cognitix Threat Defender

Facts & Features

Internal Network Security

Definition

cognitix Threat Defender is a behavior-based network security platform that analyzes the network traffic in real time and enhances this network-specific data with up-to-date threat intelligence from numerous external sources. Based on the detected behavior of network assets and users, cognitix Threat Defender enforces policies dynamically with a self-modifying policy-set. This allows for much faster reactions to threats than conventional signature-based threat detection that uses static rules.

cognitix Threat Defender operates transparently inside the network perimeter and can be installed anywhere in the network.

Reasons to Choose cognitix Threat Defender

- Granular, multi-level security policies
- Behavior-based self-modifying policies to stop lateral movement
- Single-pass correlation and policy engine
- Transparent integration inside the network without changes in configuration
- Install anywhere on hardware matching the required performance and connectivity
- GDPR compliance
- User-friendly GUI
- IT security made in Germany

Typical Use

- Increasing trust in the network through real-time asset tracking, deep analysis, and drill-down reporting
- Safeguarding business-critical operations by integrating cognitix Threat Defender transparently into the network: as first line of defense in front of the router, as second line of defense inside the core network to detect and block malicious behavior within network segments, or as last line of defense in front of high-value assets
- Protecting Industry 4.0 production networks by detecting and blocking intrusions in machine-to-machine communication

Customer Service

- Customer service directly from the manufacturer
- Security system management
- Hotline service
- Comprehensive training courses

SecurITy made in Germany

Behavior-Based Correlation

Correlation engine	Multi-stage rule evaluation for behavior modeling
Single-pass	Correlation of events across multiple historic and current traffic flows, all traffic has to pass all stages of the engine
Policy engine	Extended rule syntax to mitigate specific threats
Real-time	Data is correlated the moment it is generated
Inline	Correlation takes place inside the policy engine
Enrichment	Flows are enriched with relevant metadata
Event tracking tables	Properties of communication events are tracked across traffic flows and over time
Comprehensive	All traffic flows generated by certain hosts/assets are analyzed – not just individual flows
Versatile tool set	Build complex scenarios of multi-staged policies
Schedules	Specify during which times of the day and/or on which dates policies will be enforced

Dynamic Network Segmentation

Dynamic network objects	DNOs adapt the network segmentation dynamically at runtime without changing the physical topology
Automatic response	Changing, unwanted or suspicious behavior triggers immediate reactions
Virtual overlay	Static and dynamic network objects provide a virtual overlay security network with a dynamically changing topology on top of the physical network
Overlapping segments	Network segments can overlap
Layering	Network assets can be part of several network objects so that multiple policies can be layered and applied to these assets
VLAN	Tagged and untagged VLANs can be handled, VLAN-aware policies
Matching	The network segmentation is used for traffic source and destination matching in policies

Threat Intelligence

Large database	Threat intelligence feeds from multiple external sources
Continuously active	All network traffic is correlated with threat intelligence data in real time
Optimized data structure	No performance losses
Context	Threat intelligence data is enriched with external context and metadata
Up-to-date	Threat intelligence feeds are regularly updated
Early warning system	Take preventive measures before an attack happens
Custom IPS rule sets	User-defined IPS rule sets can be used in addition to the standard IPS rule set
Printable reports	Export incident logs in PDF reports

Tracking

Asset tracking

Automatic asset discovery	New assets are automatically tracked when they communicate in the network
Clear identification	IP and MAC addresses are tracked
Tagging	Tags can be assigned automatically, tags can be used in policy rules
Metadata	Collect specific asset metadata, e.g. hostname etc.
Logging	Asset information is logged in dedicated asset logs
Use in policies	Rules can be applied to specific assets and groups of assets
Printable reports	Export asset logs in PDF reports
GDPR-compliant	Privacy-friendly default settings for GDPR-compliant usage; data exports for specific assets and users
Backup	Backup and share the assets database

genua.

Tracking

User tracking

Compatible to IAM systems	Automatically map usernames to IP addresses
Logging	User information is logged in dedicated user logs
Printable reports	Export user logs in PDF reports
Policies	Create individual policies for specific users
Backup	Backup and share the users database

Drill-Down Reporting

Deep visibility	Intuitively click your way through multiple reporting levels
Dashboards	Dashboards provide a quick overview
Visualization	More than 600 charts and matrixes for clear visualization
Multi-angle view	Examine the traffic from multiple angles: by assets, users, protocols, URLs, etc.
Reporting periods	Select pre-defined reporting periods from one minute to one month

Monitoring

Hardware status	Information on the hardware components is displayed for various reporting periods
System health	The current status of the individual system components is shown with any warnings
Troubleshooting	Troubleshooting reports containing various log files help locating and analyzing any issues in the system

Administration

General

Web GUI	User-friendly web-based interface
Online documentation	Searchable HTML documentation provides quick help
Backups	Download and restore portable configurations

Installation

genua hardware	Choose between three hardware versions (S, M, L) as required

Logging

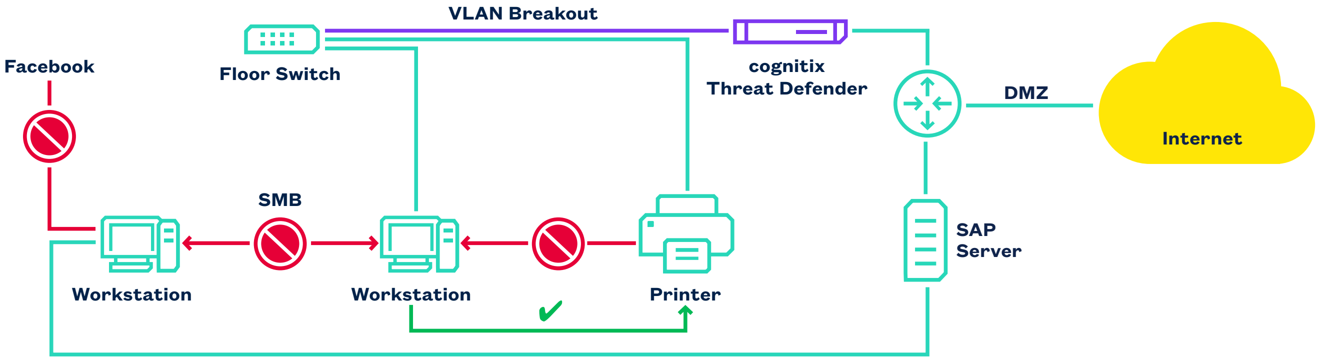
Audit log channels	Send reports via email, desktop notification or via webhook to slack/pager/messengers
Syslog	Export logging data to external recipients
IPFIX	Export logging events using standard and custom IPFIX events
JSONL	Export compact logs using JSON Lines

Central Management

genucenter	System status information can be transmitted to a genucenter central management system
SNMP	Connect to central monitoring systems via SNMPv2c and SNMPv3

More product information

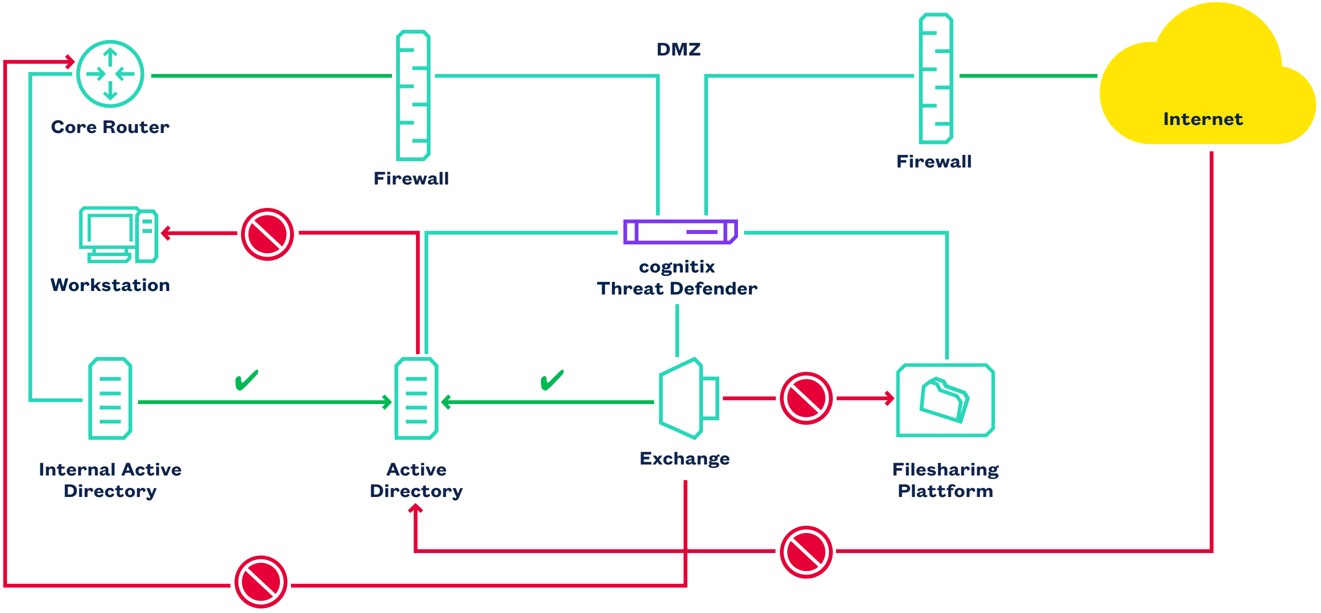
Use Cases



Safeguarding the Office Network Inside the Network Segments

Security is not defined at the router alone. This avoids long and complicated rule sets. cognitix Threat Defender in VLAN breakout mode acts as switch with security functionality. It monitors the traffic and enforces the security policy:

- Clients may access the SAP server
- Clients accessing the SAP server must not access Facebook at the same time
- Clients must not share files among each other to stop lateral movement of attackers
- Clients may access the printer but the printer must not access clients



Isolating Services in a DMZ

- Additional prevention of DoS attacks on public services
- Prevention of lateral movement of attackers within the DMZ and into internal networks (e.g. Hafnium)
- cognitix Threat Defender isolates the services inside the DMZ from each other and allows only the necessary communication:
- Exchange may communicate with Active Directory
- Exchange must not communicate with the file sharing platform
- Exchange must not access the internal network
- Active Directory must not contact any client
- An internal Active Directory is allowed to access Active Directory in the DMZ

Further Information:

www.genua.eu/threat-defender

genua GmbH
Domagkstrasse 7 | 85551 Kirchheim | Germany
+49 89 991950-0 | info@genua.eu | www.genua.eu