

endian|OS

Betriebssystem für die sichere Digitalisierung

Alle Produkte von Endian basieren auf dem EndianOS. Dabei handelt es sich um ein leistungsstarkes Betriebssystem (Operating System, kurz: OS), das darauf ausgerichtet ist, die Herausforderungen der Digitalisierung und des Zusammenwachsens von IT- und OT-Umgebungen zu meistern. Dieser Beitrag zeigt, welche einzigartigen Vorteile Anwendern dadurch entstehen.

Ein Betriebssystem verwaltet die Systemressourcen eines Computers und stellt sie den Anwendungsprogrammen zur Verfügung. EndianOS basiert auf Linux, einer Open-Source-Software, die es ermöglicht, individuelle Lösungen für spezifische Anforderungen zu erstellen. Es bildet das Rückgrat aller Endian-Lösungen und erfüllt die Anforderungen von Unternehmensnetzwerken, wie Konnektivität sowie die Verwaltung von Maschinen, Anlagen, Netzwerken, Geräten und Benutzern.

Sicherheit ist der Leitgedanke und die Basis für alle weiteren Entwicklungsschritte in EndianOS. Ohne ein solides Sicherheitskonzept kann jedes Digitalisierungsprojekt zu einem ernsthaften Geschäftsrisiko werden. Endian arbeitet nach dem Prinzip „Security by Design“ und priorisiert die Sicherheit sowohl bei der Entwicklung als auch während des gesamten Produktlebenszyklus.

Durch eine sicherheitsorientierte Konfiguration und die Integration zahlreicher Sicherheitsmaßnahmen ist EndianOS ein sogenanntes „gehärtetes Linux“, das eine hohe Widerstandsfähigkeit gegen potenzielle Bedrohungen aufweist.

EndianOS umfasst mehrere Komponenten, die in ihrer Kombination die notwendigen Lösungen für eine sichere digitale Transformation bieten:

EndianOS Lösungen

Zero-Trust-Architektur

Mit der digitalen Transformation lösen sich Unternehmensgrenzen zunehmend auf. Deshalb gelten traditionelle Sicherheitskonzepte als überholt, denn eine einfache Unterscheidung zwischen internen und externen Zugriffen ist nicht mehr ausreichend. Mit einer Zero-Trust-Architektur können Unternehmen ihre Angriffsfläche minimieren, indem sie fein abgestufte Zugriffs-, Berechtigungs- und Sicherheitsrichtlinien festlegen. Darüber hinaus sorgt eine Zero-Trust-Umgebung für eine stärkere und bessere Einhaltung von Compliance- und Audit-Anforderungen.



Netzwerkvisualisierung

Bevor ein Unternehmen ein Zero-Trust-Modell implementieren kann, muss es jedes einzelne Gerät in seinem Netzwerk identifizieren und bewerten. Herkömmliche Methoden sind kosten- und ressourcenintensiv, da sie häufige Scans erfordern. Eine kontinuierliche Netzwerkvisualisierung, bei Endian „Network Awareness“ genannt, bietet einen schnellen Überblick über alle angeschlossenen Geräte und ermöglicht so einen umfassenden Schutz vor Bedrohungen.



Mikrosegmentierung

Mikrosegmentierung ist ein Element der Zero-Trust-Architektur und steht für die Schaffung kleiner und passgenauer Netzwerkzonen. Da nicht mehr jeder auf alles zugreifen kann, erhöht sich das Sicherheitsniveau. Unternehmen können durch strenge Sicherheitsrichtlinien für die einzelnen Zonen sicherstellen, dass nur autorisierte Kommunikation im Netzwerk stattfindet. Bei Bedarf besteht die Möglichkeit, sichere Verbindungen mit geringstmöglichen Berechtigungen einzurichten.

Komponenten: Firewall, NAT (Network Address Translation), VPN (Virtual Private Network)



Bedrohungsmanagement

Die Bedrohungslage im Cyberraum wandelt sich in einem rasanten Tempo. Das EndianOS enthält deshalb mehrere Komponenten, mit denen sich Angriffe automatisiert erkennen und stoppen lassen, bevor sie das Unternehmensnetzwerk schädigen.

Mithilfe von Deep-Packet-Intrusion-Detection und -Prevention werden Sicherheitsrichtlinien festgelegt und durchgesetzt. Die Analyse der Anwendungsebene und der Protokolle stellt außerdem sicher, dass der Datenaustausch wirklich autorisiert ist. Im Zweifelsfall lässt er sich blockieren und zwar unabhängig von IP-Adresse und Port.

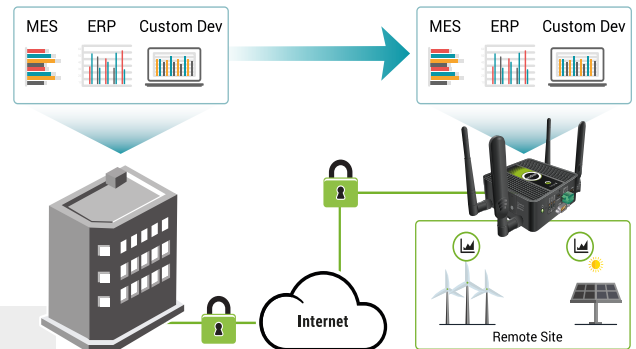
Komponenten: Firewall, IDS/IPS, Application & DNS Security



Edge Computing

Edge Computing bezeichnet die dezentrale Verarbeitung von Daten und die Erstellung von Auswertungen direkt an der Datenquelle, anstatt sie an ein zentrales Rechenzentrum oder eine Cloud weiterzuleiten. Der Einsatz von Docker- und Container-Technologien ermöglicht den Betrieb von Unternehmensanwendungen am Netzwerkrand und erweitert damit den Funktionsumfang von Edge Computing.

Komponenten: Docker Engine



EndianOS Komponenten

Um diese innovativen Konzepte für die Digitalisierung umzusetzen zu können, enthält EndianOS mehrere Komponenten, die für Konnektivität und Sicherheit sorgen und das Management der Infrastruktur ermöglichen:

Konnektivität

Innovative Konzepte wie Condition Monitoring oder Predictive Maintenance erfordern eine kontinuierliche Datenerfassung und -auswertung. Da immer mehr Maschinen und Systeme miteinander vernetzt werden, kann es schnell zu Engpässen bei der Bandbreite kommen. Für die Optimierung der Konnektivität bietet EndianOS verschiedene Funktionen:

Multi-WAN

Die Multi-WAN-Komponente ermöglicht die Nutzung mehrerer Internetverbindungen innerhalb eines Netzwerks. Damit lässt sich der Datenverkehr einfach verteilen, um die Redundanz zu erhöhen und einen durchgängigen Geschäftsbetrieb sicherzustellen.

Richtlinienbasiertes Routing

Richtlinienbasiertes Routing ermöglicht es Unternehmen, den Netzwerkverkehr und damit auch die Bandbreite über mehrere Internetverbindungen zu steuern und zu priorisieren. Dadurch wird die kontinuierliche Verfügbarkeit geschäftskritischer Anwendungen erreicht.

Bandbreitenmanagement

Unternehmen können Richtlinien für die Nutzung der verfügbaren Bandbreite durchsetzen. Geschäftsspezifische Anwendungen erhalten Vorrang, während unwichtige Aktivitäten eingeschränkt oder blockiert werden können.

Hochverfügbarkeit

Hochverfügbarkeit minimiert Ausfallzeiten durch Clustering von mindestens zwei Appliances, so dass eine Appliance den Betrieb übernehmen kann, wenn die andere ausfällt, um die Geschäftskontinuität zu sichern.

Sicherheit

Sicherheit ist die Basis für eine erfolgreiche Digitalisierung. Immer mehr Geräte sind vernetzt und in Industrieumgebungen wird zunehmend die Betriebstechnologie, sogenannte OT-Systeme, mit dem Internet verbunden. Damit vergrößert sich die Angriffsfläche für Cyberkriminelle unaufhaltsam, gleichzeitig begünstigt die steigende Komplexität menschliche Fehler. Das EndianOS enthält deshalb folgende Sicherheitsfeatures:

Firewall

Die Firewall kombiniert eine intuitive Benutzeroberfläche mit innovativen Funktionen zur Gewährleistung von Netzwerksicherheit und -effizienz. Benutzer können individuelle Firewall-Regeln erstellen, implementieren und überwachen. Dazu gehört das Blacklisting unerwünschter Anwendungen, ebenso wie die Zugriffsblockierung aus bestimmten Ländern oder Regionen.

Sicheres Virtual Private Network (VPN)

Die gesamte Kommunikation wird über ein VPN abgesichert, damit die Daten verschlüsselt werden und jederzeit vertraulich bleiben. Mit Endian VPN lässt sich ein sicherer Fernzugriff auf Netzwerke, Maschinen und Anlagen einrichten sowie eine sichere Verbindung zwischen verteilten Netzwerken herstellen.

Intrusion Detection (IDS) und Intrusion Prevention (IPS)

Durch kontinuierliches Scannen aller Datenpakete bis hin zur Anwendungsebene werden die grundlegenden Muster des Netzwerkverkehrs identifiziert. Jede Abweichung von diesem grundlegenden Muster wird durch das IDS erkannt. Wenn die Abweichung auf eine Bedrohung wie Malware zurückzuführen ist, wird sie vom IPS gestoppt.

DNS-Filterung

Die DNS-Filterung nutzt den DNS-Proxy, um Phishing- und andere Malware-Seiten zu blockieren. Dadurch wird eine weitere Sicherheitsebene hinzugefügt. So kann das Unternehmen seine eigenen Daten schützen und kontrollieren, worauf die Mitarbeiter in seinen Netzwerken Zugriff haben.

Management

Die steigende Zahl der angeschlossenen Geräte führt zu Komplexität, erhöht den Verwaltungsaufwand und begünstigt Fehler, die schnell zu Sicherheitsrisiken werden können. Mit EndianOS wird die Netzwerkverwaltung vereinfacht, während automatisierte Ansätze für mehr Sicherheit sorgen.

Netzwerkvisualisierung

Die Netzwerkvisualisierung sorgt dafür, dass Anwender den Überblick behalten, egal wie komplex ihre Netzwerke sind. Ansprechende Dashboards stellen den Netzwerkverkehr und die Aktivitäten in Echtzeit dar. Die "Time Machine"-Funktion bietet Einblicke in vergangene Netzwerkereignisse.

Automatische Updates

Nur aktuelle Sicherheitstools bekämpfen neue Bedrohungen effektiv. EndianOS automatisiert Updates für alle angeschlossenen Geräte und stellt so sicher, dass diese immer auf dem neuesten Stand sind.

EndianOS - ready for your future!

EndianOS bietet Unternehmen die ideale Grundlage für eine sichere, einfache und nachhaltige digitale Transformation. Das Betriebssystem ermöglicht die Skalierung für größere und komplexe Netzwerkinstallationen mit Unterstützung für unbegrenzte interne Netzwerkzonen. Benutzer können bei Bedarf einfach Netzwerke hinzufügen und ihre Sicherheit durch die Integration von fortschrittlichen Netzwerksicherheitsfunktionen erhöhen. Durch die Unterstützung von Edge Computing mit Docker haben Anwender auch die Möglichkeit, Anwendungen und Dienste am Netzwerkrand auszuführen.