Secure Unified Endpoint Management (SUEM)

Matrix42 Secure Unified Endpoint Management automatisiert den kompletten Prozess von der Inbetriebnahme eines Endgerätes, über das Ausrollen, Updaten und Patchen bis hin zur Absicherung der Endgeräte. Abhängig vom Betriebssystem wird dabei immer die optimale technische Verwaltungsmethode verwendet. Security ist hierbei immer integraler Bestandteil.

Module & Funktionen

Geräteübergreifendes Management

Empirum Client Lifecycle Management

- Zentralisierte Steuerung und Automation - von der Erstinstallation bis hin zum End-Of-Life-Management
- Verschaffen Sie sich Transparenz über alle Geräte und Anwendungen
- Lässt sich mit alternativen Softwareverteilungssystemen sowie dem gesamten Matrix42 Portfolio verbinden, um verschiedene inventarbezogene Aufgaben zu automatisieren und die Qualität von IT-Services stetig zu verbessern
- Komponenten: Inventory, Software Management, OS Installation, Personal Backup und Easy Recovery

Silverback Enterprise Mobility Management

- Einfache, skalierbare und sichere Geräteverwaltung von unter anderem Smartphones, Tablets, aber auch allen Geräten mit Betriebssystemen, wie Android, ChromeOS, iOS, iPadOS, macOS oder Windows 10
- Komponenten: Mobile Device Management, Mobile Application Management, Mobile Content Management

Security Built-in

Seamless Anywhere Encryption

- Transparente Verschlüsselung ohne Produktivitätsverlust
- Verschlüsselungsalgorithmen: AES-256 oder Triple DES-192 (nochmal mit bis zu RSA-4096 verschlüsselt)
- Schutz personenbezogener Daten gemäß EU-DSGVO Artikel 32
- Ent- und Verschlüsselung via Agent, nach definierten Unternehmensrichtlinien
- Datei-basierte Verschlüsselung oder Verschlüsselung ganzer Ordner in Cloud-Speichern (z. B. OneDrive, GoogleDrive, Dropbox), auf jedem beliebigen Netzwerk-Share oder auf mobilen Datenträgern, wie z. B. USB-Sticks, externe Festplatten
- Verschlüsselung von kompletten Festplatten (FDE)

Pre-Boot Authentication (PBA)

- Betriebssyteme können nur nach Ausführen der Preboot Authentication (PBA) gestartet werden
- Unterstützung der EgoSecure Full Disk Encryption sowie Microsoft BitLocker
- Multi-User-/Multi-SmartCard-Unterstützung
- Challenge-Response
- Linux-, BIOS- und UEFI-basiert

Application Control

- Black- und Whitelisting von Anwendungen, Java-Applets und DLL-Dateien
- Für Endanwender unsichtbare Kontrolle, welche Programme gestartet werden dürfen
- Schutz vor Ausführung ungewollter Anwendungen, zum Beispiel nicht ausreichend lizensierter Anwendungen, Key-Generatoren oder Raubkopien
- Unterstützt die Prävention von Malware-Ausbrüchen durch Blockieren
- Simulationsmodus (Demo-Modus)

IntellAct (UEBA)

- Wertet Daten von Insight Analysis und Secure Audit aus und löst vordefinierte Schutzmaßnahmen anhand eines Regelwerkes aus
- Möglichkeit des Vergleichs mit den Normalwerten, um Anomalien oder kritische Situationen automatisch zu erkennen und Schutzreaktionen auszulösen
- Integration in Matrix42 Workflow Studio

Digital Workspace Platform

Die Matrix42 Digital Workspace Platform vereint Anpassbarkeit, Automation und Security mit produktivitätssteigernden Funktionen. Sie ist die Basis aller Matrix42 Produkte und somit auch wesentlicher Bestandteil von Secure Unified Endpoint Management (SUEM).

Mit dem low-code **SolutionBuilder** lassen sich bestehende Oberflächen einfach anpassen oder neue, responsive User Interfaces (UI) mit wenigen Klicks erstellen. Mit dem **Workflow Studio** modellieren Sie Prozesse per Drag & Drop.

Das Resultat: Eine intuitive, anpassbare und erweiterbare Unified User Experience (UUX) über alle Produkte und Prozesse hinweg. Security Funktionen wie ein **Enterprise SSO**, **Device & Access Control** sowie Ursachenanalyse mittels **Secure Audit** und **Insight Analysis** inklusive. Das **Incident Management**, **Sofware Inventory** und eine **agenten-basierte Softwareverteilung** runden die Lösung ab.

Verfügbare Add-ons

Patch Management
- Automatisiert die Absicherung, Aktualisierung und den reibungslosen Betrieb von IT-Systemen durch die zuverlässige Installation neuester Patches
- Unterstützt eine zentrale Verwaltung von über 500.000 Patches für Windows-Systeme und über 60 weiterer Softwarehersteller

Package Cloud
- Umfasst über 4.000 geschäftsrelevante Anwendungen als anpassbare Softwarepakete mit geprüfter Qualität
- Einfache und schnelle Bereitstellung von Anwendungen als Cloud-Dienste
- Ein spezielles Team aus erfahrenen Experten erstellt die Anwendungspakete auf Grundlage vordefinierter Regeln und Richtlinien
- Zweisprachige Pakete (Deutsch und Englisch)
- Geeignet für die Softwareverteilung über Empirum Client Lifecycle Management

Endpoint Detection & Remediation (EDR)
- Blockiert den Ausbruch und Verbreitung von Malware auf Kernel-Ebene in Echtzeit
- Verkürzt die Zeitspanne vom Befall bis zur Unschädlichmachung (dwell-time), durch Automatisierung
- Generiert pro Vorfall einen einzelnen Alert und reduziert somit die Anzahl an Alerts auf ein Minimum
- Erkennt nicht legitim kommunizierende Anwendungen und blockiert die Datenkommunikation in Echtzeit
- Analysefunktion, die gesammelte Daten zur proaktiven Erkennung und Verhinderung von Angriffen sowie zur Ursachenanalyse (Threat Hunting) verwendet.
- Nicht update-gesteuert, kann vollständig isoliert genutzt werden (das heisst auch wirksamer Schutz für Altsysteme ohne Internetverbindung)

Package Robot
- Einfache Lösung zur Erstellung von Installationspaketen für die Softwareverteilung
- Installationsrekorder nimmt Installationsvorgang auf und sorgt dafür, dass Wiederholungen gemäß bewährter Verfahren durchgeführt werden

Remote Control / Remote Web Control
- Einfacher Support und Fernwartung per LAN oder Internet
- Als Cloud Service oder mit lokalem Verbindungsserver
- Hohe Performance und zertifizierte Sicherheit

Data Loss & Leakage Prevention (DLP)
- Schutz vor Diebstahl und unbefugter Weitergabe hochsensibler Daten anhand vordefinierter Suchmuster, ob auf dem Endpunkt, externen Geräten, in der Cloud oder auf dem Dateiserver
- Vordefinierte, gebräuchliche Suchmuster für nationale und internationale Nummerncodes wie zum Beispiel Versicherungsnummern, Passwort-IDs, IBAN & Swift, Kreditkartennummern
- Blockiert die Nutzung der Daten oder führt Aktionen aus, wie Dateien an einen sicheren Speicherort/in Quarantäne zu verschieben oder diese zu löschen
- Detaillierte Protokollierung von Funden
- Globale, gruppenspezifische oder individuelle Regelzuweisung

NextGen Antivirus (NGAV)
- Virenschutz bei bekannten und unbekannten Bedrohungen
- Nachweislich hohe Erkennungsrate
- Erkennung fortgeschrittener Malware durch zertifizierte Next Generation Antivirus (NGAV) und Application Communication Control