



## NETWITNESS 7.0 PRODUCT SNAPSHOT

### FEATURES

#### ► **Live Capture**

*Collect and filter at Gigabit Ethernet speed.*

#### ► **Packet File Import**

*Import, process, and analyze tera-bytes of external data.*

#### ► **Application Layer Analytics**

*Effectively analyze data starting from application layer entities like users, email addresses, files, and actions.*

#### ► **Content Search**

*Search content in every single network session.*

#### ► **Both software and hardware solutions available.**



## Instantly Respond to Network Incidents and Investigations with NetWitness 7.0

***NetWitness 7.0 is a network investigation and incident response product that provides unprecedented network traffic analysis capabilities. NetWitness 7.0 enables users to forensically collect and rapidly process raw network traffic, providing visibility and context to investigatory needs across the enterprise.***

### KEY BENEFITS

#### ***Unmatched Analytics***

Based on over 9 years of development, the patented collection, processing, and analytical methods of NetWitness 7.0 provide deep insight into network entities, their behavior at the application layer, and provides the actual session content for analysis. The network context that NetWitness 7.0 provides is unlike any other product available, because it was designed from the ground up to model and analyze traffic, not simply "monitor" it.

#### ***Incident Response & Investigations***

Responding to and investigating network incidents can be time-consuming and frustrating without the right solutions. And, with zero-day attacks, you need answers fast. NetWitness 7.0 provides an intuitive, easy-to-use interface that allows you to isolate and definitively determine the intent, magnitude & scope threats, whether external or internal. With NetWitness 7.0, what would typically take hours or days to resolve, can take only seconds.

#### ***Enhance Existing Network Security Infrastructure***

Today there is a large successful market of mature products that focus on the identification of threats or problems. Network technologies like IDS/IPS, SEM, Anti-virus, Content Monitoring, and fraud detection, to name a few, do an excellent job of identifying an event that often triggers the starting point of an investigation. NetWitness 7.0 enhances existing log based, network layer & host based security products by providing effective investigations for event resolution. By eliminating the need to infer on triggers and events, you gain total insight and context of and around network incidents.

#### ***Deployment Strategy***

NetWitness 7.0 can be deployed in a live collection mode as well as process pre-collected packet files from other systems. In addition, it is an integral component to the NetWitness investigative framework that enables enterprises to perform network wide investigations.

