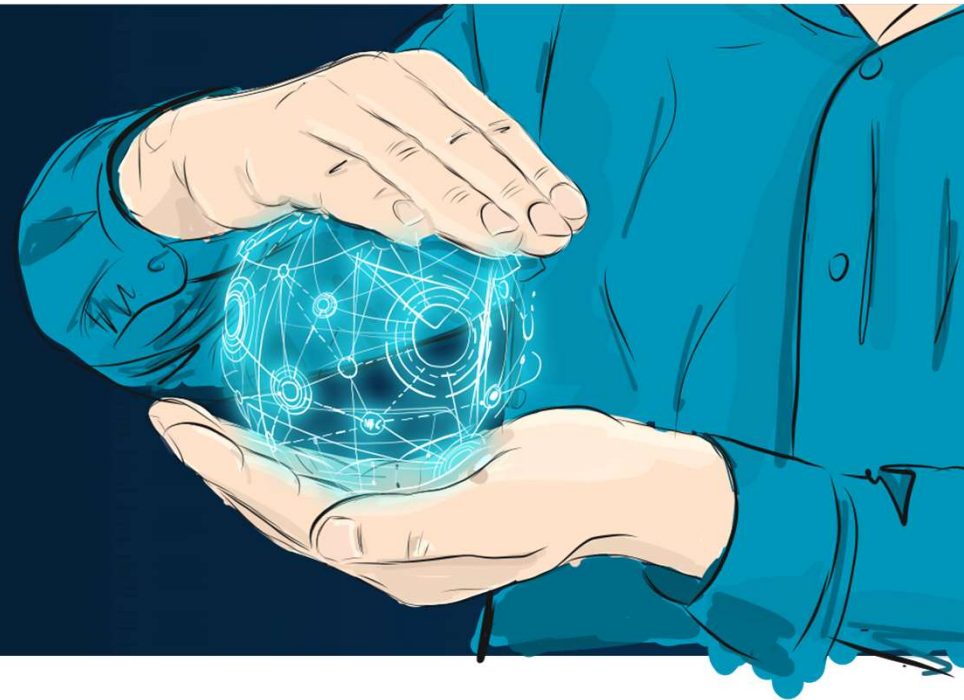




NETWORK ACCESS CONTROL MIT MACMON

ZTNA – intelligent einfach für Netzwerke und Cloud



macmon secure GmbH

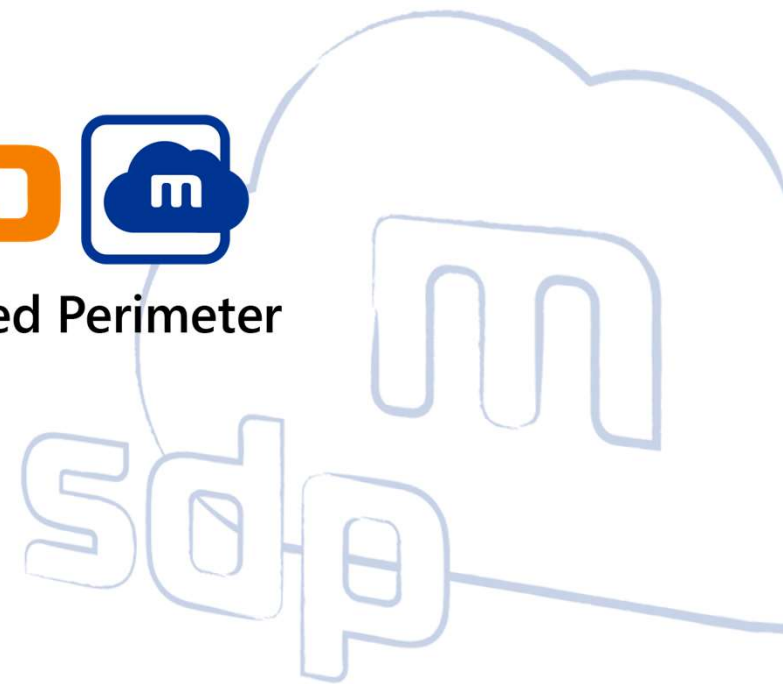
Eine Marke – zwei Produkte



Network Access Control



Secure Defined Perimeter



Innovator

des Jahres 2021

WEIL IMMER JEMAND EIN **NEUES GERÄT** HAT



macmon secure GmbH

Best of Breed ZTNA-Anbieter

- Gründung: 2003 in Berlin, 70 Mitarbeiter
- Erfahrenes Team mit Entwicklung, Support (24x7) und Beratung an zentraler Stelle in Berlin
- Ca. 1.600 Installationen in Europa – hohe Kundenzufriedenheit (>95%)
- Vielzahl an Integrationen mit weiteren führenden Sicherheitstechnologien
- Seit 2022 Teil der BELDEN-Gruppe



Belden – Eine lange Tradition

Gegründet von Joseph Belden im Jahre 1902

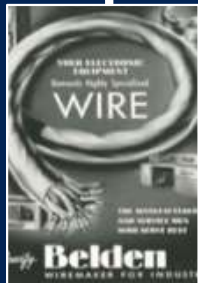


Seit unseren Anfängen als Hersteller hat sich Belden konsequent auf die Kunden konzentriert und sich einen Ruf für Qualität, Einfallsreichtum und Werthaltigkeit aufgebaut.

Rundfunk in den 1920er Jahren



Computer-Netzwerke in den 1980er-90er Jahren



Zu den frühen Kunden gehört Thomas Edison



Fernsehen in den 1950er Jahren



Belden Heute

Komplettes Produktportfolio mit Kabel-, Konnektivitäts- und Netzwerkprodukten



Aktivitäten in **Amerika, Europa, dem Nahen Osten, Afrika und dem asiatisch-pazifischen Raum**

25+ Produktionsstätten



Over **7,900** Mitarbeiter

Umsatz: **\$2.4B USD**



NYSE: **BDC**



Roel Vestjens, President & CEO

Belden Portfolio

Die branchenweit umfassendste Suite von Netzwerklösungen bietet Unternehmen weltweit vollständige Konnektivität und Sicherheit.



Industrial Automation Solutions

Networking
Connectivity
Network Security

Schlüsselmärkte

Discrete Manufacturing
Process Facilities
Energy
Transportation



Smart Buildings Solutions

Connectivity
Network Security

Schlüsselmärkte

Healthcare
Data Centers
Government
Professional Broadcast
Hospitality
Financial
Commercial Real-Estate



Broadband & 5G Solutions

Broadband Fiber
Broadband Copper

Schlüsselmärkte

MSO / Cable Operators
TELCOs / Mobile Network

Business Platform: Industrial Automation

Industrielle Kabel- und Netzwerklösungen maximieren die Sicherheit und Produktivität geschäftskritischer industrieller Infrastrukturen.



Industrial Cable Solutions

Fiber/Copper Cable

- Industrial Ethernet Cable
- Data Bus Cable
- Multi-Conductor Cable
- Fiber Optic Cable
- VFD Cable
- Flex Cable
- Hook-up & Lead Wire
- Portable Cordage
- Power & Control Tray Cable
- Instrumentation Cable
- Armored Cable
- IMSA Traffic Signal Cable
- SpaceMaker Cable

Industrial Network Solutions

Networking

- Wireless Network
- Management
- Software
- Gateways
- Switches
- Routers

Connectivity

- Active I/O Modules
- Passive Distribution Boxes
- Connectors
- High-Density Fiber & Copper Infrastructure Solutions

Network Security

- **Network Access Control / Zero Trust Network Access**
- Security Configuration Management
- Industrial Firewalls
- Managed Services

INS Product Portfolio – Hirschmann



Industrial Network Solutions

Sowohl schnelle IT-Entwicklungen als auch der stetige Fokus auf Effizienz treiben den Bedarf an intelligenteren und vernetzteren Geräten und Maschinen voran.

Ein massives Wachstum an Daten, Audio und Video muss sicher und in Echtzeit erfasst und übertragen werden.

Industrial Network Solutions bietet innovative Lösungen, die aktuelle und zukünftige Anforderungen an die Netzwerkinfrastruktur in reifen und aufstrebenden Märkten erfüllen.

macmon Technologiepartnerschaften & Schnittstellen



Weitere Schnittstellen zu diversen Herstellern wie:

Cisco, Fortinet, Kaspersky, LogPoint, Symantec, TrendMicro...

Generische Anbindungen über:

RADIUS Proxy, SAML 2.0, Microsoft AD & LDAP, WSUS/SCCM, REST-API (Inbound & Outbound)



ASSET-MANAGEMENT



IDENTITÄTS-QUELLEN



COMPLIANCE



INFRASTRUKTUR

Auch Diese Kunden setzen macmon NAC ein – als Produkt



AEB

RWE

MBDA
MISSILE SYSTEMS



STADT ESSLINGEN AM NECKAR



Network Access Control – NAC

Die Beantwortung von offenen Fragen

Haben Sie UFOS in Ihrem Netzwerk? (unbekannte fremde Objekte)



Wer ist gerade in Ihrem Netzwerk?



Wie lange brauchen Sie um ein Gerät / eine Bedrohung zu isolieren?



Wissen Sie welche Geräte sich momentan in Ihrem Netzwerk befinden?



Wer hat denn bei Ihnen die Macht über das Netzwerk?



Network Access Control – NAC

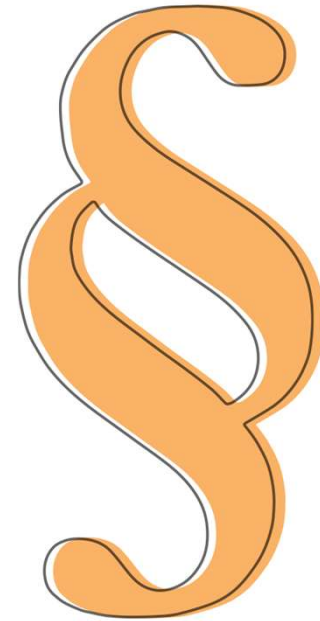
Die Erfüllung diverser Vorgaben und Anforderungen

- Datenschutz-Grundverordnung
- DIN EN 80001-1
- Payment Card Industry Compliance (PCI)
- ISO IT Sicherheitsstandard gemäß ISO 27001/27002
- Audits (z. B. Tisax)

BSI IT-GRUNDSCHUTZ-KATALOGE

Genehmigungsverfahren für IT-Komponenten (Maßnahme 2.216):

„Die Installation und Benutzung nicht freigegebener IT-Komponenten muss verboten und die Einhaltung dieses Verbotes regelmäßig kontrolliert werden.“

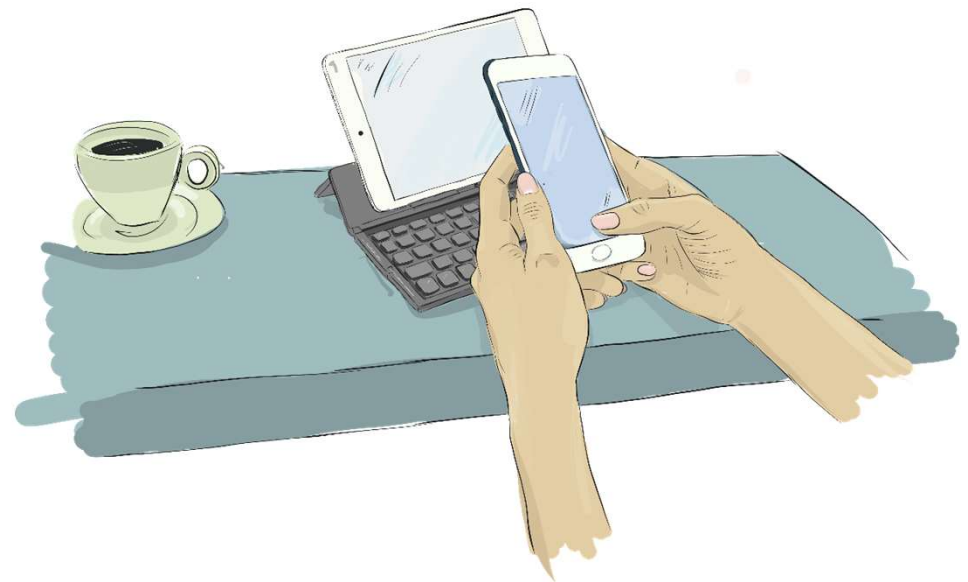


Use cases

Ein Mitarbeiter zieht innerhalb des Unternehmens um und benötigt Zugriff auf die gewohnten Ressourcen.



Ein Gast meldet sich mit seinem Handy und seinem Tablet über den Gastzugang im Netzwerk an.



Network Access Control – NAC

Die Verhinderung von Vorfällen!

COMPUTERWOCHE
VOICE OF DIGITAL

Alle aktuellen Webcasts

Suchen nach ...

Netzwerksicherheit

US-Geheimdienst drängt Unternehmen zu Zero Trust

23.03.2022 Von Jan Gold (Autor) [FOLGEN](#)

Die NSA empfiehlt Unternehmen, eine Zero-Trust-Umgebung aufzubauen, um ihre Infrastruktur besser vor Angriffen zu schützen. Ausführliche Konfigurationstipps für Administratoren liefert die NSA gleich mit.

Die Nationale Sicherheitsbehörde (NSA) hat diese Woche detaillierte Empfehlungen für Unternehmen zum Schutz ihrer Netzwerkinfrastruktur vor Angriffen ausgesprochen. Sie gibt Tipps zur sicheren Konfiguration häufig verwendeter Netzwerkprotokolle und drängt auf die Anwendung grundlegender [Sicherheitsmaßnahmen](#) für alle Netzwerke.



Um Netzwerke vor Cyber-Angriffen wie einer DDoS-Attacke besser zu schützen, empfiehlt die NSA den Aufbau einer Zero-Trust-Umgebung.

Foto: Marcel Poncu - shutterstock.com

Der Bericht der NSA unterstreicht die Bedeutung von Zero Trust für die Netzwerksicherheit, doch der Großteil befasst sich mit konkreten Schritten, die Netzwerkadministratoren unternehmen sollten, um ihre [Infrastruktur](#) vor Angriffen zu schützen. Zu den Konfigurationstipps für Netzwerkadministratoren gehören

- die Verwendung sicherer, häufig geänderter [Kennwörter](#) für alle administrativen Konten,
- die Begrenzung von Anmeldeversuchen und

MEHR ZUM THEMA

- Authentifizierung neu gedacht: Zero Trust verstehen und umsetzen
- Wolke braucht grüne Wiese: Erfolgsfaktoren für Cloud-native im Unternehmen
- In 5 Schritten zum Zero-Trust-Netzwerk (Hersteller: Palo Alto Networks)
- Cyber-Security-Vollkasko für Unternehmen

KOSTENLOSE NEWSLETTER

- Cloud Computing
- Digitalisierung
- Freiberufler & Gründer
- IT-Management
- Job-Karriere
- Mittelstand
- Mobile
- Nachrichten mittags
- Nachrichten morgens
- Newsletter zur Corona-Krise
- Produkte/Technologien
- Security
- Software & Cloud
- Stellenmarkt
- Wochenrückblick

E-Mail-Adresse eingeben... [Bestellen](#)

AKTUELLE WEBCASTS

golem.de
HOME NICHT VIDEOS VORGELESEN FORUM FREIWERBBLICHT

TOP THEMEN: Jobs, 13.03.2019 Netzpolitik, Homeoffice, Smartwatch, Auto, mehr...


IT-KARRIERE STELLENMARKT SEMINARE IT-KÖPFE GEGENSTÄNDLICH

JPL

Nasa über Raspberry Pi gehackt

Mit einem Raspberry Pi können tolle Dinge angestellt werden - in ein Netzwerk der Nasa sollte aber auch ein Bastelrechner nicht ohne weitere Prüfung eingebunden werden: Hacker konnten Daten der Marsmissionen erbeuten, indem sie einen ungesicherten Raspberry Pi als Einstieg nutzten.

22. Juni 2019, 12:54 Uhr, Tobias Körtzsch



Die Nasa wurde gehackt.


Hacker haben ungefähr 500 MByte an Daten aus dem Netzwerk des Jet Propulsion Laboratory (JPL) der Nasa erbeutet, indem sie einen Raspberry Pi als Einstiegspunkt nutzten. Der Bastelrechner war ohne Autorisierung in das Netzwerk eingebunden und entsprechend nicht ausreichend gesichert.

Stellenmarkt

Anwendungsbetreiber (m/w/d) IT-Support
NORDHAWKEMIE, Elmhorn

Betriebsingenieur (m/w/d) Netzwerkschicht
RT Kabel Brandenburg GmbH, Brandenburg an der Havel
Detaillierte

Der Angriff erfolgte bereits im April 2018 und blieb ein Jahr lang unentdeckt, wie Zdnet [in](#) unter Berufung auf einen Bericht der Nasa [in](#) schreibt. Der Zwischenfall ist unter anderem Thema eines Sicherheitsberichts des Office of Inspector General (OIG) der Nasa, das firmeninterne Untersuchungen durchführt.



Video: NGIS Omega Test der ersten Sojus/Nasa (B4E)

Wirtschaft > Insulin: Wenn IT-Einbrecher lebenswichtige Medizingeräte entern

Frankfurter Allgemeine
Wirtschaft

F.A.Z.-INDEX [2443,05](#) +0,51% [DAX](#) [12.593,61](#) +0,60% [EUR/USD](#) [1,1720](#) -0,25% [DOW JONES](#) [24.776,60](#) +1,31% [ALLE KURSE](#)

INSULIN

Wenn IT-Einbrecher lebenswichtige Medizingeräte entern

VON JONAS JANSEN - AKTUALISIERT AM 05.10.2016 - 17:27



Der Pharmakonzern Johnson & Johnson meldet eine Sicherheitslücke in vernetzten Insulinpumpen. Der Fall ist besonders spektakulär.

[FACEBOOK](#) [TWITTER](#) [XING](#) [EMAIL](#) [PRINT](#) [SHARE](#) [LINK](#) [BOOKMARK](#)

Das amerikanische Medizintechnikunternehmen Johnson & Johnson (J&J) hat in dieser Woche Hunderttausende unangenehme Briefe verschicken müssen. In dem Schreiben, das an Ärzte und etwa 114.000 Patienten in Nordamerika rausging, musste J&J einräumen, dass es eine Sicherheitslücke in einer Insulinpumpe gibt und Hacker theoretisch das Gerät fernsteuern könnten. Das kann für Diabetiker lebensgefährlich sein, wenn die Insulinzufuhr manipuliert wird, also etwa mehr Insulin durch die tragbare Pumpe ausgeschüttet wird, die über einen Katheter mit dem Körper verbunden ist.

Hackerangriffe 2020

Nachgezählte Hackerangriffe

11

erfolgreiche Hackerangriffe

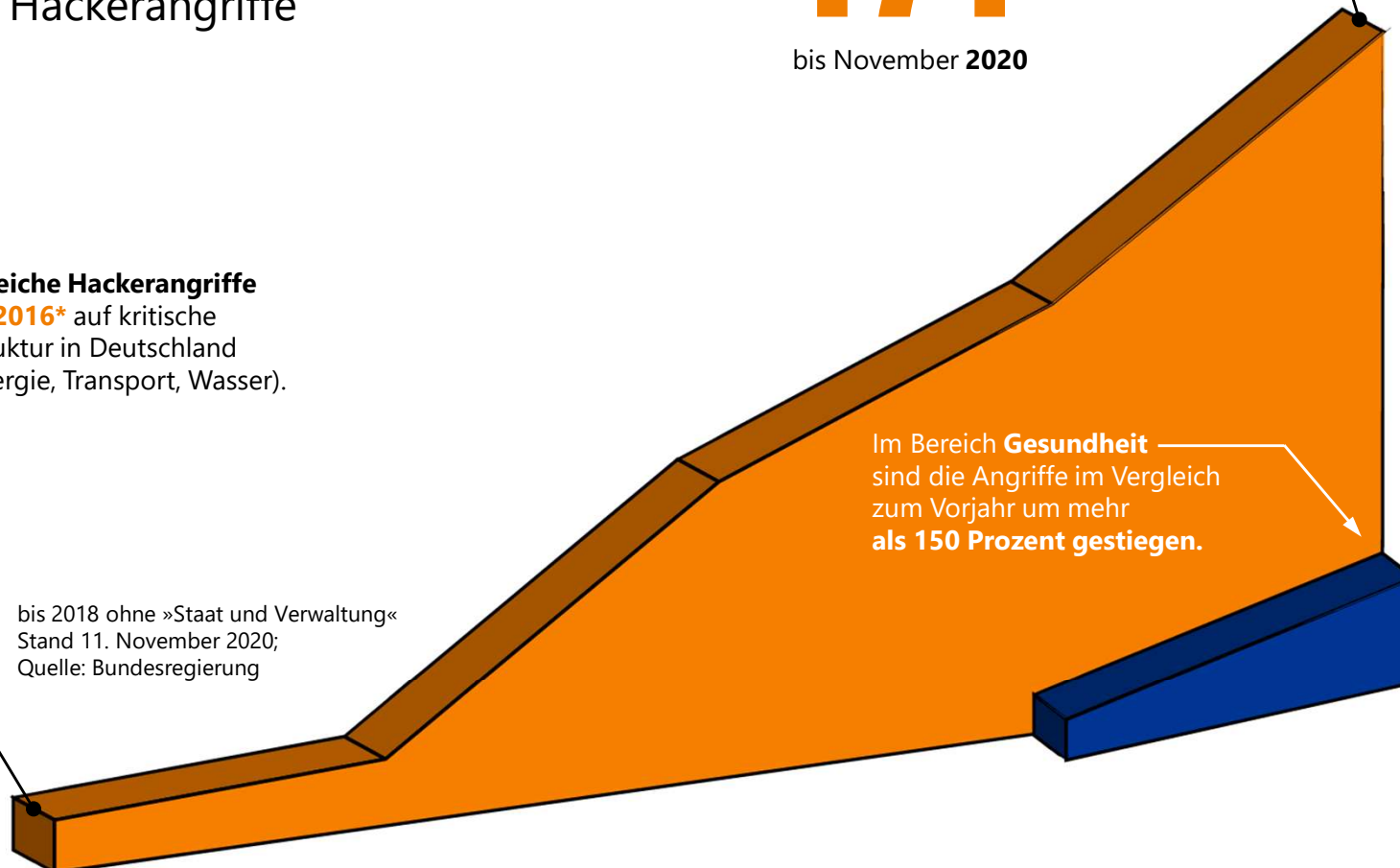
gab es **2016*** auf kritische Infrastruktur in Deutschland (z.B. Energie, Transport, Wasser).

bis 2018 ohne »Staat und Verwaltung«
Stand 11. November 2020;
Quelle: Bundesregierung

171

bis November 2020

Im Bereich **Gesundheit** sind die Angriffe im Vergleich zum Vorjahr um mehr **als 150 Prozent gestiegen.**

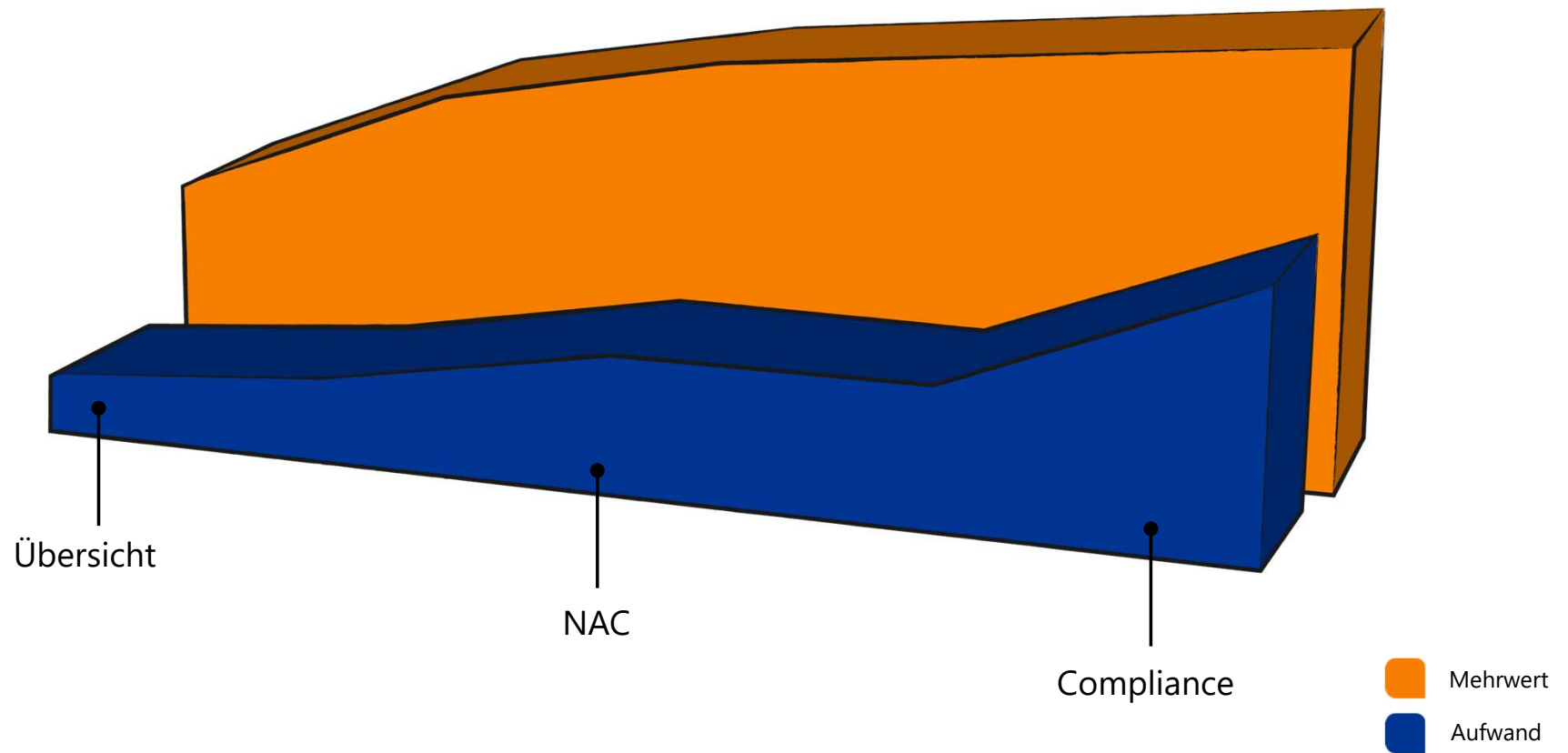


- Gesamt
- Bereich Gesundheit

Grafik aus **DER SPIEGEL** 49/2020

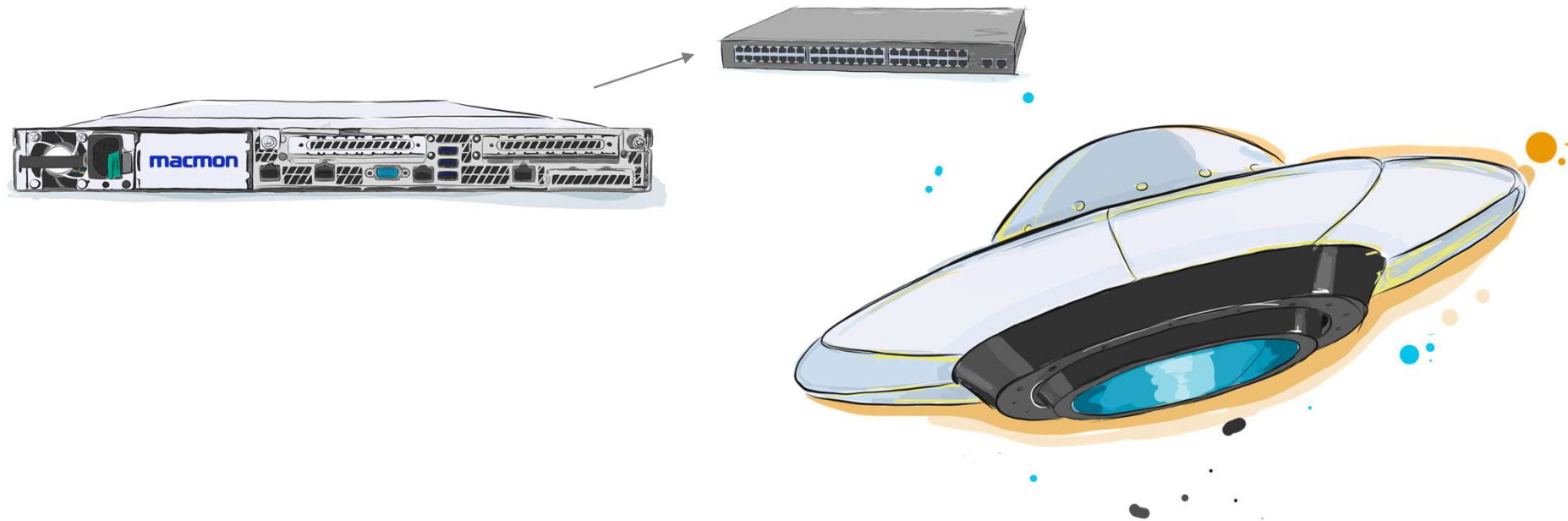
Network Access Control – NAC

Drei Kernthemen



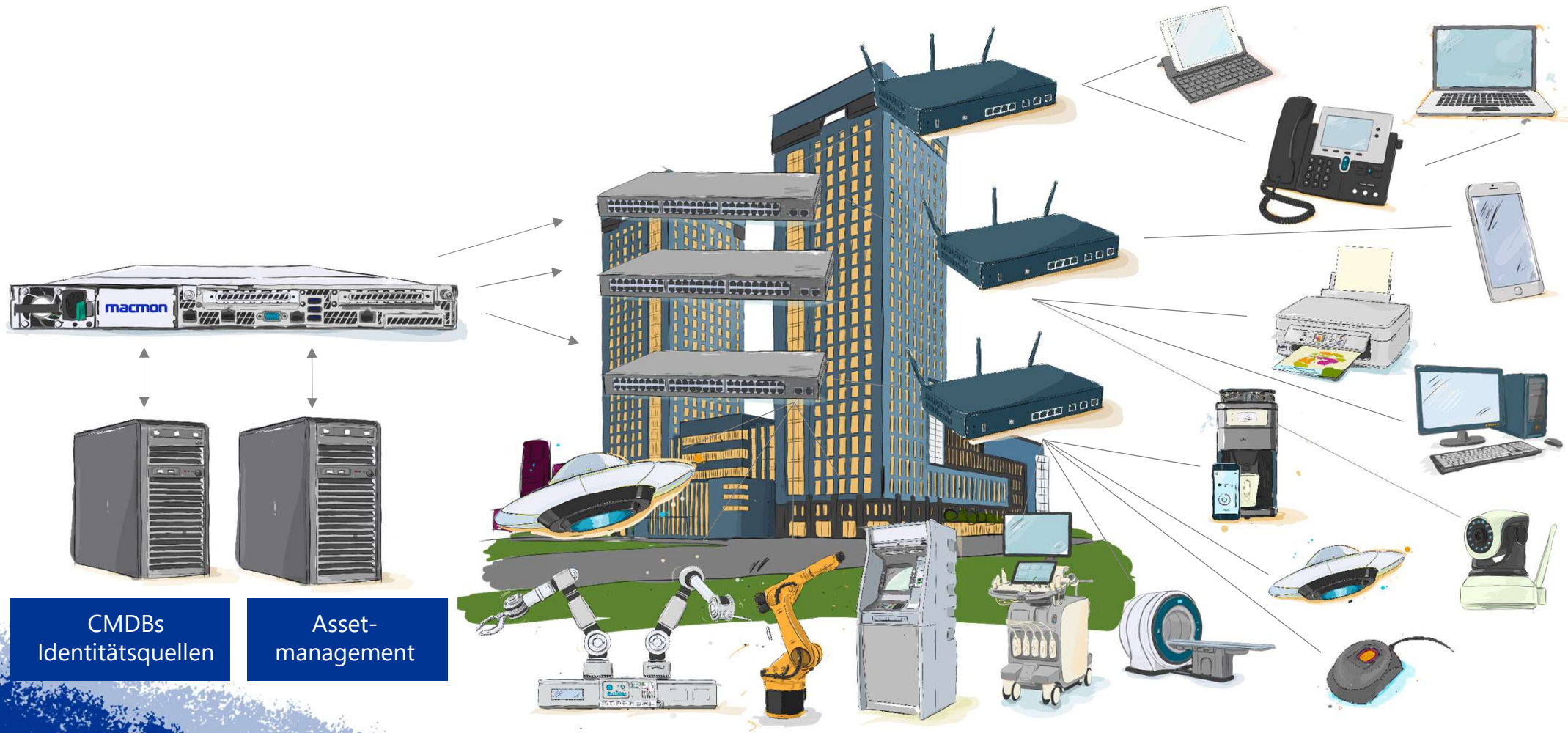
Die Übersicht

Sehen was im Netzwerk ist und aufspüren von **U**nbekannten **F**remden **O**bjekten



Die Übersicht

Sehen was im Netzwerk ist und aufspüren von **U**nbekannten **F**remden **O**bjekten



Automatische Netzwerktopologie

The screenshot displays the macmon network topology tool interface. The main window shows a network diagram titled "Display topology (macmon - Demo)" with a current view of "_default_". The diagram illustrates a multi-site network topology with four main sites: Berlin, Paris, London, and Rome. Each site is represented by a colored rounded rectangle containing various network devices and their interconnections.

- Berlin (Grey):** Contains a central HP ProCurve Switch 2911 (Id: 483) connected to several Cisco 2960 switches and a file server (fileserver.wuesten.nw_access).
- Paris (Dark Grey):** Contains a central HP ProCurve Switch 2911 (Id: 483) connected to several Cisco 2960 switches and a server (GS-323XP).
- London (Orange):** Contains a central HP ProCurve Switch 2911 (Id: 483) connected to several Cisco 2960 switches and a wireless access point (CN20031671).
- Rome (Blue):** Contains a central HP ProCurve Switch 2911 (Id: 483) connected to several Cisco 2960 switches and a wireless access point (CN20031671).

Interconnections are shown as green lines between the central switches of the Berlin, Paris, and Rome sites. The London site is also connected to the Paris site. A search filter is visible on the right side of the interface, showing checked options for "Network device", "Network device IP", "Network device group", "Location", and "VLANs".

Dashboard – alles auf einen Blick

Dashboard (macmon - Demo)

Search 56:57

- Endpoints
- User
- Network
- Policies
- Compliance
- Reports
- Past Viewer
- Scalability
- Statistics
- Status
- Settings
- Help

Summary of Events

12:04:06 (690 ms)

Network status

Status	Object	Value	Details
🟡	Corporate devices	9 / 10	Deactivated corporate devices: 1
🔴	Unauthorized endpoints	164 / 391	164 online/391 total
🟢	Guest devices	0 / 0	0 guest devices online/0 guest devic...
🟢	BYOD devices	0 / 0	0 BYOD endpoints online/0 BYOD en...
🟢	Events	283	283 events processed in the last hour

12:06:06 (379 ms)

Overall Compliance

12:07:08 (354 ms)

Last compliance Issues

Source	Reason	MAC	Status	Change	Group
Flowmon	Behavior anomaly - Priority: Medium - Description: Number of replies in t...	00-DC-29-E3-15-D4	almost noncompliant	20. Oct 21:12	AccessPoint
Flowmon	Attack	00-0C-29-46-56-81	noncompliant	17. Sep 08:31	
baramundi	UpToDate	00-0C-29-47-D0-83	compliant	08. Jul 12:27	Default
baramundi	Old-Software	00-19-89-0F-DF-36	noncompliant	05. Jul 10:49	PC
baramundi	Old-Software	00-18-8B-21-70-15	noncompliant	05. Jul 10:48	PC
baramundi	Not-Compliant	00-00-74-EA-7D-F2	noncompliant	05. Jul 10:47	Printer
baramundi	Not-Compliant	00-0C-29-6A-83-EA	noncompliant	05. Jul 10:47	Default
baramundi	Not-Compliant	00-0E-7F-DE-1D-86	noncompliant	05. Jul 10:47	Printer
baramundi	missing_patches	00-0C-29-2C-57-64	noncompliant	05. Jul 10:46	Default
baramundi	missing_patches	00-0C-29-32-86-D0	noncompliant	05. Jul 10:46	Default

12:08:09 (365 ms)

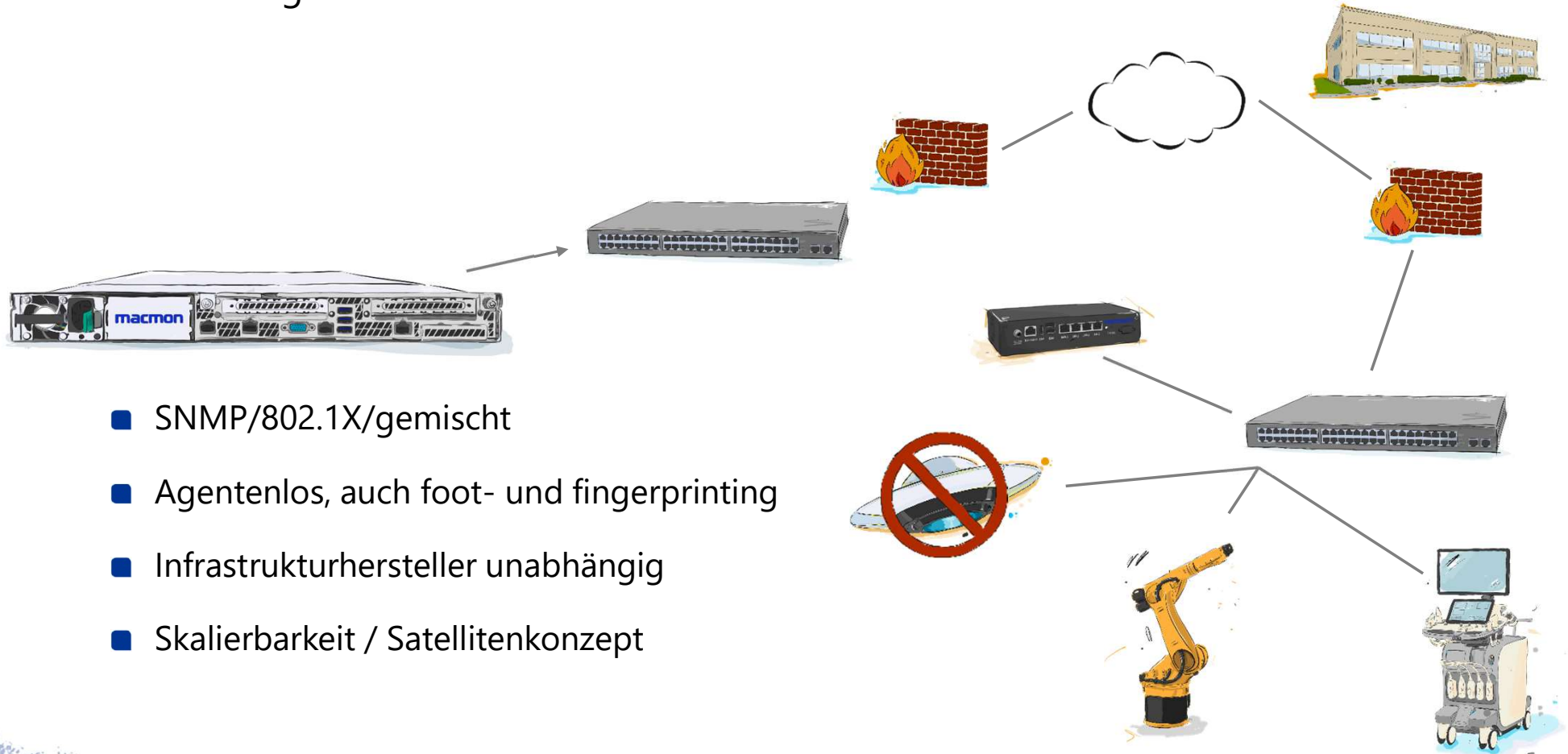
Last denied Authentication

MAC	Identity	RADIUS server	Access granted	Access time	Certificate owner	Access type	Authenticat
No entries available							

12:23:45 (378 ms)

Steuerung der Zugänge

Schützen Sie alle eingesetzten Geräte in Ihrem Netzwerk



- SNMP/802.1X/gemischt
- Agentenlos, auch foot- und fingerprinting
- Infrastrukturhersteller unabhängig
- Skalierbarkeit / Satellitenkonzept

Dynamisches Regelwerk

The screenshot displays the 'Manage NAC policies (macmon - Demo)' interface. It features a dark blue sidebar on the left with navigation options: Endpoints, User, Network, Policies (with sub-items: Events, GUI, NAC, RADIUS (non NAC), Guest portal), Compliance, Reports, Past Viewer, Scalability, Statistics, Status, Settings, and Help. The main content area has tabs for 'Authentication', 'Rules', and 'Permissions', with 'Rules' selected. An 'Add rule' button is present. Below is a table of active rules:

Actions	Status	Name	Description	Result
	active	Deny guest access for endpoints that were not registered by the guest themselves	Guests can process 802.1X authorizations with their own guest devices only	
	active	No NAC for the CEO	The CEO should never be handled via NAC Standard authorization	1 Permission(s)
	active	Guest VLAN	Meeting rooms only uses guest VLAN	1 Permission(s)
Hide built-in rules				
	active	Default rule for enforcement configuration of compliance, endpoints and endpoint groups.		
	active	Move unknown and deactivated endpoints to unauthorized VLAN.		
	active	Access deny		

Zugangsverwaltung

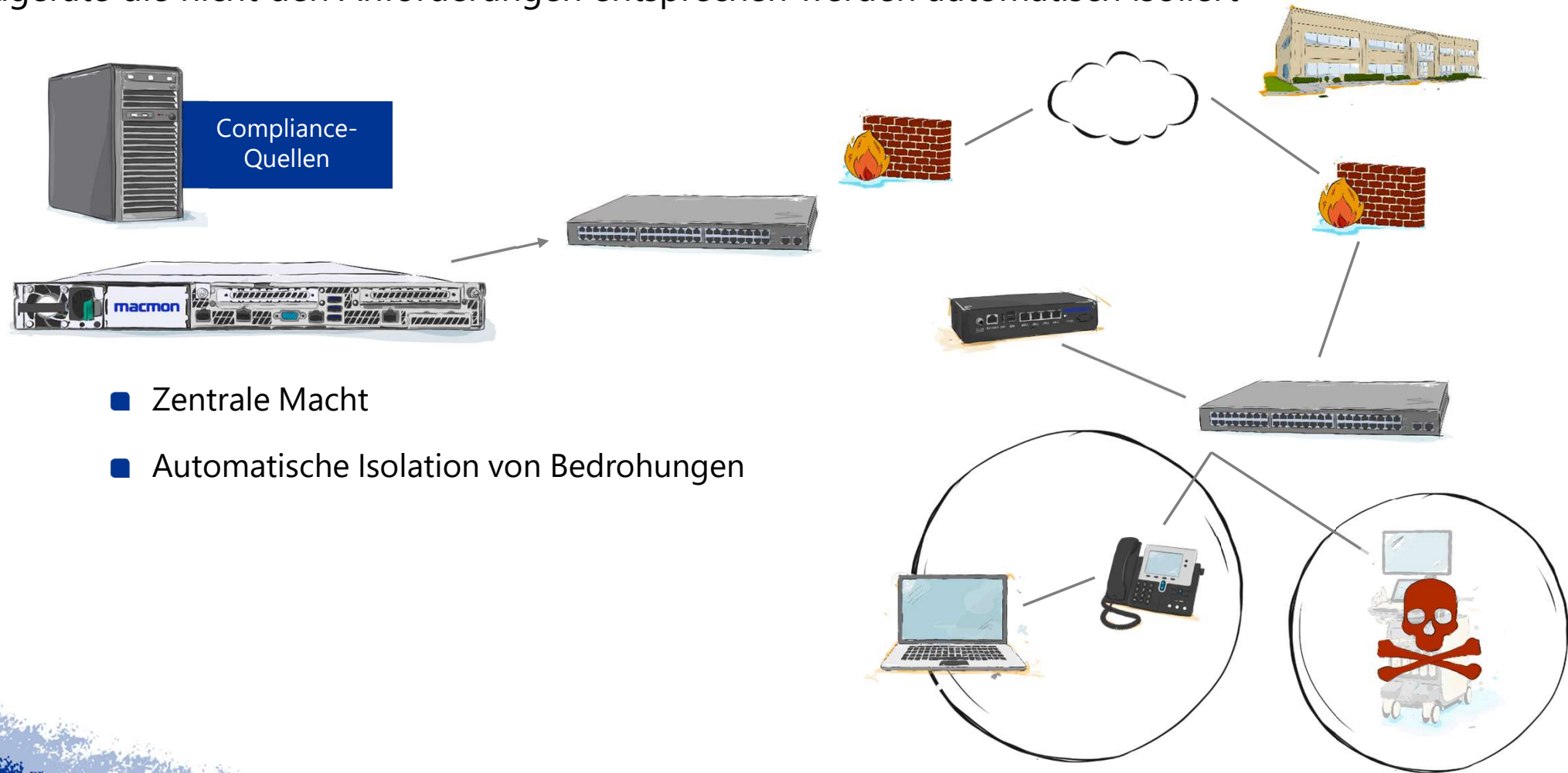
Neue Geräte werden mit notwendigen Zugängen versorgt



- VLAN-Konzepte & Sicherheitszonen
- Dynamisch, automatisch und in jeder Umgebung

Zugangsverwaltung

Endgeräte die nicht den Anforderungen entsprechen werden automatisch isoliert



Compliance-Report

mac **Reports (macmon - Demo)** 2022-03-22 12:24:15 CET
Version 5.30.1-50261

Authorized MACs **510** Unauthorized MACs **390** Detected MACs **413** Client Compliance macmon-Agents IP-MAC assignments Advanced Security

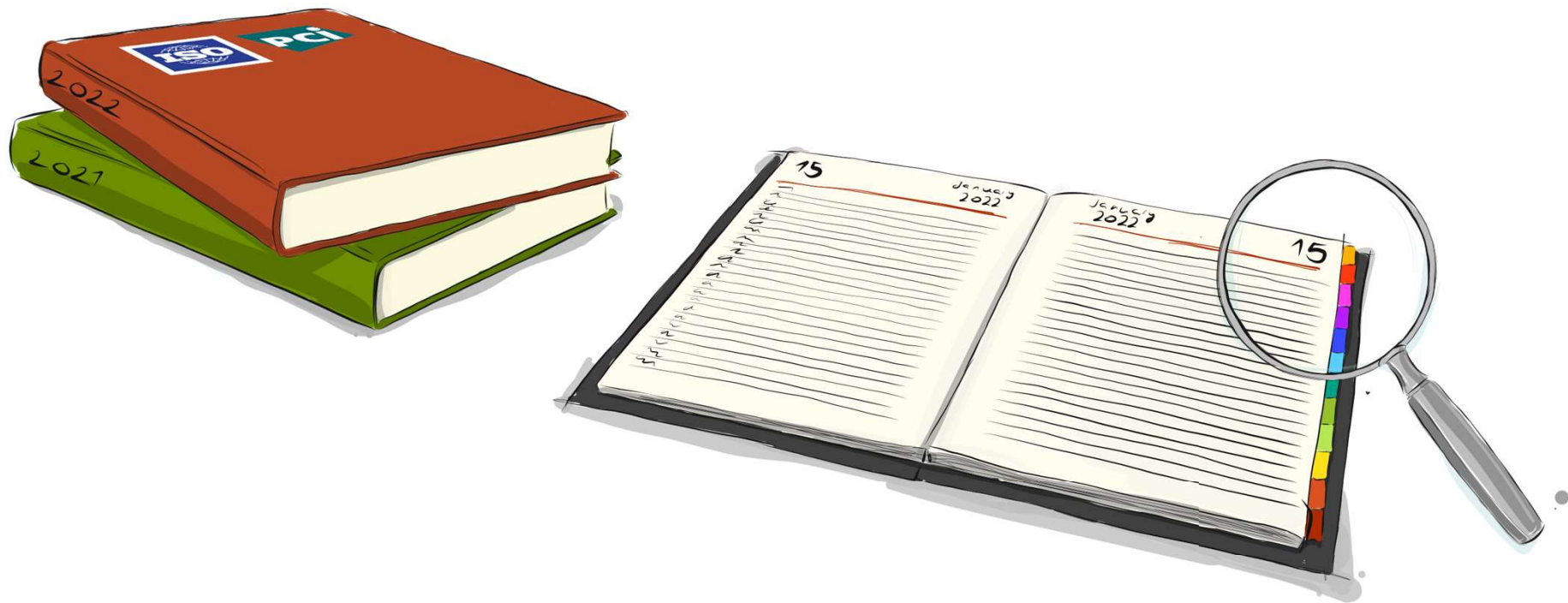
View Graphic 20 1-20 of 50

MAC	Last IP	Last DNS name	Host name (DHCP)	Group	Status	Source	Reason	MAC online	MAC in ARP	Change
00-00-71-00-00-77				Network	non-compliant	Barracuda	Joint_a_Botnet			2019-02-08 16:10:27
00-00-71-00-00-77				Network	non-compliant	EgoSecure	Application			2018-03-08 17:42:38
00-00-71-00-00-77				Network	compliant	macmon-agent	Firewall aktiviert			2019-03-25 10:36:00
00-00-74-EA-7D-F2				Printer	non-compliant	baramundi	Not-Compliant			2021-07-05 10:47:02
00-00-74-F1-DF-60				Printer	non-compliant	SophosCentral	real_time_protection_inactive			2020-04-30 11:24:30
00-01-2E-2B-A3-0A				PC	non-compliant	Extrahop	Several_DB_Login_Attempts			2018-03-08 17:42:39
00-0C-29-2C-57-64				Default	non-compliant	baramundi	missing_patches			2021-07-05 10:46:01
00-0C-29-32-B6-D0				Default	non-compliant	baramundi	missing_patches			2021-07-05 10:46:01
00-0C-29-46-56-81	10.10.10.99	openldap.example.local,			non-compliant	Flowmon	Attack			2021-09-17 08:31:21
00-0C-29-47-DD-83				Default	compliant	baramundi	UpToDate			2021-07-08 12:27:13
00-0C-29-48-CC-23				Default	non-compliant	EgoSecure	Forbidden_Application			2019-02-08 16:10:28
00-0C-29-48-CC-23				Default	non-compliant	Extrahop	Ransomware			2018-03-08 17:42:39
00-0C-29-6A-83-EA				Default	non-compliant	baramundi	Not-Compliant			2021-07-05 10:47:02
00-0C-29-8C-42-22				Default	non-compliant	EgoSecure	"Unknown USB dongle"			2018-03-08 17:42:39
00-0C-29-8C-42-22				Default	compliant	McAfee	up-to-date and running			2018-03-08 17:42:39
00-0C-29-B4-2E-8A				Default	non-compliant	Trend Micro	Malware found			2018-03-08 17:42:39
00-0C-29-B6-86-3E				Default	non-compliant	Barracuda	Joint_a_Botnet			2019-02-08 16:10:31
00-0C-29-B6-86-3E				Default	non-compliant	Extrahop	Several_DB_Login			2018-03-08 17:42:39
00-0C-29-E3-15-D4	10.10.10.2	test02win.example.local,		AccessPoint	almost non-compliant	Flowmon	Behavior anomaly - Priority: Medium - Description: N...	yes	yes	2020-10-20 21:12:46
00-0E-7F-DE-1D-86				Printer	non-compliant	baramundi	Not-Compliant			2021-07-05 10:47:02

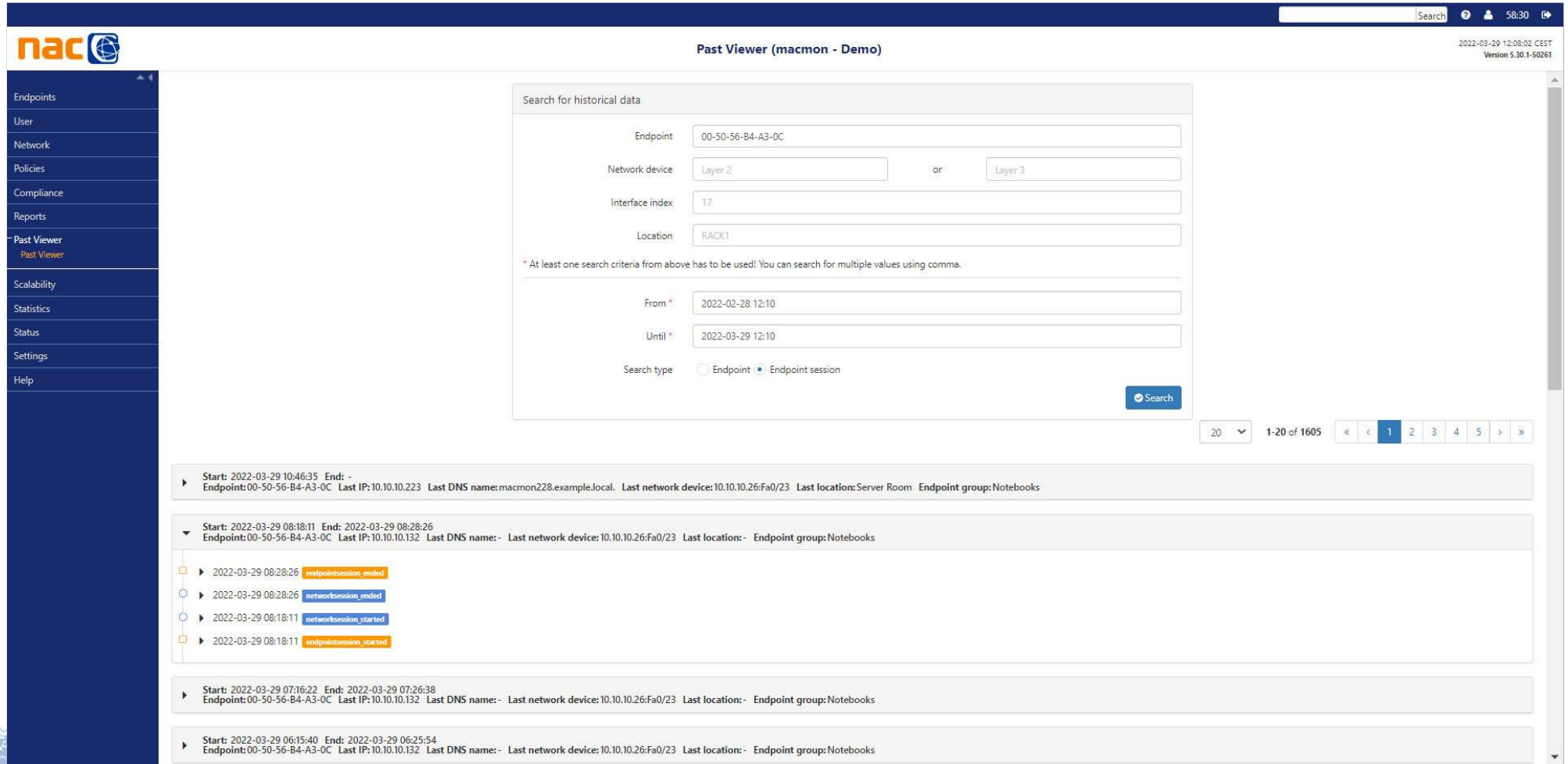
1-20 of 50

Past Viewer

Wer war wann, wo und mit welcher IP und welchem Namen im Netzwerk?



Past Viewer



The screenshot shows the 'Past Viewer (macmon - Demo)' interface. On the left is a dark blue navigation sidebar with the 'nac' logo at the top and menu items: Endpoints, User, Network, Policies, Compliance, Reports, Past Viewer (highlighted), Scalability, Statistics, Status, Settings, and Help. The main content area has a search form titled 'Search for historical data' with fields for Endpoint (00-50-56-B4-A3-0C), Network device (Layer 2 or Layer 3), Interface index (17), and Location (RACK1). Below these are 'From' (2022-02-28 12:10) and 'Until' (2022-03-29 12:10) date pickers, and a 'Search type' section with radio buttons for 'Endpoint' and 'Endpoint session'. A 'Search' button is at the bottom right of the form. A note states: '* At least one search criteria from above has to be used! You can search for multiple values using comma.' Below the search form is a pagination control showing '1-20 of 1605' and page numbers 1 through 5. The results section displays four entries, each with a start/end time, endpoint, last IP, last DNS name, last network device, last location, and endpoint group. The second entry is expanded to show a sequence of events: endpoint session ended, network session ended, network session started, and endpoint session started.

Search for historical data

Endpoint: 00-50-56-B4-A3-0C

Network device: Layer 2 or Layer 3

Interface index: 17

Location: RACK1

* At least one search criteria from above has to be used! You can search for multiple values using comma.

From: 2022-02-28 12:10

Until: 2022-03-29 12:10

Search type: Endpoint Endpoint session

Search

20 1-20 of 1605 1 2 3 4 5

Start: 2022-03-29 10:46:35 End: -
Endpoint: 00-50-56-B4-A3-0C Last IP: 10.10.10.223 Last DNS name: macmon228.example.local Last network device: 10.10.10.26:Fa0/23 Last location: Server Room Endpoint group: Notebooks

Start: 2022-03-29 08:18:11 End: 2022-03-29 08:28:26
Endpoint: 00-50-56-B4-A3-0C Last IP: 10.10.10.132 Last DNS name: - Last network device: 10.10.10.26:Fa0/23 Last location: - Endpoint group: Notebooks

- 2022-03-29 08:28:26 endpoint session ended
- 2022-03-29 08:28:26 network session ended
- 2022-03-29 08:18:11 network session started
- 2022-03-29 08:18:11 endpoint session started

Start: 2022-03-29 07:16:22 End: 2022-03-29 07:26:38
Endpoint: 00-50-56-B4-A3-0C Last IP: 10.10.10.132 Last DNS name: - Last network device: 10.10.10.26:Fa0/23 Last location: - Endpoint group: Notebooks

Start: 2022-03-29 06:15:40 End: 2022-03-29 06:25:54
Endpoint: 00-50-56-B4-A3-0C Last IP: 10.10.10.132 Last DNS name: - Last network device: 10.10.10.26:Fa0/23 Last location: - Endpoint group: Notebooks

Past Viewer

Corporate devices (macmon - Demo) 2022-03-22 12:31:17 CET
Version 5.30.1-50261

Corporate device details: 00-50-56-B4-A3-0C
Registered: 2021-02-25 16:58:41 Last change: 2021-11-04 09:29:19
[Back to corporate device list](#) [Action](#)

Common

Manufacturer	VMWARE !
Group	Notebooks
Inactive	<input type="checkbox"/>
Endpoint/Identity Store	00-50-56-B4-A3-0C / LocalDatabase
User/Identity Store	-
Valid until	
Inventory No.	
Comment	
First seen	2021-03-17 15:35:16
Last seen	2022-03-22 12:31:18
Last IP	10.10.10.237 Ping: 0.410 ms
Last DNS name	macmon.example.local.
Service	
Team account / Kostenstelle	
802.1X User	
PPSK	
Preset IP address	
Permitted VLANs	
MAB password	00-50-56-B4-A3-0C

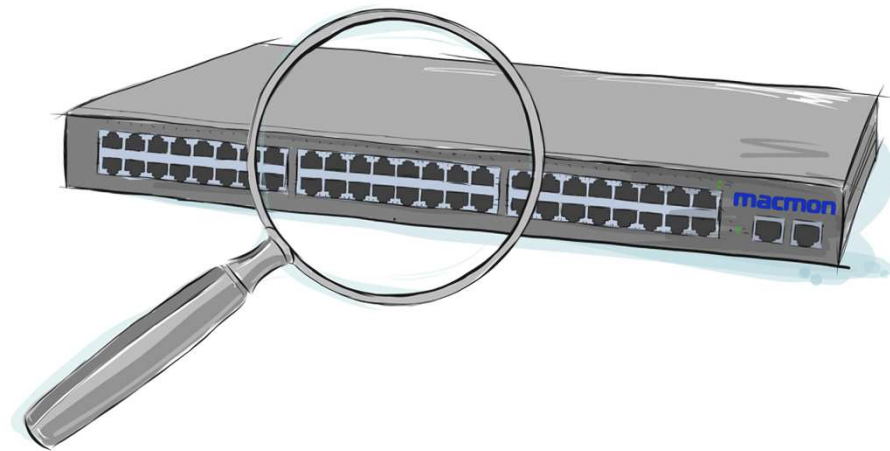
[Save changes](#) [Abort](#)

Status **Interfaces** ARP, DNS and DHCP Advanced Security **Past Viewer** Other

- Start: 2022-03-22 03:54:46 End: -
Last IP: 10.10.10.237 Last DNS name: macmon.example.local. Last network device: 10.10.10.26 Last location: -
 - 2022-03-22 03:54:46 **networksession_started**
 - 2022-03-22 03:54:46 **endpointsession_started**
- Start: 2022-03-20 15:41:55 End: 2022-03-22 03:51:32
Last IP: 10.10.10.237 Last DNS name: macmon.example.local. Last network device: 10.10.10.26:Fa0/23 Last location: -
 - 2022-03-22 03:51:32 **endpointsession_ended**
 - 2022-03-22 03:51:32 **networksession_ended**
 - 2022-03-20 15:41:55 **networksession_started**
 - 2022-03-20 15:41:55 **endpointsession_started**
- Start: 2022-03-19 15:32:25 End: 2022-03-20 15:39:43
Last IP: 10.10.10.237 Last DNS name: macmon.example.local. Last network device: 10.10.10.26:Fa0/23 Last location: -
 - 2022-03-20 15:39:43 **endpointsession_ended**
 - 2022-03-20 15:39:43 **networksession_ended**
 - 2022-03-19 15:32:25 **networksession_started**
 - 2022-03-19 15:32:25 **endpointsession_started**
- Start: 2022-03-11 02:22:28 End: 2022-03-19 15:31:13
Last IP: 10.10.10.237 Last DNS name: macmon.example.local. Last network device: 10.10.10.26:Fa0/23 Last location: -
- Start: 2022-03-07 16:53:17 End: 2022-03-11 02:21:17
Last IP: 10.10.10.237 Last DNS name: macmon.example.local. Last network device: 10.10.10.26:Fa0/23 Last location: -

Switch Viewer

Schnell erfassbare Details über den Ist-Zustand



Switch Viewer

Search
59:41

Details for file:virt/Paris_Core (macmon - Demo)
2022-03-22 14:00:25 CET
Version 5.30.1-50261

Endpoints

User

Network

- Network devices
- Device groups
- Device classes
- Manually stated links
- Network segments
- Device suggestions
- Link suggestions
- Network device discovery
- Test dialog scripts
- Topology

Policies

Compliance

Reports

Past Viewer

Scalability

Statistics

Status

Settings

Help

◀ To network device list
Action ▾
🖨

Common

Network device:	file:virt/Paris_Core
Network device address:	file:virt/Paris_Core ↗
ID:	134
Resolved IP:	- / -
Further IP addresses:	10.10.7.1/24, 10.10.8.1/24, 10.10.9.1/24, 10.10.10.1/24, 10.10.11.1/24, 10.10.13.1/24, 10.10.14.1/24, 10.10.15.1/24, 10.100.0.1/16, 10.100.7.30/24, 127.0.0.1/32, 172.20.0.1/16, 192.168.101.1/24, 192.168.102.2/24, 192.168.110.222/24
snmp-SYSNAME	HP ProCurve Switch 2910al-48G
Scan:	▶ Yes
NAC (SNMP):	inactive
Network device class:	HP ProCurve Switch 2910al-48G (J9147A)
Network device group:	Switch Paris
Description:	
Location:	
Ignore new hardware:	✘ No
802.1X status:	inactive
Statistics enabled:	✔ Yes
Serial numbers:	

Status overview 🔄
Action status
Statistics
VLANs
Credentials
SNMP
MIB probe

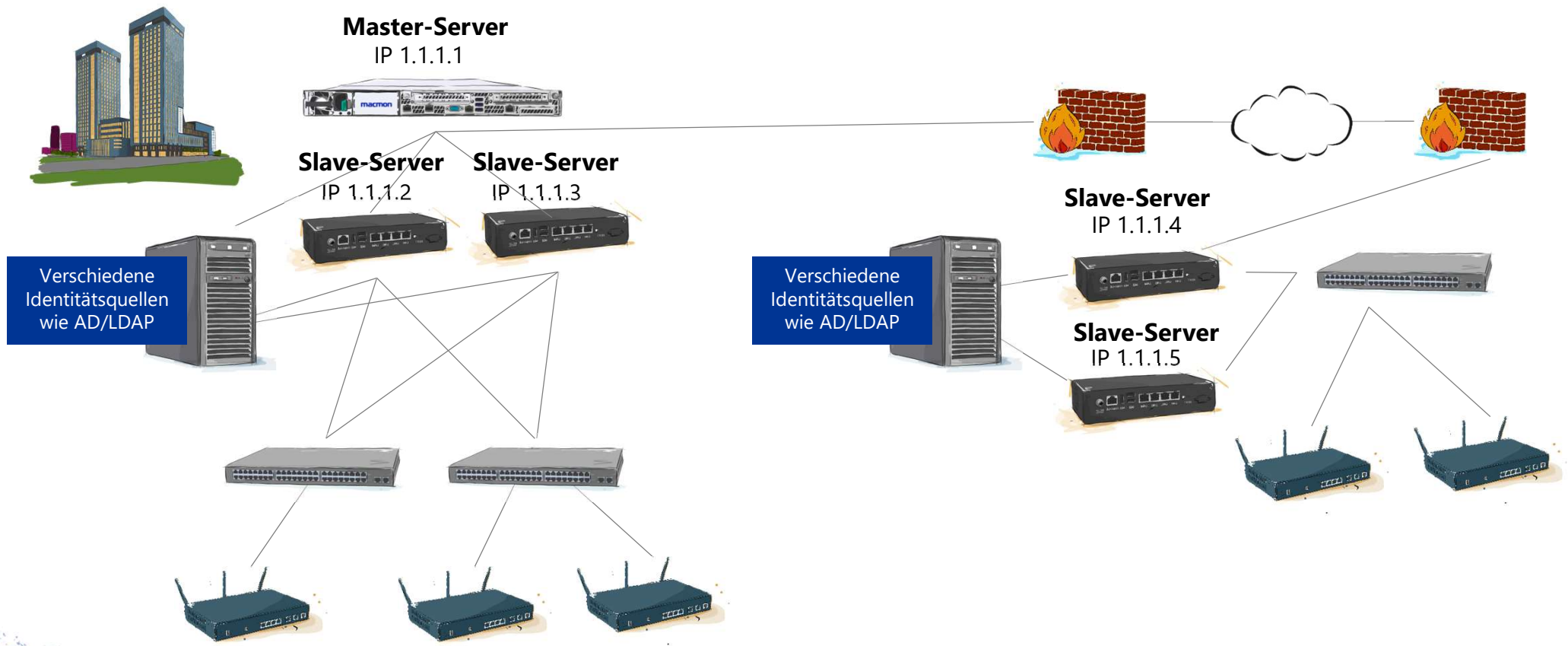
Status ✔

Last scan	2022-03-22 14:00:11 (vertriebsdemo50)
Duration of the last scan	25ms
Scan interval	1 Minute, 0.18 Seconds
Last trap	-
Last RADIUS request	-
Neighbors	➕ file:virt/Berlin_Core1 / 12 cdp
Live check:	Cannot be performed for file-based network devices.

HP ProCurve Switch 2910al-48G (J9147A) | chassis 0

Scalability

Beispielhaftes Set-Up für eine verteilte und hochverfügbare Umsetzung



Scalability

macmon Search 58:12

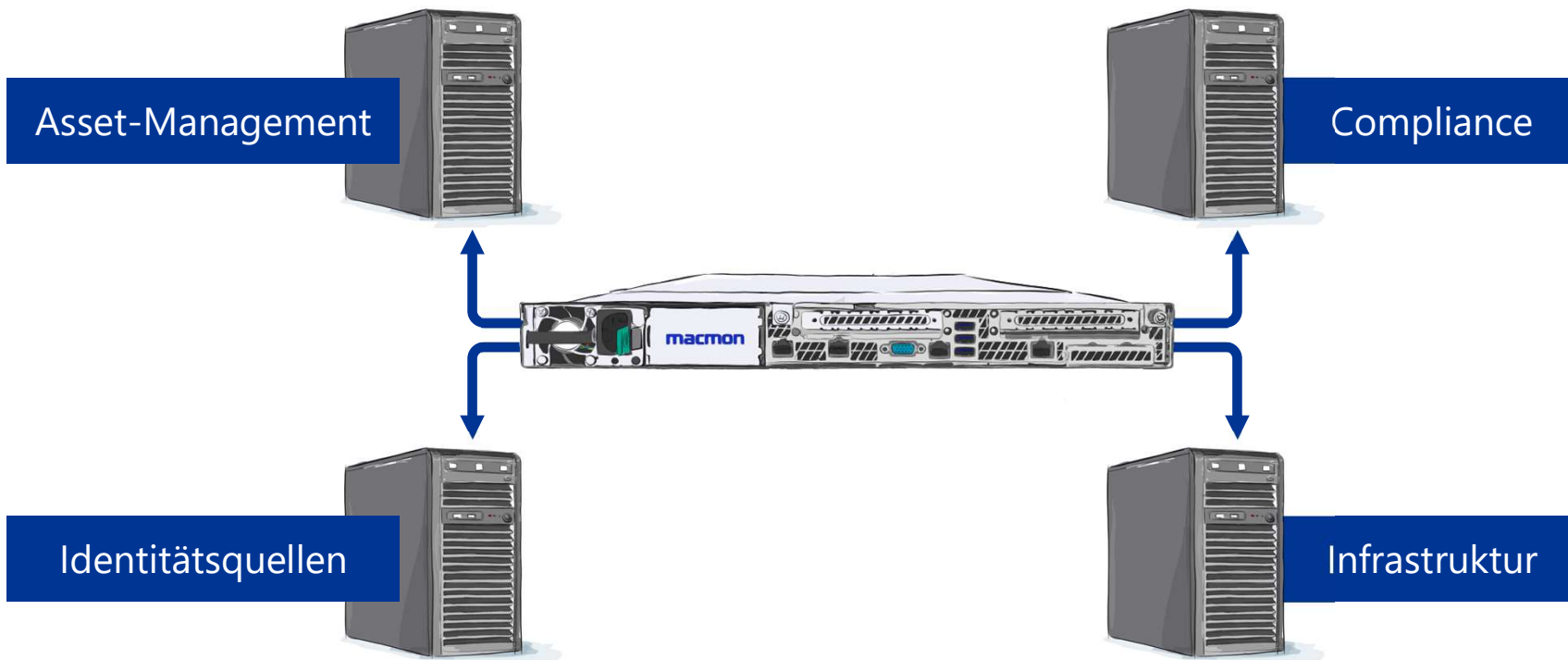
Servers (macmon - Demo) 2022-03-29 12:12:40 CEST
Version 5.30.1-50261

Endpoints
User
Network
Policies
Compliance
Reports
Past Viewer
Scalability
Servers
Statistics
Status
Settings
Help

Server name	IP address	Role	Status	Last error
macmon19	10.10.30.19	SLAVE	Connected	
macmon15	10.10.30.15	SLAVE	Connected	
macmon11	10.10.30.11	SLAVE	Connected	
macmon8	10.10.30.8	SLAVE	Connected	
macmon6	10.10.30.6	SLAVE	Connected	
macmon17	10.10.30.17	SLAVE	Connected	
macmon18	10.10.30.18	SLAVE	Connected	
macmon25	10.10.30.25	SLAVE	Connected	
macmon28	10.10.30.28	SLAVE	Connected	
macmon24	10.10.30.24	SLAVE	Connected	
macmon20	10.10.30.20	SLAVE	Connected	
macmon22	10.10.30.22	SLAVE	Connected	
macmon9	10.10.30.9	SLAVE	Connected	
macmon12	10.10.30.12	SLAVE	Connected	
macmon23		SLAVE	Disconnected	
macmon10	10.10.30.10	SLAVE	Connected	
macmon21	10.10.30.21	SLAVE	Connected	
macmon26	10.10.30.26	SLAVE	Connected	
macmon7	10.10.30.7	SLAVE	Connected	

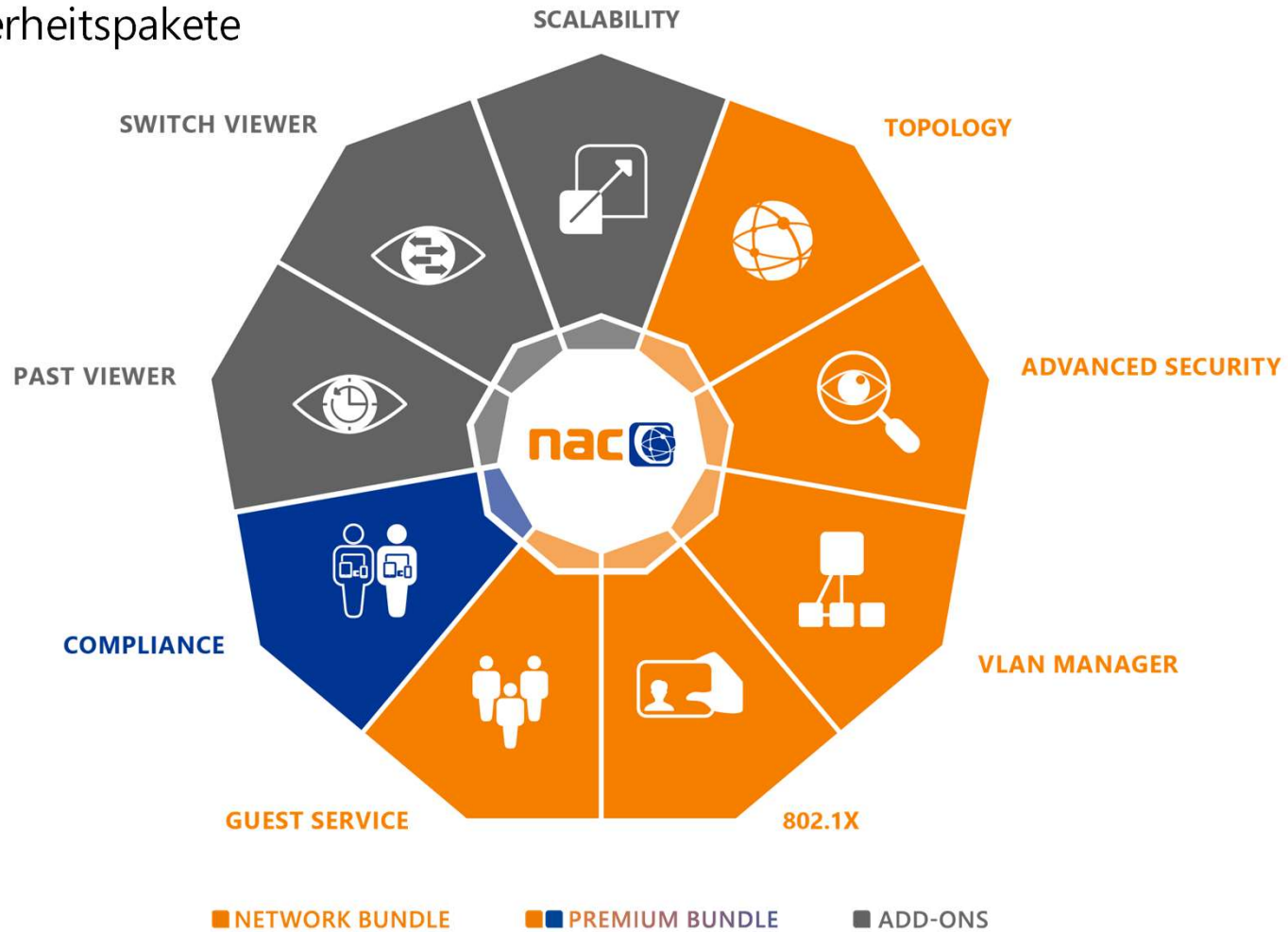
macmon-Technologiepartner

Koppeln Sie macmon NAC mit führenden Sicherheitslösungen



macmon Kernfunktionen

Abgestimmte Sicherheitspakete



Kunden über die Vorteile von macmon NAC

1 Sofortige Netzwerkübersicht mit grafischen Reports & Topologie

2 Einführung innerhalb eines Tages & intuitives tägliches Handling

3 Mischbetrieb mit und ohne 802.1X

4 Intelligente AD Integration mit dynamischem Regelwerk

5 Einfache und effektive Netzwerksegmentierung

6 Hoch flexibles Gästeportal

7 Sinnvolle Integrationen mit anderen Security-Produkten

8 Herstellerunabhängigkeit

9 NAC-Lösung mit deutschem Hersteller-Support

Kundenbeispiele – Industrie

Wichtige Faktoren

Roboter und Maschinen können nicht mit üblichen Mitteln (Virenschutz, Patches, ...) geschützt werden

Dienstleister müssen für Störungsbeseitigungen und Wartungsarbeiten Zugang zum Netz haben

Sicherheitsvorfälle können Sach- und Personenschäden bewirken

Produktionsnetze „wachsen“ oft unkontrolliert, da proprietäre Kommunikationssysteme (Feldbus, Interbus, Profibus, ...) zunehmend durch Ethernet ersetzt werden



AEB

VORWEG GEHEN

MBDA
MISSILE SYSTEMS

Kundenbeispiele – Gesundheitswesen

Wichtige Faktoren

Medizinisches IT-Netzwerk und allgemeines IT-Netzwerk müssen getrennt werden
(DIN EN 80001-1, Risikomanagement für IT-Netzwerke mit Medizinprodukten)

Schutz der Arzt-Patientenbeziehung bzw. Wahrung des Patientengeheimnisses
(ärztl. Schweigepflicht, § 203 StGB)

Für private Träger: Beim Rating von Basel II (künftig auch EURO-SOX), ist die
IT-Infrastruktur direkt an die Erteilung von Finanzmitteln durch Banken gekoppelt;
Defizite in der IT-Sicherheit führen i.d.R. zur Kürzung der Kreditlinie

Das IT-Netzwerk wird durch die Einbindung von Medizinprodukten zu einem medizinischen
IT-Netzwerk und fällt somit in den Zuständigkeitsbereich des Medizinproduktegesetzes (MPG)



Kundenbeispiele – Banken & Versicherungen

Wichtige Faktoren



Geldautomaten und andere NAC-GAP Geräte im Netz sind in die Sicherungsmaßnahmen einzubeziehen

Sicherung öffentlicher Bereiche mit Publikumszugang ist erforderlich

Die ausgeprägte Filialstruktur kann durch eine Live-Überwachung effektiv kontrolliert werden

Payment Card Industry Compliance (PCI)

Reduzierung und Fokussierung auf den entscheidenden Scope

Kundenbeispiele – Wissenschaft & Forschung

Wichtige Faktoren

Innovationen deutscher Forschungs- und Entwicklungseinrichtungen sind begehrtes Ziel von wissenschaftlicher und wirtschaftlicher Konkurrenz

Sicherheitsvorfälle können Abfluss von Know-How und Forschungsdaten bewirken, und damit mittelbar auch die Wettbewerbsfähigkeit gefährden

Gaststudenten/Gastwissenschaftler, Gäste und externe Mitarbeiter bedürfen abgestufter Zugangs- und Zugriffsberechtigungen

Die Live-Überwachung erleichtert die Kontrolle und Steuerung in weit gefächerten Organisationsstrukturen, auch weltweit

macmon ermöglicht die Administration mit wenig Personalkapazität



Kundenbeispiele – Behörden

Wichtige Faktoren



STADT ESSLINGEN AM NECKAR



Landkreis
Sigmaringen



Klare Anforderungen des BSI sind zu erfüllen

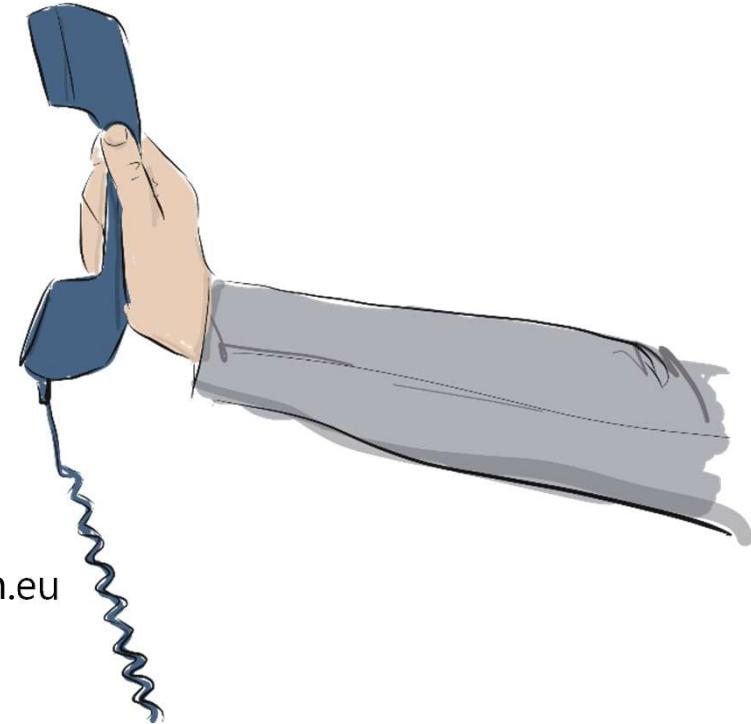
macmon ermöglicht die Administration mit wenig Personalkapazität

Die Live-Überwachung erleichtert die Kontrolle und Steuerung in weit gefächerten Organisationsstrukturen, auch weltweit

Aus der Verarbeitung sensibler, oft personenbezogener Daten resultiert ein besonders hoher Schutzbedarf

Kontakt

Zero Trust, but one: macmon



macmon secure GmbH

Alte Jakobstr. 79-80 | 10179 Berlin

+49 30 23 25 777-0 | vertrieb@macmon.eu

www.macmon.eu

