genua Ein Unternehmen der Bundesdruckerei

cognitix Threat Defender

Facts & Features

Overview:

cognitix Threat Defender is a behavior-based security platform using artificial intelligence and data analytics. It analyzes the network traffic in real time and the interactive drill-down reporting feature visualizes complex relationships. cognitix Threat Defender 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. It can be deployed anywhere in the network and supports numerous hardware platforms. Shortly, it will be available as a complete hardware appliance.

Typical Use:

- Gaining control of networks and increasing trust through real-time asset tracking, deep analysis and drill-down reporting.
- Protecting networks behind the perimeter firewalls by detecting and blocking malicious behavior within network segments.
- Protecting Industry 4.0 production networks by detecting and blocking intrusions in machine-to-machine communication.

Throughput:

The performance depends on the hardware system used. A single-socket reference system (Intel Xeon E5-2690v4: 14 cores / 28 threads; 128 GB ECC RAM; 40 Gbit/s network connectivity) achieves a throughput of 5.85 Gbit/s (BreakingPoint Enterprise mix) with the full feature set enabled (real world measurement). The throughput can be increased by scaling up the hardware.

Reasons to Choose cognitix Threat Defender:

- State-of-the-art technology with artificial intelligence and data analysis
- 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

Reasons to Choose genua:

- Leading German specialist for IT security
- Founded in 1992 – implementation of numerous major projects for industrial, government, and military organizations

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
Inline real-time	Data is correlated inside the policy engine the moment it is generated
Enrichment	Flows are enriched with relevant metadata
Event tracking tables	Track properties of communication events across traffic flows and over time
Comprehensive	Analyzes all traffic flows generated by certain hosts/assets and 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	React to changing, unwanted or suspicious behavior
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	Define overlapping network segments
Layering	Network assets can be part of several network objects so that multiple policies can be layered and applied to these assets
VLAN	Handle tagged and untagged VLANs, VLAN-aware policies
Matching	Use network segmentation 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 constantly updated
Early warning system	Take preventive measures before an attack happens
Printable reports	Export threat intelligence logs in PDF reports

Tracking

Asset Tracking	
Automatic asset discovery	New assets are automatically tracked when they communicate in the network
Clear identification	Track IP and MAC addresses
Metadata	Collect specific asset metadata, e.g. OS type, hostname etc.
Logging	Asset information is logged in a dedicated asset log
Use in policies	Rules can be applied to specific assets and groups of assets
Printable reports	Export asset logs in PDF reports
Backup	Backup and share the asset database
User tracking	
Compatible to IAM systems	Automatically map usernames to IP addresses
Logging	User information is logged in a dedicated user log
Printable reports	Export user logs in PDF reports
GDPR-compliant	Select one of three GDPR modes to specify how much information is collected
Policies	Create individual policies for specific users
Backup	Backup and share the user database

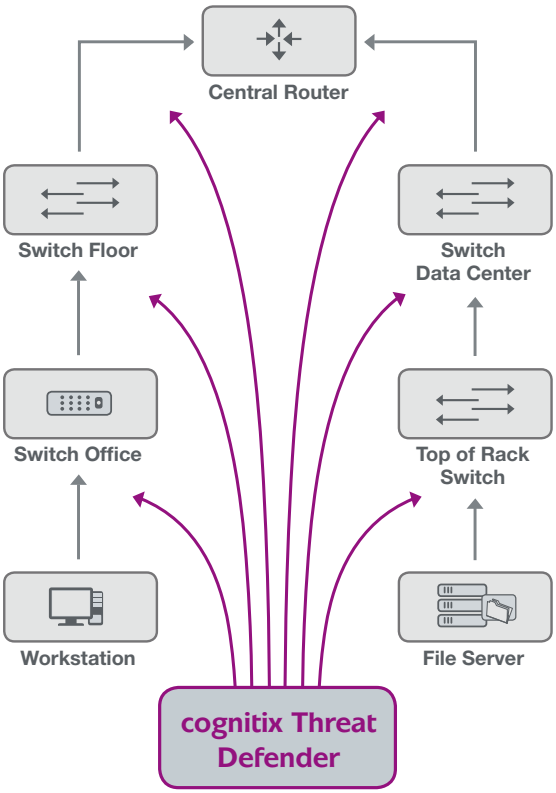
Drill-down reporting

Deep visibility	Intuitively click your way through multiple reporting levels
Dashboards	Four 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

Administration

General	
WebGUI	User-friendly web-based interface
Online documentation	Searchable HTML documentation provides quick help
Backups	Download and restore portable configurations
Updates	
GUI	Download and install updates via the GUI
Schedulable	Schedule and automatically install updates outside business hours
Logging	
Audit log channels	Send reports via email, desktop notification or via webhook to slack/pagers/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

Application Examples



Modern Network Protection with AI and Data Analytics

cognitix Threat Defender goes beyond intrusion prevention. With data analytics, threat intelligence, and as a platform for AI applications, it builds a second line of defense in the network to complement firewall solutions that control and secure traffic at the interfaces. cognitix Threat Defender analyzes the entire data traffic in the network in real-time, detects suspicious behavior and can dynamically apply granular security policies for threat prevention. This enables it to prevent attacks before they cause damage and spread across the network.

Further information:
www.genua.eu/thread-defender

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

TD-FF-0919-01-E