NetWitness

Decoder

How do you know what really happened on your network if you don't have a record of it?
Can you prove definitively what communications did or did not occur on your network?
Do you want to have a higher level of assurance regarding actual specific activities on your network?

NetWitness® Decoder is the cornerstone of the NetWitness NextGen™ infrastructure and the key component of an enterprise-wide network data recording solution. Decoder is a real-time, distributed, highly configurable network recording appliance that enables users to collect, filter, and analyze full network traffic in an infinite number of dimensions.

Unlike every other network recording or monitoring products on the market, Decoder fully reassembles and globally normalizes traffic at every layer for full session analysis. The patented Decoder represents a breakthrough in network traffic monitoring that dynamically builds a complete taxonomy of data across all layers and applications, including full packets. Decoder creates a definitive foundation of Total Network Knowledge™ that can be mined in real-time by the NetWitness® Investigator Enterprise and Informer applications. NetWitness Decoder now also includes NetWitness® Live, which provides you with access to multi-source threat intelligence. For more advanced applications, users can leverage NextGen's available API/SDK to build more organizational-specific applications which utilize Decoder and the NextGen infrastructure. Decoder represents the intersection of network metrics, rich application flow and content information that differentiates NetWitness® products from any other capabilities on the market.

Now Available in a Portable Version!

NetWitness has now introduced NetWitness® NextGen Eagle, a portable and compact version of the NetWitness® Decoder. NextGen Eagle broadens NetWitness' capabilities from fixed network infrastructure devices to include a compact, mobile monitoring system to support law enforcement, incident responders, auditors, intelligence, and consulting staff for field-duty scenarios. Unlike other portable vendor offerings, NextGen Eagle also supports WiFi monitoring with an exceptional depth of analysis.

Product Features:

- Supports 10G infrastructures
- Supports NetWitness® Live
- Linux-based, highly configurable, full packet capture and reassembly device
- Modular and fully upgradeable hardware platform across entire product line
- Indefinitely scales your collection infrastructure upon a distributed, highly manageable, real-time framework

- FlexParse™ enabled for rapid, user definable parsing and modelling
- Supports threat intelligence feeds that track BOTs, designer malware, darknets, proxies and fast flux networks, etc.
- Protocol and application exploitation: HTTP, FTP, TFTP, TELNET, SMTP, POP3, NNTP, DNS, HTTPS, SSL, SOCKS, 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 and many others.
- Expandable SAS storage capacity & supports SAN solutions
- Available API/SDK for custom application development
- Supports NetWitness Identity for correlating users to network traffic
- Supports RSA SecurID and LDAP authentication

Deployment:

Place NetWitness® Decoder(s) wherever you want to capture traffic: egress, core, facility, or segment. They can be operated continuously or tactically and ingest any network capture feed from any source. Decoders are designed to interoperate with Investigator Enterprise and Informer, as well as push data to central NetWitness® Concentrators for aggregated analytical views.

NetWitness® Appliance Models:

SKU	Interface	Storage	Form Factor	Power	Weight
NWA 100-8D	One copper Ethernet 100/1000 for management One copper 100/1000 Ethernet capture interface	2TB Total Storage Not redundant	1 RU x 14" (D) x 1.75" (H) x 16.8" (W)	Single 260 (W) 120/240V	25 lbs
NWA 1200-16D	Four 100/1000 Ethernet copper capture interfaces, Or two 1000 Ethernet fiber interfaces, Or two 10G XFP interfaces	12TB Total Storage Redundant with hotswap	2 RU x 27.75" (D) x 3.44" (H) x 17.6" (W)	Dual Redundant 850 (W) 120/240V auto switch	66lbs
NWP 50-16D	One copper Ethernet 100/1000 for management One copper Ethernet 100/1000 for capture One WiFi interface for capture	3TB Total Storage Redundant	Briefcase x 5.75" (D) x 11.5" (H) x 16.8" (W)	Single 520 (W) 120/240V	16 lbs

*All appliances are UL, FCC, CE and VCCI approved & RoHS Compliant

Concentrator and Broker

- As an enterprise, can you track malicious and anomalous activity and trends across all network assets?
- Are there relationships between unexplained network activities across your organization?

How can you build global reports regarding the effectiveness of your security controls?

NetWitness® Concentrator and Broker are high performance Linux-based network appliances that extend the reach of NetWitness NextGen™ across your entire enterprise, and facilitate real-time and historical reporting and alerting. For the first time, comprehensive network and application layer detail can be aggregated and analyzed across multiple capture locations and made available to NextGen's analytic applications, Informer and Investigator. NetWitness Concentrators aggregate clusters of NetWitness® Decoders in real-time, and NetWitness Broker provides a real-time, single, hierarchical enterprise view across your entire network. NetWitness® Live, fully integrated in the NetWitness infrastructure, provides users full content analysis of network threat intelligence from multiple, globally-distributed threat intelligence sources.

NetWitness Concentrator is designed to aggregate data hierarchically for ultimate scalability and deployment flexibility across various organization-specific network topologies and infrastructures. As a result, Concentrators can be tiered in deployments to give visibility into multiple capture locations.

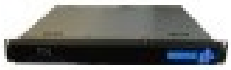
NetWitness Broker also is designed to operate hierarchically; however, its function is to broker queries across an entire enterprise deployment. Broker provides a single point of access to NextGen data and is designed to operate and scale in any network environment, independent of network latency, throughput, or data volume.
Concentrator and Broker are fully compatible with all NetWitness analytical products. For more advanced applications, users can leverage NextGen's available API/SDK to build organizational-specific applications which utilize the NetWitness NextGen™ infrastructure.

Product Features:

- Supports 10G infrastructures
- Supports NetWitness® Live
- 64-bit Linux-based, modular and fully upgradeable hardware platform across the entire product line
- Easily aggregate multiple NetWitness® Decoder collection systems
- Deploy a single enterprise analysis point with Broker
- Manage and configure appliances from a single point

- Indefinitely scale your collection infrastructure upon distributed, highly manageable, real-time framework
- Expandable SAS storage capacity & supports SAN solutions
- Available API/SDK for custom application development
- Supports RSA SecurID and LDAP authentication

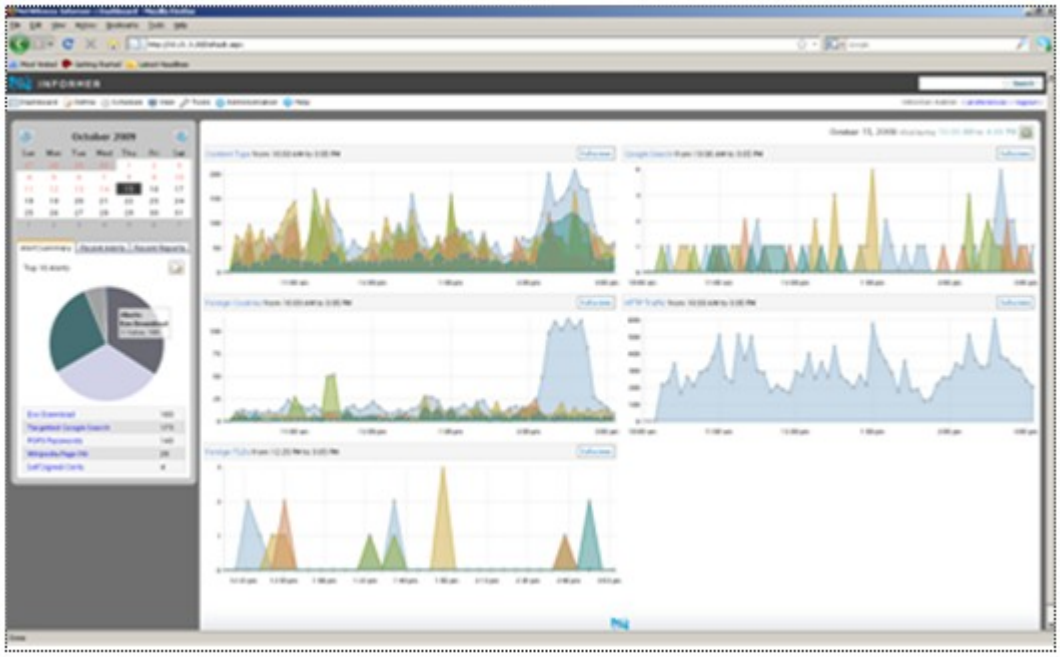
NetWitness® Appliance Models:

Product	SKU	Interface	Storage	Rack Unit	Power	Weight
Broker	NWA 100-8b 	Two copper Ethernet 100/1000	2TB Total Storage. Redundant	1 U x 16.8" (W) x 14" (D) x 1.75" (H)	260 W, stand alone 120/240V auto switch	25 lbs
Concentrator	NWA 400-16c	Two copper Ethernet 100/1000	4TB Total Storage. Not Redundant	1 U x 17.2" (D) x 25.6" (H) x 1.7" (W)	560 W, stand alone 120/240V auto switch	38lbs
Concentrator	NWA 1200-32c *	Two copper Ethernet 100/1000 Or two fiber Ethernet 1000	12TB Total Storage. Redundant with hotswap.	2 U x 17.6" (D) x 27.75" (H) x 3.44" (W)	850 W, Dual Redundant 120/240V auto switch	66lbs

All appliances are UL, FCC, and CE approved & RoHS Compliant.
*Also VCCI approved.

Informer

- Is your network communicating with Botnets?
- Is sensitive data leaking from your network?
- Does your organization have insiders whose activities are illegal or competitive?
- Are you monitoring operational regulatory compliance?



NetWitness® Informer is the enterprise reporting, live charting and alerting application of the NetWitness NextGen™ product suite. Informer leverages the power and Total Network Knowledge inherent in the NextGen data capture and session reconstruction infrastructure, and the analytics of NetWitness Investigator Enterprise to provide detailed reporting, charting and alerting on network performance, insider threats, data leakage, compliance monitoring, I/T asset misuse, hacker activities, and a host of other threats.

NetWitness® Informer is a revolutionary new approach to network reporting and alerting. Informer goes beyond traditional network reporting and alerting products on the market because it does not simply rely upon log files, netflow, or other limited data sets to generate reports. Informer uses the comprehensive network traffic that is captured and reconstructed by the NextGen infrastructure to provide a real-time glimpse into incidents, threats, anomalies, misconfigurations, compliance violations, and other malicious or benign activities on your network. Informer is a fully interactive, intuitive web-based report engine with design features that enable users of any level to create the perfect report without sophisticated programming or outside help. In addition, every report result is backed up with hard evidence, with one click into NetWitness Investigator Enterprise. And by integrating NetWitness Investigator Enterprise with NetWitness® Live, you also have access to multi-source threat intelligence.

Every network reporting product on the market today uses log files or complex network layer or flow information as its data source. Not only does NetWitness® Informer provide the type of insight provides by these products, but it also goes above and beyond to allow access to unprecedented details into network applications and application layer content. This efficiency allows users to replace dozens of reports from existing technologies, with a single Informer report. And it is this intersection of network metrics, rich application flow and content information that differentiates NetWitness® NextGen from any other capability on the market.

Deployment:

Connect NetWitness® Informer to any NetWitness® Decoder or NetWitness® Concentrator for reporting against that infrastructure

Product Features:

- Supports NetWitness® Live
- Hundreds of predefined report rules, categories and templates
- Flexible, WYSIWYG drag-and-drop report builder & scheduling engine
- Fully customizable, XML-based rules and report library for infinite report and alert combinations
- Live-charting for real-time dashboard of activity
- Full role-based access controls
- HTML and PDF report formats included
- Supports CEF, SNMP, SysLog, SMTP data push
- Offered as Windows® server software –or- integrated appliance for total flexibility

Report Examples:

- Security - profile and alert on zero-day, Botnet, DYN, DNS and intrusion activity with complete content
- Compliance - audit network-based components of policies and regulations such as FISMA, HIPPA, ISO 1779, SOX\GLB, and PCI standards
- IT Operations - report and chart across application and network layer metrics
- Business Intelligence - profile sensitive data flow in real-time with total access to all events and content surrounding suspect activity
- Insider Threat - monitor and profile computer, user, and resource activity across every application and device
- Legal – support e-Discovery, criminal investigations, or liability audits through network entity profiling and analysis

Screenshots:

NetWitness Informer features a fully customizable graphical user interface. Alerts can be viewed in real-time and multiple alerts and charts can be tiled into a customized view. **Download NetWitness Investigator Free!** Read More»

Minimum system requirements:

NetWitness recommends the following minimum hardware requirements for NetWitness Informer software.

- Windows® 2003 Server or Vista
- Microsoft IIS 5.0+
- 2GB RAM
- 1 Ethernet Port
- Internet Explorer v7 (also supports Firefox, Chrome and Safari browsers)
- .NET 2.0 with AJAX.NET Extensions

NetWitness® Informer Appliance:

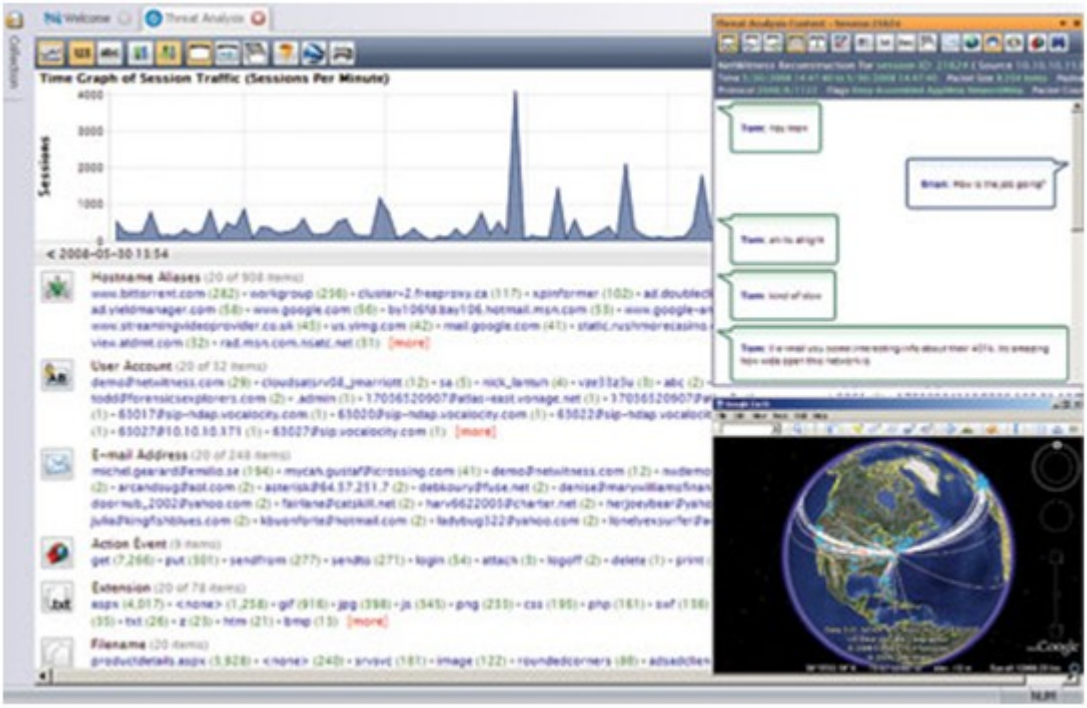
SKU	Interface	Storage	Rack Unit	Power	Weight
NWA 100-4i	Two copper Ethernet 100/1000	2TB Total Storage. Redundant	1 RU x 16.98" (W) x 14" (D) x 1.75" (H)	Single 260 W, 120/240V	25 lbs

*All appliances are UL, FCC, CE and VCCI approved & RoHS Compliant

Investigator

- How do you resolve alerts from your IDS or SIM that you do not understand?
- Can you quickly understand the scope and impact of malicious activity on your network?
- How can you investigate who is leaking information to your competitors or the press?

NetWitness® Investigator is the award-winning interactive threat analysis application of the NetWitness NextGen product suite. Investigator provides security operations staff, auditors, and fraud and forensics investigators the power to perform unprecedented free-form contextual analysis of raw network data captured and reconstructed by the NetWitness NextGen infrastructure. Developed originally for the U.S. Intelligence Community, and now used extensively by Law Enforcement, Defense, and other public and private organizations, Investigator is based upon 10 years of development and deployment in some of the most demanding and complex threat environments.



With its groundbreaking user interface and unprecedented analytics, Investigator lets you see your network traffic in a new way. Unlike packet analysis products which display network traffic in the context of confusing network nomenclature, Investigator uses a lexicon of nouns, verbs and adjectives – characteristics of the actual application and logic layer protocols parsed by NextGen during session reconstruction.

Both novice and expert users can use Investigator to pivot terabytes of network traffic easily to dive deeply into the context and content of network sessions in real-time -- making threat analysis that once took days, take only minutes. It is this intersection of network metrics, rich application flow, and content information that differentiates NetWitness® products from any other capability on the market today.
In addition to the rich data Investigator receives from the NextGen infrastructure of NetWitness Decoders and Concentrators, Investigator Enterprise can locally capture live traffic and process packet files from virtually any existing network collection device for quick and easy analysis. And by integrating NetWitness Investigator Enterprise with NetWitness® Live, you also have access to multi-source threat intelligence.

Product Features:

- Supports NetWitness® Live
- SSL Decryption (with server certificate)
- Interactive time charts, and summary view
- Interactive packet view and decode
- Hash Pcap on Export
- Enhanced content views
  - Real-time, Patented Layer 7 Analytics
  - Effectively analyze data starting from application layer entities like users, email, address, files , and actions.
  - Infinite, free-form analysis paths
  - Content starting points
  - Patented port agnostic service identification
- Extensive network and application layer filtering (e.g. MAC, IP, User, Keywords, Etc.)
- IPv6 support
- Captures live from any wired or wireless interface
- Full content search, with Regex support
- Exports data in .pcap format
- Imports packets from any open-source, home-grown and commercial packet capture system(e.g. .pcap file import)
- Bookmarking & History Tracking
- Integrated GeoIP for resolving IP addresses to city/county, supporting Google Earth visualization
- Customizable right-click functionality
- Supports WLAN 802.11 Microsoft, Linux and Mac OS radio devices as well as various header formats including CACE's per packet information
- Supports RSA SecurID and LDAP authentication

Choose your Edition:

No matter what your IT problem, existing infrastructure, or technology preference—there's an edition of NetWitness® Investigator that's right for you. Use the descriptions below to help you choose your edition.

Investigator

With Investigator you are provided with a full featured, stand-alone product capable of local live capture and local packet file importing. Ideal for tactical and point analysis of network traffic. Supports 25 simultaneous 1GB captures - far exceeding data manipulation capabilities of packet tools like Wireshark

Investigator Enterprise

Licensed to customers with a NetWitness NextGen™ infrastructure, Investigator Enterprise is ideal for enterprise users that require remote analytical access to NetWitness NextGen™ Linux-based appliances.

Deployment:

NetWitness Investigator is licensed per computer host, and can be used to locally process packet files, collect live from a network tap or span port with insight into network traffic of your choice. In addition, Investigator is fully integrated with all NetWitness NextGen™ products.

Screenshots:

NetWitness Investigator's industry leading interactive user interface provides the threat analyst the ability to drill into multiple dimensions of terabytes captured traffic across all network layers. View complete information about any network sessions by drilling into fully reconstructed content and visualize your network traffic geographically via Google Earth.

Minimum system requirements:

NetWitness recommends the following minimum hardware requirements for NetWitness Investigator:

- Windows® 2003 Server or Vista 32-bit
- Single 2Ghz Intel-based processor (Dual-core recommended)
- 1GB RAM (2GB Recommended)
- 1 Ethernet Port
- Internet Explorer v7+ (IE v6 may limit some functionality)
- Ample data storage to process and collect

To buy NetWitness or to find out how to integrate NextGen with enterprise SecureGRC™ integrated IT-GRC and security framework click here