MATRIX42

Secure Unified Endpoint Management (SUEM)

Matrix42 Secure Unified Endpoint Management automates the entire process from the commissioning of an endpoint, to rolling out, updating and patching, through to securing the endpoint. When determining the technical management method, the operating system is accounted for to ensure the best possible fit. Security is always an integral part.

Modules & functions

Cross-device Management

Empirum Client Lifecycle Management

- Centralized control and automation from initial installation to end-of-life management
- Transparency across all devices and applications
- Connects with 3rd-party software distribution systems and the entire Matrix42 portfolio to automate various inventory-related tasks and continuously improve the quality of IT services
- Components: Inventory, Software Management, OS Installation, Personal Backup, and Easy Recovery

Silverback Enterprise Mobility Management

- Simple, scalable, and secure device management for smartphones, tablets, and all devices with operating systems such as Android, ChromeOS, iOS, iPadOS, macOS, or Windows 10
- Components: Mobile Device Management, Mobile Application Management, Mobile Content Management

Built-in security

Seamless Anywhere Encryption

- Transparent encryption, no loss of productivity
- Encryption algorithms: AES-256 or Triple DES-192 (additionally encrypted with up to RSA-4096)
- Protection of personal data in accordance with GDPR Article 32
- Decryption and encryption via agent and according to defined corporate guidelines
- Encryption of folders and files in cloud storage devices (e.g., OneDrive, GoogleDrive, Dropbox), on any network share, or on mobile storage devices such as USB sticks, external hard drives
- Full Disc Encryption (FDE)

Pre-Boot Authentication (PBA)

- Operating systems can only be started after executing the Preboot Authentication (PBA)
- Support for EgoSecure and Microsoft BitLocker
- Multi-user/multi-SmartCard support
- Challenge response
- Linux-, BIOS- and UEFI-based

Application Control

- Black- and whitelisting of applications, Java applets, and DLL files
- Monitoring of programs that may be launched; process is invisible to end users
- Protection against execution of unwanted applications, for example, insufficiently licensed applications, key generators, or pirated copies
- Helps prevent malware outbreaks by blocking malicious code
- Simulation mode (demo mode)

IntellAct (UEBA)

- Evaluates data from Insight Analysis and Secure Audit and triggers predefined protective measures based on a set of rules
- Option to compare current data with normal values to automatically detect anomalies or critical situations and trigger protective reactions
- Integration with Matrix42 Workflow Studio

Digital Workspace Platform (DWP)

The Matrix42 Digital Workspace Platform combines configurability, expandability, and security with productivity-enhancing features. It forms the basis of all Matrix42 products and is thus an essential component of Secure Unified Endpoint Management (SUEM).

With the low-code **SolutionBuilder**, existing interfaces can be easily adapted or new, responsive user interfaces (UI) can be created with just a few clicks. **Workflow Studio** allows you to model processes via drag & drop.

The result: an intuitive, configurable, extendable, and at the same time update-proof unified user experience (UUX) across all products and processes. Security functions such as an **Enterprise SSO**, **Device & Access Control**, as well as root cause analysis using **Secure Audit** and **Insight Analysis** are included. **Incident Management**, **Software Inventory**, and **agent-based Software Deployment** complete the solution.

Available add-ons

Patch Management
- Automates the backup, update, and smooth operation of IT systems by reliably installing the latest patches
- Supports centralized management of over 500,000 patches for Windows systems and over 60 other software manufacturers

Package Cloud
- Includes over 4,000 business-relevant applications as adaptable software packages with tested quality
- Simple and fast provision of applications as cloud services
- A special team of experienced experts creates the application packages based on predefined rules and guidelines
- Bilingual packages (German and English)
- Suitable for software distribution via Empirum Client Lifecycle Management

Endpoint Detection & Remediation (EDR)
- Blocks Kernel-level malware outbreaks in real time
- Automated process shortens the time span from infestation to rendering harmless (dwell time)
- Generates a single alert for each incident and thus reduces the number of alerts to a minimum
- Detects applications that are communicating without authorization and blocks real-time data communication
- Analysis function that uses collected data for proactive detection and prevention of attacks and for root cause analysis (threat hunting)
- Not update controlled, can be used completely isolated (this also means effective protection for legacy systems without Internet connection)

Package Robot
- Simple solution for creating installation packages for software distribution
- Installation recorder starts the installation process and ensures that repetitions are carried out according to proven procedures

Remote Control / Remote Web Control
- Easy support and remote maintenance via LAN or Internet
- As a cloud service or via local connection server
- High performance and certified security

Data Loss & Leakage Prevention (DLP)
- Protection against theft and unauthorized disclosure of highly sensitive data using predefined search patterns, whether on the endpoint, external devices, in the cloud, or on the file server
- Predefined, common search patterns for national and international number codes such as insurance numbers, password IDs, IBAN and Swift, credit card numbers
- Blocks the use of the data or performs actions such as moving files to a secure location/quarantine or deleting them
- Detailed logging of findings
- Global, group-specific, or individual rule assignment

NextGen Antivirus (NGAV)
- Virus protection against known and unknown threats
- Proven high detection rate
- Detection of advanced malware by certified Next Generation Antivirus (NGAV) and Application Communication Control