

Matrix42 Endpoint Security

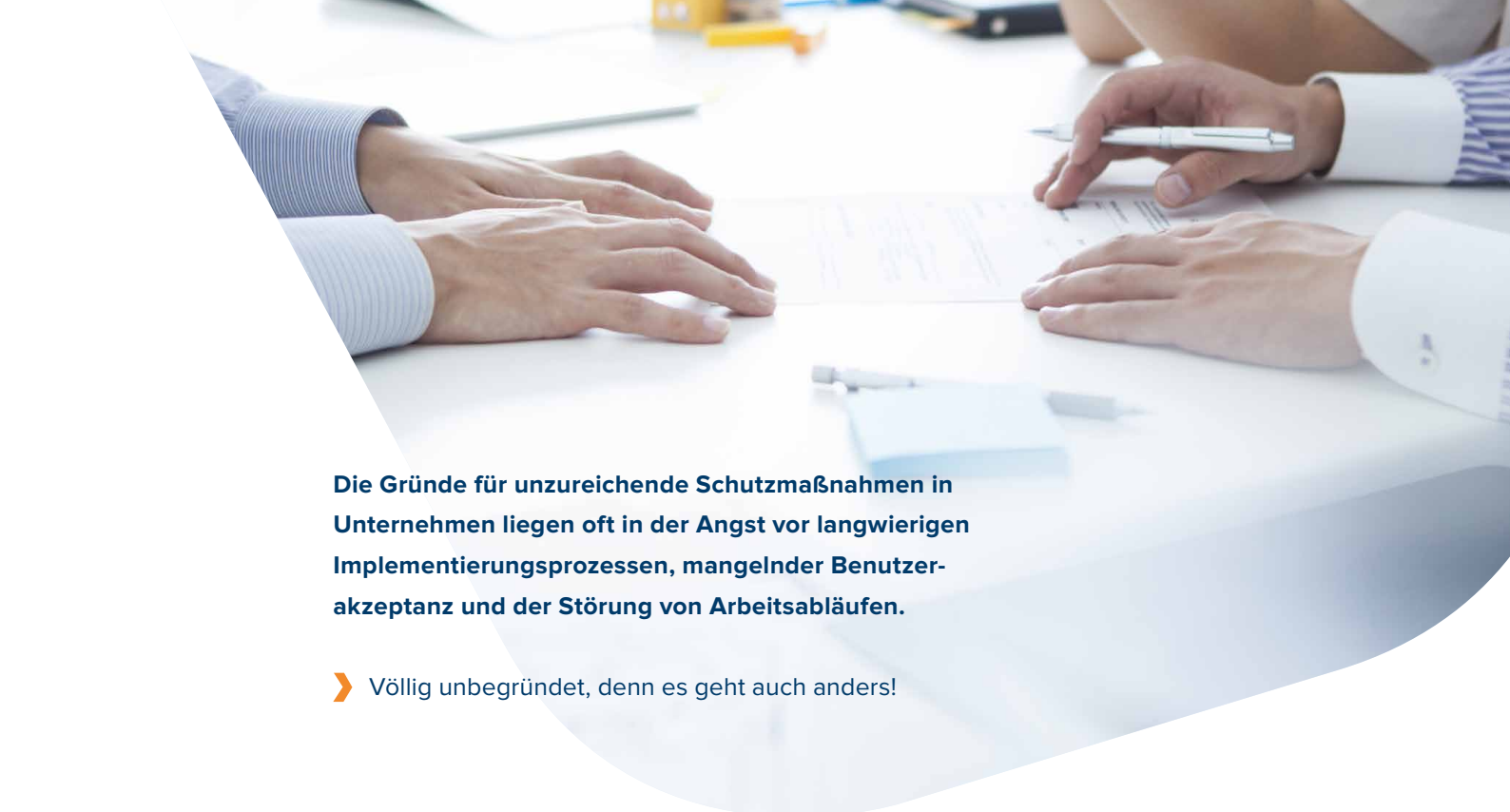
Sicherheitslücken schließen
und Daten schützen



Endpoint Security – ein heißes Thema

Die digitale Vernetzung und die Zunahme an Gerätevielfalt bieten nicht nur mehr Möglichkeiten, Malware einzuschleusen, sondern auch Daten auszuschleusen und zu stehlen. Herkömmliche Schutzkonzepte aus Firewall und Antivirenlösung reichen längst nicht mehr aus, um Sicherheitslücken zu schließen.

- › **67% der deutschen Unternehmen** wurden bereits erfolgreich attackiert. Dabei entstehen 37% der Sicherheitsvorfälle in Organisationen durch menschliche Fehler, 34% durch nicht ausreichend gesicherte Endpoints.¹
- › **Alle 40 Sekunden** kommt es im Schnitt zu einer Ransomware-Attacke. Zukünftig wird mit Angriffen in einem 14-sekündigen Rhythmus und globalen Schadenskosten von rund 11,5 Milliarden US-Dollar gerechnet.² Durch die Einzigartigkeit gezielt programmierter Ransomware bieten Antivirenlösungen meist keinen Schutz gegen derartige Attacken, da nur bekannte Schadsoftware gefiltert werden kann.
- › **55 % aller Datensicherheitsverletzungen** basieren auf Verstößen gegen Compliance-Richtlinien.³ Gleichzeitig haben 70% der Unternehmensmitarbeiter mehr Benutzerrechte als sie zur Ausübung ihrer Funktion bräuchten.⁴



Die Gründe für unzureichende Schutzmaßnahmen in Unternehmen liegen oft in der Angst vor langwierigen Implementierungsprozessen, mangelnder Benutzerakzeptanz und der Störung von Arbeitsabläufen.

› Völlig unbegründet, denn es geht auch anders!

Matrix42 Endpoint Security passt sich an Unternehmensprozesse an, ist einfach zu bedienen und bietet zugleich ein hohes Maß an Sicherheit.



All-in-one Lösung für Ihre Datensicherheit:

Alle Funktionen sind in ein Gesamtkonzept integriert und lassen sich an Ihren Unternehmensbedarf anpassen.



Zuverlässiger Systemschutz im Hintergrund:

Gewohnte Arbeitsabläufe werden nicht gestört



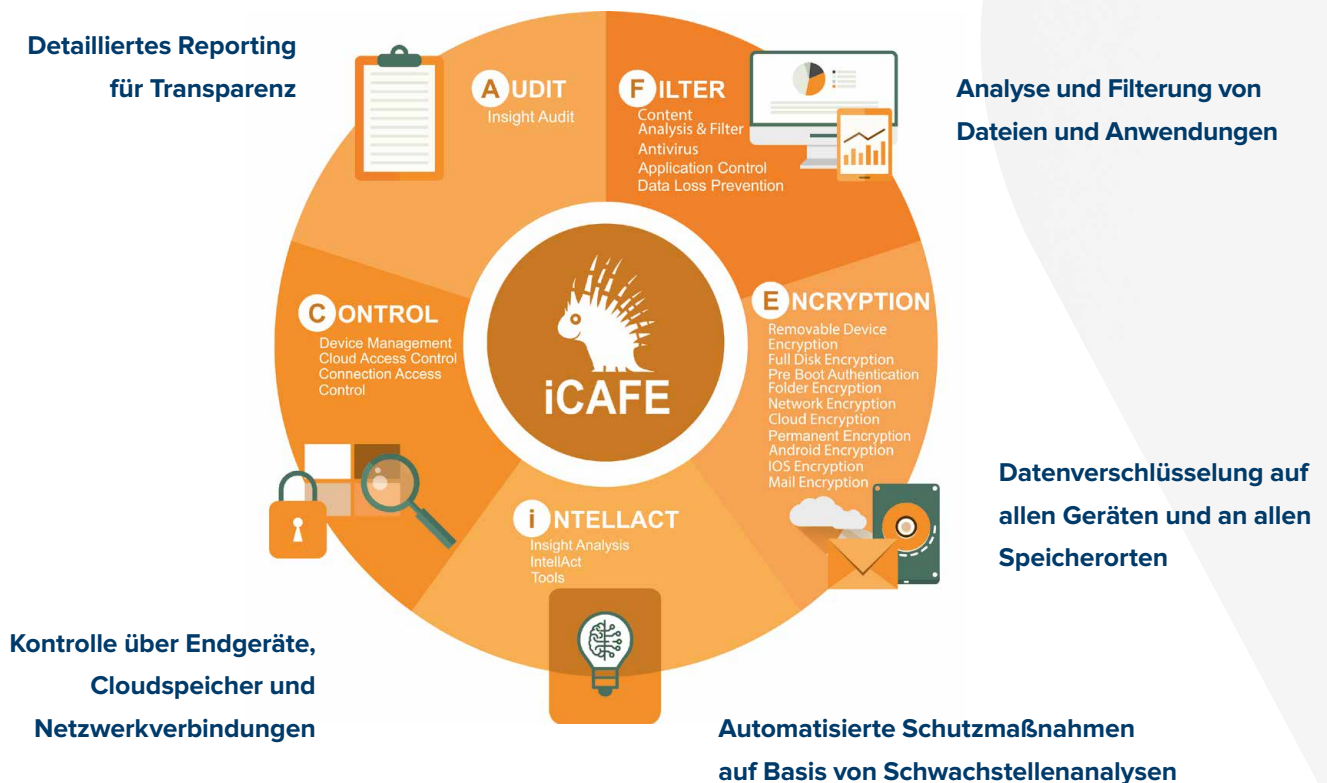
Sehr geringer Administrationsaufwand:

Schnelle Implementierung und einfache Bedienung

Alles läuft
wie bisher,
aber sicher.

Matrix42 Endpoint Security – eine ganzheitliche Lösung

Matrix42 Endpoint Security ist eine modulare Rundumlösung, die mit zahlreichen Sicherheitsfeatures zum Schutz Ihrer Geräte, Systeme und Daten ausgestattet ist. Dank der einfachen Bedienung sind aufwendige und kostspielige Schulungsmaßnahmen nicht erforderlich.



Hauptmerkmale der Lösung

- Zentrale Steuerung und Verwaltung über einen Server, eine Datenbank und eine Verwaltungskonsole
- Globales Rechtekonzept mit getrennter Rechteverwaltung für Computer und Benutzer
- Unterstützung von gängigen Verzeichnisdiensten und automatisierte Synchronisation von Verzeichnisdienstobjekten mit der Verwaltungskonsole
- Verwaltung von Offline-Clients
- Mandantenverwaltung
- Rollen- und Rechtekonzept für Administratoren



Hauptmerkmale der Module

› Access Control

Kontrolliert und steuert die Nutzung von Geräten (z. B. USB-Sticks, CDs, Drucker) oder Schnittstellen (z. B. Firewire, USB) auf Endpoints.

- › Getrennte Zugriffsverwaltung für Online- und Offline-Betrieb
- › Merkmalbasierte Freigabe einzelner Gerätemodelle und Gerätegruppen
- › Tastatur-/Mauskontrolle (Bad-USB-Schutz)
- › Kontrolle von Netzwerkverbindungen (WLAN, Antibridding)
- › Dateifilter zum Blockieren bestimmter Datenformate

› Secure Audit

Macht sämtliche Datenflüsse in der Systemlandschaft transparent, zeigt potenzielle Schwächen in den Schutzeinstellungen und bietet die Grundlage zur Ermittlung forensischer Informationen. So werden Compliance-Anforderungen erfüllt und das Erkennen unternehmensgefährdender Entwicklungen ermöglicht.

- › Protokollierung von Datenflüssen auf Endgeräten
- › Schutz der Protokolldaten nach 4- oder 6-Augen-Prinzip
- › Shadowcopy: Erstellt Schattenkopien aller Dateien, auf die ein Zugriff erfolgt ist

› Application Control

Verhindert, dass Schadsoftware durch unkontrollierte Installationen auf Endpoints in das Netzwerk gelangt. Der Anwendungsfilter verhindert außerdem, dass unlicenzierte Softwareprodukte genutzt werden und vermeidet so Haftungsrisiken und wirtschaftliche Schäden.

- › Granulare Rechtevergabe an Benutzer und Computer über Anwendungspakete
- › Global definierbare Liste vertrauenswürdiger Anwendungen
- › Zusätzliche Kontrolle von Programmbibliotheken (DLLs) und Java-Archiven (JARs)
- › Lernmodus erfasst ausgeführte Anwendungen am Endpoint

› Encryption

Verschlüsselt Speichermedien, Verzeichnisse, Clouds, einzelne Dateien oder ganze Festplatten, sodass nur berechtigte Personen darauf zugreifen können. Über eine mobile App lassen sich Daten auf externen Geräten und in Clouds auch auf mobilen Geräten oder Fremdsystemen entschlüsseln. Eine zusätzliche Authentifizierung schützt verschlüsselte Festplatten beim Ausbau der Hardware oder dem Umgehen der Windows-Anmeldung.

- › Removable Device Encryption
- › Local Folder Encryption
- › Network Share Encryption
- › Cloud Storage Encryption
- › Permanent Encryption
- › Full Disk Encryption
- › Pre Boot Authentication

› Insight Analysis & IntellAct Automation

Gibt per Mausklick eine grafisch aufbereitete Übersicht über sämtliche Datenflüsse im Netzwerk und löst passende Schutzmaßnahmen automatisch aus.

- › Darstellung und Auswertung sicherheitsrelevanter Vorgänge am Endpoint
- › Vorgangstatistik in grafischer und tabellarischer Form
- › Statistikberechnung für benutzerdefinierte Vorgänge
- › Definition von Regeln für Computer, Benutzer und Server, um passende Schutzmaßnahmen automatisch anzustoßen

› Data Loss Prevention

Durchsucht Dateien auf Endgeräten nach vorgegebenen Inhalten und Schlagworten und blockiert deren Abfluss, damit vertrauliche Daten wie z. B. Kreditkartennummern das Unternehmen nicht verlassen.

- › Unterstützung aller gängigen Dokumentformate und einer Vielzahl anderer Dateiformate
- › Suche in Echtzeit (externe Speichermedien) oder zeitgesteuert (Festplatten)
- › Globale, benutzerspezifische oder gruppenspezifische Regelzuweisung

› Antivirus

- › **Antivirus** integriert den reaktiven Virenschanner von BitDefender
- › **Avira Antivirus Management** zur zentralen Verwaltung von Avira-Clients über die Verwaltungskonsole

› Security Tools

- › **Secure Erase** zum sicheren Löschen von Daten auf Endpoints
- › **Password Manager** zum Speichern und Verwalten von Passwörtern in verschlüsselten Passwort-Containern
- › **Inventory** zur Auflistung und Überwachung installierter Hardware an Endpoints
- › **Green IT** zur effizienten Energienutzung an Endpoints
- › **BitLocker Management** zur Steuerung von Microsoft BitLocker über die Verwaltungskonsole

Bundles

| Endpoint Security Compliance | Endpoint Security Protection | Endpoint Security Prevention |
|---|---|---|
| Access Control, Audit, Application Control, Removable Device Encryption | Access Control, Audit, Application Control, Removable Device Encryption, Local Folder Encryption, Network Share Enc., Cloud Storage Enc., Full Disk Enc., Pre Boot Authentication | Access Control, Audit, Application Control, Removable Device Encryption, Local Folder Encryption, Network Share Enc., Cloud Storage Enc., Full Disk Enc., Pre Boot Authentication, Insight Analysis, IntellAct Automation |

Standorte

Hauptsitz Deutschland

Matrix42 AG
Elbinger Straße 7
60487 Frankfurt am Main
Deutschland
Telefon: +49 69 66773-8220
Fax: +49 69 66778-8657
info@matrix42.com

Niederlassung Schweiz und Österreich

Matrix42 Helvetia AG
Grabenstrasse 32
6300 Zug
Schweiz
Telefon: +41 41 720-4220
info@matrix42.ch

Weitere Niederlassungen im Ausland

finden Sie auf unserer Website:
www.matrix42.com

Über Matrix42

Matrix42 unterstützt Organisationen dabei, die Arbeitsumgebung ihrer Mitarbeiter zu digitalisieren. Die Softwarelösungen für Unified Endpoint Management, Software Asset- und Service Management sowie Endpoint Security verwalten Geräte, Anwendungen, Prozesse und Services einfach, sicher und richtlinienkonform.

Die Matrix42 AG hat ihren Hauptsitz in Frankfurt am Main, Deutschland, und vertreibt und implementiert Softwarelösungen weltweit mit lokalen und globalen Partnern.