Engine for a Secure Digital Transformation

All Endian products are based on EndianOS, a secure operating system (OS) designed to address the challenges of digitization and the convergence of IT and OT environments. This article explains the unique advantages that users gain from it.

An operating system (OS) manages a computer's system resources and makes these available to application programs. EndianOS is based on Linux, an open-source software that offers the opportunity to build individual solutions tailored to specific needs. It serves as the backbone of all Endian solutions, meeting the demands of enterprise networking like connectivity as well as the management of machines, equipment, networks, devices and users.

Security is the guiding principle and the basis for all further development steps in EndianOS. Without a solid security concept, any digitization project could become a serious business risk. Endian operates according to the principle of "Security by Design," prioritizing security during development as well as throughout the entire product lifecycle.

Through security-focused configuration and the integration of numerous security measures, EndianOS is what's known as "hardened Linux," demonstrating high resilience against potential threats.

EndianOS includes several components that, when combined, offer the solutions necessary for a secure digital transformation:

EndianOS solutions

Zero-Trust Architecture

As digital transformation blurs corporate boundaries, traditional security concepts become outdated. A simple differentiation between internal and external access is no longer sufficient. A Zero-Trust Architecture enables companies to minimize their attack surface by establishing fine-grained access, authorization, and security policies. Moreover, a Zero-Trust environment ensures better compliance and audit requirements.

Network Visualization

Before implementing a Zero-Trust model, it's essential to identify and evaluate each device within the network. Conventional methods are costly and resource-intensive, often requiring frequent scans. Continuous network visualization, referred to as "Network Awareness" by Endian, offers a quick overview of all connected devices, ensuring comprehensive protection against threats.

Micro-segmentation

Micro-segmentation is a component of the Zero-Trust Architecture, creating small, precisely tailored network zones. With restricted access, the security level increases. By enforcing strict security policies for each zone, companies can ensure that only authorized communication is authorized within the network, establishing secure connections with minimal permissions.

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

Threat Management

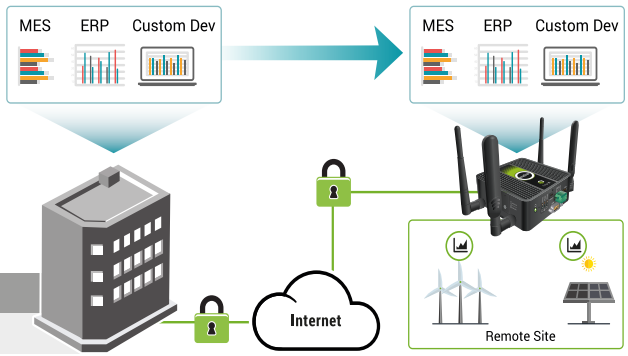
The threat situation in cyberspace is changing at a rapid pace. EndianOS therefore contains several components that can be used to automatically detect and stop attacks before they damage the corporate network.

Deep packet intrusion detection and prevention is used to set and enforce security policies. The analysis of the application level and the protocols also ensures that the data exchange is really authorized. If in doubt, it can be blocked, regardless of IP address and port.

Components:
Firewall, IDS/IPS, Application, DNS Security

Edge Computing

Edge computing refers to the decentralized processing of data and calculations directly at the data source instead of forwarding them to a central data center or cloud. The use of Docker and container technologies enables the operation of enterprise applications at the edge of the network and thus expands the functional scope of edge computing.



Components:
Docker Engine

Components of EndianOS

To implement these solutions, EndianOS includes several components ensuring connectivity, security, and infrastructure management:

Connectivity

Innovative concepts such as Condition Monitoring or Predictive Maintenance require constant data collection and evaluation. As more machines and systems become interconnected, bandwidth constraints may quickly arise. To optimize connectivity, EndianOS offers several features:

Multi-WAN

The Multi-WAN component allows the use of multiple internet connections within a network. It simplifies traffic distribution to enhance redundancy and ensure continuous business operations.

Policy Routing

The use of policy routing enables businesses to prioritize and manage the flow of network traffic (and thus bandwidth) across multiple internet connections. This ensures the continuous availability of critical business applications.

Bandwidth Management

Companies can enforce policies on how available bandwidth is used. Business-specific applications receive priority, while unimportant activities can be limited or blocked.

High Availability

High Availability minimizes downtime by clustering at least two appliances, allowing one to take over if another fails to ensure business continuity.

Security

Security is the foundation for successful digitization. The growing interconnectivity of devices, especially in industrial environments where more and more Operational Technology (OT) systems are connected to the Internet, expands the attack surface for cybercriminals. This requires robust security features in EndianOS:

Firewall

The firewall combines an intuitive user interface with innovative functions to ensure network security and efficiency. Users can create, implement, and monitor individual firewall rules, such as blacklisting unwanted applications or blocking access from specific countries or regions.

Secure Virtual Private Network (VPN)

All communication is secured via a Virtual Private Network (VPN) so that data is encrypted and remains confidential at all times. The Endian VPN can be used to establish secure remote access to networks, machines and plants, as well as to create a secure connection between distributed networks.

Intrusion Detection (IDS) and Intrusion Prevention (IPS)

Continuous scanning of all data packets, extending to the application layer, identifies network traffic baselines. Any deviation from this baseline is detected by the Intrusion Detection System (IDS). If the deviation is due to a threat such as malware, the Intrusion Prevention System (IPS) halts it.

DNS filtering

DNS filtering uses the DNS proxy to block phishing and other malware sites. This adds another layer of security. As a result, the company can protect its own data and control what employees have access to on its networks.

Management

The increasing number of connected devices leads to complexity, raising the administrative workload and favoring errors that can swiftly become security risks. With EndianOS, network management becomes simplified, while automated approaches ensure enhanced security.

Network Visualization

The network visualization ensures users maintain an overview, no matter how complex their networks are. Engaging dashboards represent real-time network traffic and activities. The “Time Machine” feature provides insight into past network events.

Scheduled Updates

Only up-to-date security tools effectively combat new threats. EndianOS automates updates for all connected devices, ensuring they are always current.

EndianOS - ready for your future!

EndianOS provides organizations with the ideal foundation for a secure, simple and sustainable digital transformation. The operating systems enables scaling for larger and complex network installations with support for (virtually) unlimited internal network zones. Users can easily add networks on demand and increase their security by integrating advanced network security features. With the support for edge computing with Docker users have also the opportunity to rund applications and services at the network edge.