Fact Sheet

MATRIX42

EgoSecure Data Protection

Funktionen

Access Control
- Kontrolle und Steuerung der Zugriffe auf externe Geräte und Schnittstellen der Client-Umgebung
- Zugriffsberechtigung zu Cloud-Diensten
- Kontrolle aller Datenübertragungswege
- Kontrolle von Netzwerkverbindungen (z.B. WLAN, Antibridging, USB-Netzwerkadapter)
- BadUSB-Schutzmaßnahmen
- Dateifilter zum Blockieren bestimmter Datenformate
- Whitelisting von externen Geräten
- Revisionssicherheit nach Basel II, Sarbanes-Oxley, PCI-Konformität

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, z.B nicht ausreichend lizensierte Anwendungen, Key-Generatoren und Raubkopien
- Unterstützt die Prävention von Malware-Ausbrüchen durch Blockieren
- Simulationsmodus (Demo-Modus)

Secure Audit
- Überprüfung des gesamten Datenverkehrs von und auf jedem Endpunkt in Echtzeit
- Nachvollziehbarkeit des Datenflusses gemäß EU-DSGVO Artikel 30, 33
- Schutz vor Missbrauch und Anonymisierung von Audit-Daten gemäß Personal-/Betriebsratskonformität

Insight Analysis
- Überblick über aller Datenbewegungen im Unternehmensnetzwerk
- Sammelt Fakten über die datenschutzrelevanten Situation im Netzwerk
- Visualisierung aller datenschutzrelevanter Vorgänge in einem übersichtlichen Dashboard
- Kumulierte Ergebnisdarstellung (Benutzerdaten sind anonymisiert)
- Automatisierte Berichterstellung und E-Mail Versand

IntellAct Automation
- 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 die Schutzreaktion auszulösen
- Integration in Matrix42 Workflow Studio

Encryption
- Transparente On-the-Fly-Verschlüsselung (ohne Produktivitätsverlust)
- Verschlüsselungstypen: Allgemein, Gruppenverschlüsselung, individuelle Verschlüsselung, unverschlüsselt
- 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, abhängig von definierten Unternehmensrichtlinien z.B. Entschlüsselung nur möglich, wenn sich die Datei auf dem Firmengerät befindet
- Umfangreiches Richtlinienmodell

Cloud und Netzwerk-Share
- Verschlüsselung von Ordnern und Dateien in Cloud-Speichern (z.B. OneDrive, GoogleDrive, Dropbox) oder auf jedem beliebigen Netzwerk-Share
- Verschlüsselungs-Keys werden zu keinem Zeitpunkt in der Cloud oder auf dem Netzwerk-Share gespeichert

Removable Device
- Verschlüsselung auf Dateiebene
- Verschlüsselt Daten auf mobilen Datenträgern, wie z.B. USB-Sticks, externe Festplatten, etc.
- Unbegrenzte Datengröße, z.B. auch Verschlüsselung von Terabyte großen Platten

Local Folder
- Absicherung dedizierter Dateien und Ordnerstrukturen
- Gezielte Berechtigung für einzelne Personen, auch bei gemeinsamer Geräte-Nutzung
- Zuverlässige Absicherung von sensiblen Daten auch gegenüber Mitarbeitern mit Admin-Rechten – z.B. IT-Mitarbeiter

Full Disk Encryption (FDE)
- Verschlüsselung der gesamten Festplatte
- Verschlüsselungsalgorithmen: AES-256, Triple DES-192 oder BlowFish-448
- Windows 10 Build-Upgrade-Support
- Passwortgeschützte Emergency-Recovery-Datei zur Wiederherstellung von nicht mehr zugänglichen Festplatten

Preboot 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-basiert, BIOS-basiert und UEFI-basiert

Permanent Encryption
- Persistente Verschlüsselung von Dateien auf jedem beliebigem Datenträger
- Zugriff auf Dateien nur für Berechtigte möglich. Entschlüsselung am Zielgerät per Passworteingabe, PKI-Token oder EgoSecure-Agent
- Verschlüsselungsstatus bleibt unabhängig vom Zieldatenträger erhalten
- Erzeugt verschlüsseltes Datenpaket, das als E-Mail-Anhang versendet oder über einen Web-Upload bereitgestellt wird

Zukaufbare Module und Add-Ons

Data Loss & Leakage Prevention
- Schutz vor Diebstahl und unbefugter Weitergabe hochsensibler Daten anhand vordefinierter Suchmuster, egal ob auf dem Endpunkt, externen Geräten, in der Cloud oder auf dem Dateiserver
- Vordefinierte, gebräuchliche Suchmuster für nationale & internationale Nummerncodes wie Versicherungsnummern, Passwort-IDs, IBAN & Swift, Kreditkartennummern etc.
- 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

Automated Endpoint Detection & Response mit Post-Infection Protection
- Blockiert den Ausbruch von Malware auf Kernel-Ebene in Echtzeit
- Verkürzt durch Automatisierung die Zeitspanne vom Befall bis zur Unschädlichmachung (dwell-time)
- Generiert pro Vorfall einen einzelnen Alert und reduziert somit die Anzahl an Alerts auf ein Minimum
- Erkennt jede nicht legitim kommunizierende Anwendung 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

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