NETWITNESS

NextGen™ Infrastructure

In today's rapidly evolving threat environment, how do you know what is really happening on your network? With the ability to record and analyze everything (every session, communication, service, application and user), you can always know with clarity and definitive answers what did or did not occur on your network, and obtain an unprecedented level of situational awareness and continuous monitoring.

NetWitness® NextGen™ is the single core security platform that makes this capability a reality through three core components: Decoder, Concentrator and Broker. Decoder is the cornerstone and the frontline component of an enterprise-wide network data recording and analysis infrastructure. Decoder is a highly configurable network appliance that enables the real-time collection, filtering, and analysis of all network data. Position Decoder(s) wherever you want on the network: egress, core, or segment.

Unlike any other packet capturing or network monitoring product on the market, Decoder fully reassembles and globally normalizes network traffic at every layer of the OSI model for real-time, full session analysis. The appliances can be operated in continuous capture mode or tactically to consume network traffic from any source. Decoder's patented technology represents a breakthrough in network monitoring that dynamically creates a complete ontology of searchable metadata across all network layers and user applications.

Decoders are architected to work in conjunction with Concentrators that aggregate metadata for analysis from Decoders in real-time, and Broker which provides a real-time, single enterprise view across your entire network.

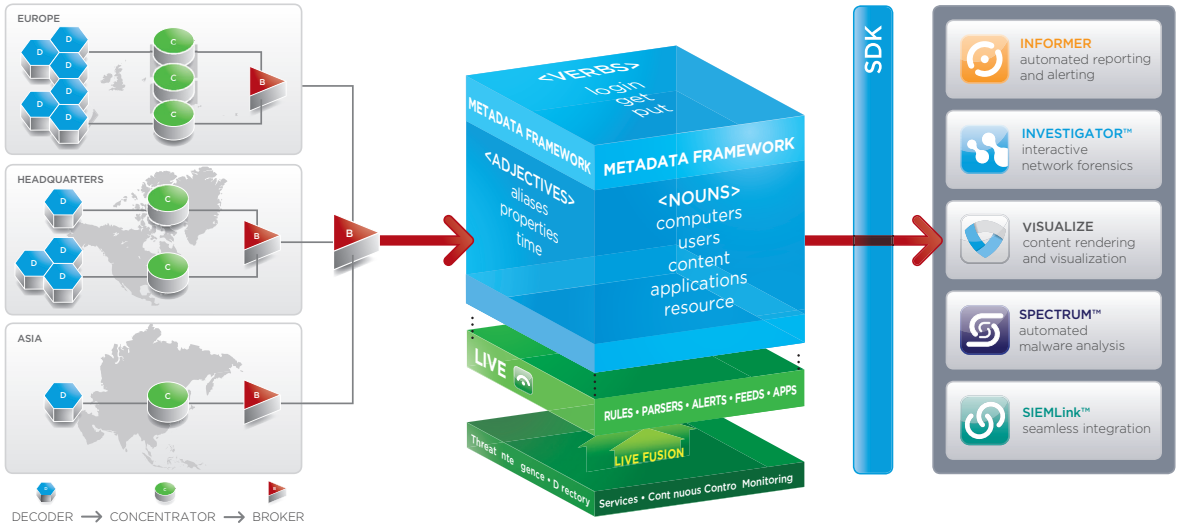
Concentrator is designed to aggregate metadata hierarchically to enable scalability and deployment flexibility across various organization-specific network topologies and geo-locations. As a result, Concentrators can be deployed in tiers to provide visibility and high availability into multiple Decoder capture locations.

Broker operates at the highest level of the hierarchical NextGen infrastructure. Its function is to facilitate queries across an entire enterprise-wide deployment where multiple Concentrators are employed. Broker provides a single point of access to all the NextGen metadata and is designed to operate and scale in any network environment, independent of network latency, throughput, or data volume.

Depending on your network topology and operational performance requirements, all or a subset of the NextGen components could be required to create a flexible, scalable infrastructure that grows with your business.

NETWITNESS NEXTGEN™

Enterprise Security Platform



PLATFORM OPTIONS

To meet your growth needs and operational uses cases, NetWitness has developed a series of high performance NextGen platform options:

Portable – NetWitness Eagle is a portable and compact version of the NetWitness Decoder. Eagle enables powerful and rapid field deployment of the NetWitness network monitoring platform with a briefcase-size footprint. Unlike other portable solutions, Eagle also supports Wi-Fi monitoring with the same level of forensic analytics the NetWitness community has come to expect.

Branch – For optimizing branch performance on a single platform and lowering total cost of ownership, the NetWitness NextGen Hybrid is a combined Decoder/Concentrator platform. Hybrid enables the branch office or small security team to scale to next-generation requirements and still meet important operational security initiatives for responsive incident management and threat mitigation capabilities.

Data Center – For high availability, enterprise-wide environments, NetWitness NextGen Decoder, Concentrator and Broker appliances offer the deployment flexibility to meet bandwidth and storage performance requirements. NextGen's hierarchical architecture allows geographically dispersed locations to be sized appropriately while maintaining operational standards for real-time situational awareness.

Service Provider – For the most demanding environments that require unlimited scalability and global network monitoring, the NetWitness NextGen platform brings industry-leading technology and experience to support any security operations team. From a global organization operating their own backbone to national service providers, NextGen offers an extensible platform to maximize investment value and deliver the operational performance needed to inform and enable better risk management and business decisions.

Each NextGen component has a critical role in enabling scalability and achieving an organization's operational performance metrics. In order to enable application layer traffic analysis in real-time at Data Center and Service Provider levels, a next-generation computing architecture must scale out as well as scale up. The distributed and hierarchical nature of NetWitness' NextGen infrastructure allows an organization to incrementally add traffic processing, database and storage capacity as-needed. The "one box does it all" at the point of capture simply cannot maintain system integrity and performance while processing network traffic and running analytical queries

NextGen Platform Options

Portable Tactical	Branch Fixed Capacity	Data Center High Performance	Service Provider Unlimited Scalability
Usage: Incident Response Tactical Operations	**Usage**: Remote Office Managed Services Small Security Teams	**Usage:** Enterprise Monitoring SOC Operations	**Usage:** National Monitoring Large SOC Operations Indefinite Retention
 NWA50 "Eagle"	 NWA200 Hybrid  NWA100 Broker	 NWA1200/2400 Decoder  NWA1200/2400 Concentrator  NWA100 Broker	 EMC² NetApp
Features: Briefcase Form-Factor Encrypted/Removable Drives 2TB Retention	**Features:** 1U Form-Factor Fixed Capacity Distributed Visibility 8TB Retention	**Features:** 1U & 2U Form-Factors Bandwidth Scalable Distributed Visibility 12 or 24TB Retention DAS & SAN Storage Available	**Features:** 1U & 2U Form-Factors Bandwidth Scalable Distributed Visibility 12 or 24TB Retention DAS & SAN Storage Available
Throughput 100Mbps **Saturated Storage** 1TB/day	250Mbps 2.5TB/day	1Gbps 10TB/day	10Gbps 100TB/day	40Gbps 400TB/day

at the same time. Moreover, recording traffic without being able to use or analyze it does not satisfy customer expectations.

The NextGen infrastructure is designed to interoperate directly with NextGen AppSuite products: Investigator, Informer, Visualize, Live and SIEMLink. Users can create their own custom applications that meet their operational and business needs by utilizing our open API/SDK to seamlessly integrate with the NextGen platform and to extend the value of their existing security investment. By having all this information immediately accessible, customers have the agility to respond to emerging threats and forensic investigations, identify broken business processes, mitigate intentional data exfiltration and confront tomorrow's challenges. NextGen represents the intersection of network telemetry and rich application layer content and context that differentiates NetWitness from any other solution on the market.

FEATURES

- 64-bit Linux-based, highly configurable network appliances
- Up to 10Gbps throughput performance
- Applies metadata for efficient indexing, storage and searchability
- Scalable architecture to create a distributed recording framework
- File object exporting (.exe, .pdf, .doc, .gif, .jpeg, .wav, .mps and many others)
- Integrates with expandable DAS storage and SAN solutions, including EMC and NetApp
- Integrates with NetWitness Live to add list-based content and context, including NetWitness Profilers (indicators, parsers, reports and rules), to recorded network information
- Available open API/SDK to empower custom application development
- FlexParse™ enabled for rapid, user defined parsing and modeling
- Supports RSA SecurID and LDAP authentication
- Supports SNORT signatures
- Protocol and application exploitation:

  HTTP, FTP, TFTP, TELNET, SMTP, POP3, NNTP, DNS, SOCKS, HTTPS, SSL, SSH, Vcard, PGP, SMIME, DHCP, NETBIOS, SMB/CIFS, SNMP, NFS, RIP, MSRPC, Lotus Notes®, TDS(MSSQL), TNS(Oracle®), IRC, Lotus Sametime®, MSN IM, RTP, Gnutella, Yahoo Messenger, AIM, SIP, H.323, Net2Phone®,Yahoo Chat, SCCP (Cisco® Skinny), Bittorrent, GTALK, Hotmail, Yahoo Mail, GMail, TOR, Social Networking, Fast Flux, VLAN tagging and many others.

APPLIANCE MODELS

* Optional (2) 1Gbps Fiber ** Optional (2) 1Gbps Fiber or (1) 10Gbps Adapter

	Model	Processor	RAM	Interfaces	Storage	Power	Form Factor	Weight
Broker	100 series	Dual-Core	8GB	100/1000 Copper (2)	2TB Redundant	Single 260W	1U, Half-Depth	25 lbs
	200 series	Quad-Core	8GB	100/1000 Copper (2)	4TB Redundant	Redundant Max 450W	1U, Full-Depth	34 lbs
Concentrator	1200 series	Quad-Core	32GB	100/1000 Copper (2)*	up to 12TB Redundant	Redundant Max 850W	2U, Full Depth	66 lbs
	2400 series	Dual Hex-Core	up to 128GB	100/1000 Copper (2)*	14.5TB Redundant	Redundant Max 800W	2U, Full Depth	65 lbs
Decoder	100 series	Dual-Core	8GB	100/1000 Copper (2)	2TB Not Redundant	Single 260W	1U, Half-Depth	25 lbs
	1200 series	Quad-Core	16GB	100/1000 Copper (6)**	12TB Redundant	Redundant Max 850W	2U, Full Depth	66 lbs
	2400 series	Hex-Core	32GB	100/1000 Copper (6)**	24TB Redundant	Redundant Max 800W	2U, Full Depth	65 lbs
Eagle	50 series	Quad-Core	up to 16GB	(2) 100/1000 Copper	up to 4TB Redundant	Single up to 520W	Briefcase	up to 20 lbs
Hybrid	200 series	Dual Quad-Core	32GB	100/1000 Copper (2)	8TB Redundant	Redundant Max 700W	1U, Full-Depth	34 lbs

ABOUT NETWITNESS

NetWitness® is the next-generation network monitoring platform that delivers clarity and definitive answers to improve security and optimize risk management. By recording a content-based and contextual understanding of an organization's network activity, we provide forensic accuracy into past activities, real-time analysis for situational awareness, and the agility to adapt and confront tomorrow's challenges.

NetWitness Corporation | 500 Grove Street, Suite 300 | Herndon, VA 20170
T: 703.889.8950 | F: 703.651.3126 | sales@netwitness.com

Learn more at **netwitness.com**