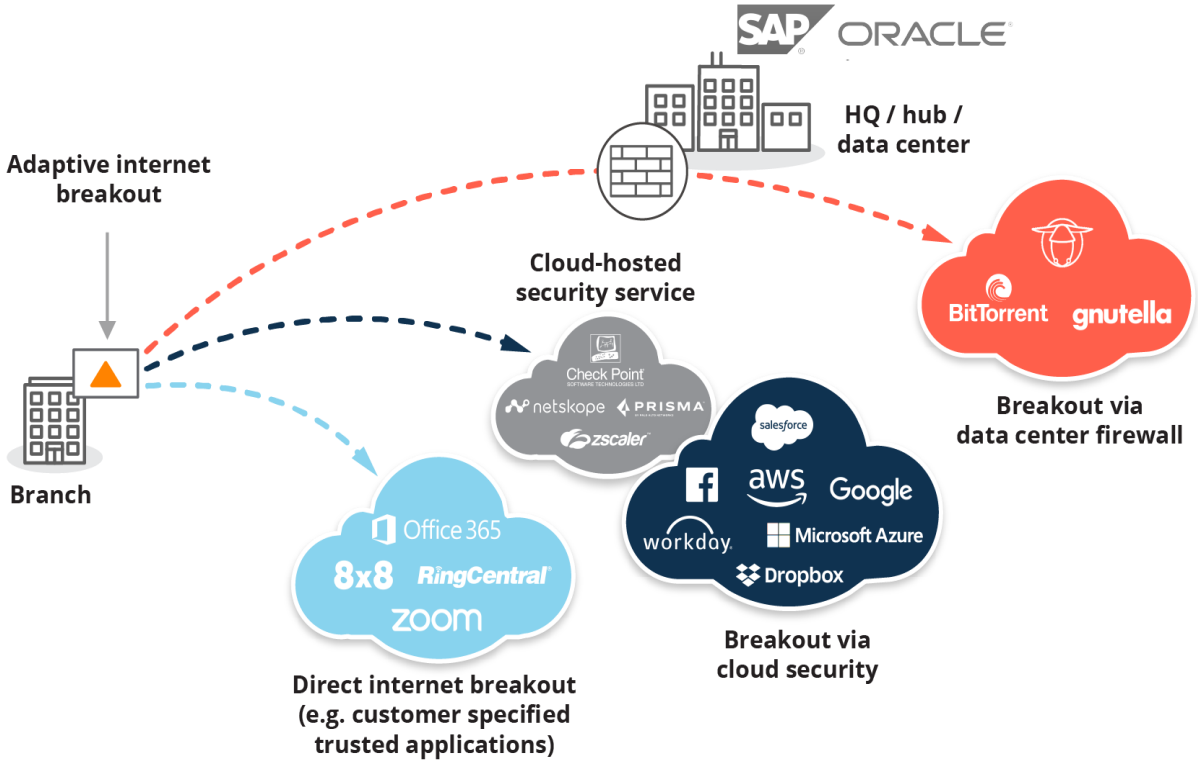
HPE aruba networking

IoT Security

Security from EDGE to CLOUD



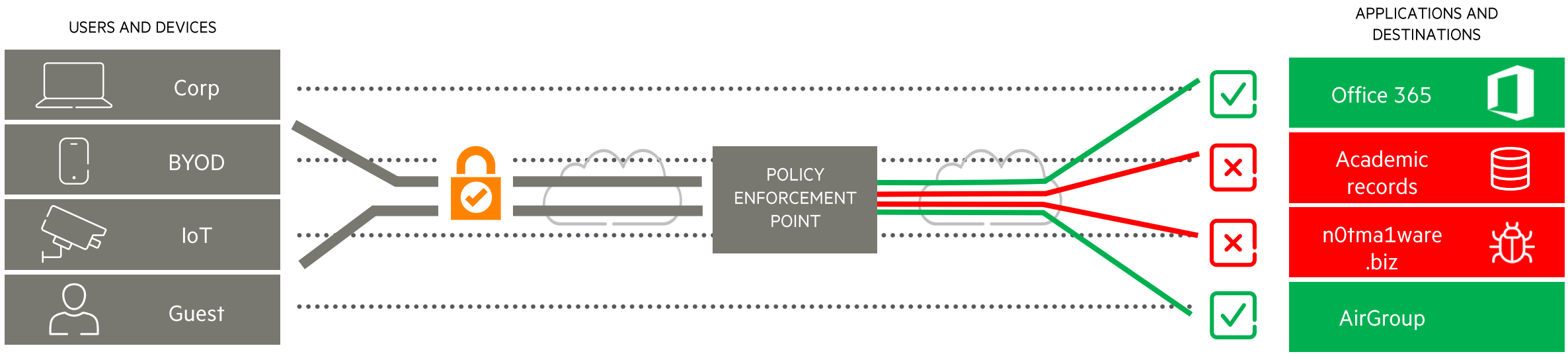
Aircraft turnaround time and Routes are essential to keeping flights on time and passenger experience better. Routes are used to ensure that flights stay with the “flow” of traffic, remain clear, avoid congestion, clear weather updates and where aircraft are deviating or refusing to fly.



Consistent secure connectivity from users to applications with Improved Application Performance

Dynamic Segmentation

Automatically enforce least-privilege access to resources based on identity



Choice & flexibility in enforcement model

HPE aruba networking

IoT Security

LET'S INNOVATE TOGETHER

We are customer first, customer last

Silicon Valley born: We are unconventional and innovative

Agile: "We are the biggest small company"