# NetWitness® Logs

NetWitness® Logs is a security monitoring and forensics tool that collects, analyzes, reports on and stores log data from a variety of sources to support security policy compliance and regulatory compliance initiatives. The solution is modular and scalable and can be deployed across any type of enterprise. Unlike other log-centric SIEMs, NetWitness Logs parses, enriches and indexes logs at capture time, creating sessionized metadata that serves to dramatically  accelerate alerting and analysis.

NetWitness Logs supports collection over a wide range of protocols, including Syslog, ODBC, SFTP, SCP, FTPS, SNMP, Check Point LEA, WinRM and more. It ingests logs from more than 350 event sources, including various industry-leading network and security devices, popular applications and operating systems. Additionally, it stores raw logs and extracts metadata. The ability to centrally monitor logs no matter their source and deploy collection components on-premises, virtually, across hybrid architectures or completely within public clouds like  Amazon Web Services (AWS) and Microsoft Azure and applications like Microsoft Office 365 and Salesforce makes NetWitness Logs a versatile solution. Pervasive log visibility facilitates administration and analysis of data across distributed and virtual environments, which enables rapid detection, investigation, reporting and management of all log data.

## Compliance

The NetWitness Logs solution includes compliance use cases and prebuilt templates for SOX, PCI, HIPAA NERC and many other regulations.

## Reporting

NetWitness Logs gives you the flexibility to customize views and formatting for reports. Predefined reports comprise one or more rules that you can also leverage within other custom-built reports.

## Automation for log discovery

If you are understaffed or overburdened with constantly changing diverse environments to monitor, the NetWitness Logs discovery workflow eases  these challenges. Unlike other log collectors that require manual configuration,  NetWitness Logs has automated heuristic parsing to aid security teams in rapidly ingesting new sources. New "dynamic parsing" technology automatically

## Compliance and reporting

- Compliance reports consist of Account Create/Delete/Modify; Admin Accesses to Compliance Systems; User Accesses to Compliance Systems; Escalation of Privileges; Firmware Updates; Configuration Changes; Successful Remote Access, etc.

- Regulations that have specific reports include, for added convenience:
  - Basel II
  - Bill 198
  - Family Educational Rights and Privacy Act (FERPA)
  - Federal Financial Institutions Examination Council (FFIEC)
  - Federal Information Security Management Act (FISMA)
  - Gramm-Leach-Bliley Act (GLBA)
  - Good Practice Guide 13 (GPG13)
  - Health Insurance Portability and Accountability Act of
  - 1996 (HIPAA)
  - International Organization for Standardization 27002 (ISO 27002)
  - North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- National Industrial Security Program Operating Manual (NISPOM)
  - Payment Card Industry (PCI)
  - Sarbanes-Oxley Act of 2002 (SOX)
  - Statement on Standards for Attestation Engagements No. 16 (SSAE)

renders raw data from most log sources and provides immediate access to critical security data in the form of useful metadata. The automatic parsing of new log sources helps organizations adapt to the ever-increasing variety of log sources.

Log sources that do not have a corresponding parser will be processed automatically against rules. Metadata will be extracted automatically based on rules, and the metadata will be available for Enrichment, Investigation, Reporting and Alerting from new sources. Automation of log parsing provides immediate visibility into logs from new, custom or unsupported sources.

For more challenging logs, the NetWitness Log Parser Tool helps users easily create parsers for new, unsupported or custom event sources. Additional support for custom log parsing is also available via the RSA Link community.

## Speed and versatility

NetWitness Logs makes it possible to configure and selectively manage retention of raw data and metadata. Short-term retention provides extremely fast access to data. Longer-term retention balances the needs for cost-effective storage and indexed access for compliance purposes.

## User and entity behavior analytics

NetWitness Detect AI delivers cloud-native advanced behavior analytics that leverages unsupervised machine learning to enable high-fidelity threat detection without the need of traditional signatures.

## Flexible bandwidth management

To manage bandwidth challenges, administrators can control what is pulled and aggregated from satellite offices to centralized locations. NetWitness Logs provides options to limit pull protocols with preset limits for quantity and the types of logs collected. This includes the compression and encryption of log data that is processed and aggregated between different components in the architecture.

## See beyond the clouds

You can deploy NetWitness Logs within private, public or hybrid cloud architectures. In addition, you can easily monitor Office 365 environments or Salesforce applications. Modular components can be deployed virtually and within public clouds, including AWS and Amazon, to enable visibility across complex cloud environments.

## Endpoint visibility

NetWitness Endpoint Insights offers essential endpoint inventory scans paired with Microsoft Windows log forwarding and filtering capabilities to reduce the costs and complexity of investigating threats. NetWitness Endpoint Insights is a purpose-built agent to provide visibility into host configurations,  process details and user context as well as simplifying  the monitoring of Windows logs.

## Evolve beyond logs

Extend threat detection capabilities beyond just logs with the NetWitness Platform. NetWitness Logs integrates seamlessly with other modular components of the NetWitness Platform, including NetWitness Network, NetWitness Endpoint, NetWitness Detect AI and NetWitness Orchestrator. This tight integration and a unified platform extend your visibility, creating correlated metadata with the power of an evolved SIEM across your network with visibility to logs, packets, NetFlow and endpoints for faster detection and response.