What’s New

NetIQ Sentinel

NetIQ® Sentinel™ provides organizations with an efficient security information and event management (SIEM) solution that merges real-time intelligence with identity monitoring and anomaly detection, to provide accurate assessments of IT activities and threats. Easy to both deploy and use, Sentinel delivers SIEM technology with incredible time-to-value.

What’s New Over the Last 2 Years

- Replaced Oracle JDK with Azul Zulu OpenJDK, an open source alternative.
- Regulate users who can send events or attachments from Change Guardian and Secure Configuration Manager to Sentinel.
- Certified on new platforms*: RHEL Server 6.10 and 7.6 (64-bit), SLES 12 SP4 64-bit, Elasticsearch 5.6.13, and Microsoft Windows Server 2019.
- Limit the number of concurrent active sessions per user to slow attackers.
- Sentinel can now be configured to terminate sessions and log out inactive users.

Did You Know?

- Sentinel ships with packaged intelligence to detect many threats out-of-the-box, without time consuming configuration.
- It offers seamless integration with NetIQ Identity Manager and Change Guardian.
- Sentinel includes contextualized identity and change monitoring intelligence, with built-in rules and anomaly detection.
- Can leverage ArcSight’s industry-leading SmartConnector Framework.
- Sentinel offers a Big Data (Hadoop) backend that can collect and store large amounts of data quickly and efficiently.

New York City Health and Human Services

“Using Sentinel and Sentinel Log Manager, we’re better prepared for audits and can minimize the risk of security breaches.”

JOE FLEISCHMAN
Project Manager, Office of the CIO

State Grid Shanghai Municipal Electrical Power Company

“The native integration between Sentinel and our Micro Focus unified identity system allowed us to introduce many more security features without having to change our system architecture”

MR LU SHIDA
Director

*Platform certification can vary by deployment (traditional, appliance, data indexing, etc.)