



TriGeo nDepth™

Explore. Discover. Respond.

Explore

The devil is in the details, which is why IT departments and auditors need fine grained control over the information they collect and the tools to explore it.

TriGeo nDepth™ is the first IT Search network security appliance designed to blend real-time event correlation, deep forensic analysis and point and click response. The result is that IT departments now have a platform that can capture and review plain-language alerts, dive deep into the underlying logs and proactively respond to suspicious and malicious activity.

Deep Dive

nDepth gives enterprises powerful search functionality for highly granular forensic analysis of network events – encompassing all users, devices and applications.

TriGeo's IT Search solution aggregates and archives all log data in real time, with patented data collection, storage and indexing technology that delivers secure, fast and repeatable searching across terabytes of data.

Leveraging TriGeo's proprietary agent technology, nDepth ensures complete "chain-of-custody" log management with a process that is both secure and bandwidth friendly.

Discover

Like the search engines we use every day, nDepth empowers IT teams to follow the forensic thread wherever it leads and discover the root cause – whether it's network troubleshooting, security incident investigation or policy enforcement.

Unbeatable Combination

nDepth is an add-on appliance designed to complement TriGeo SIM by linking real-time alerts with the underlying network activity.

While data is analyzed and events are correlated by TriGeo SIM, they're simultaneously indexed and archived by TriGeo nDepth.

The nDepth data can be explored at any time, for any reason, across any period, but when events do occur nDepth surfaces the details needed to take forensic analysis to a whole new level.

Respond

TriGeo nDepth integrates completely with TriGeo SIM to provide a single, seamless console for real-time event analysis, forensic exploration and point and click remediation.

TriGeo SIM is the only Security Information and Event Management



(SIEM) solution that proactively defends the network with unique active responses that include the ability to quarantine, block, route and control services, processes, accounts, privileges and more.

Learn More

TriGeo extends the reach of IT teams with a unique combination of real-time analysis, event correlation, IT search, business intelligence and active response.

To learn more, visit us on the web, register for a live presentation or give us a call at 1-866-664-9292.

TriGeo nDepth Hardware Specifications

nDepth is packaged as a 2U rack-mount appliance designed for high-speed data collection, indexing, analysis and long term storage. It supports a multi-appliance distributed search and storage model as well as off-line data archival and restoration.

nDepth Appliance

RAM: 8GB
CPU: Dual 3GHz, Dual-Core
OS: Hardened Linux
Data Capacity: 2TB, RAID 5

nDepth Console*

RAM: 1GB (minimum)
CPU: Single 1.5GHz+
OS: Windows XP, Vista, Linux
Disk: 100MB

*Integrated with TriGeo SIM Console



www.trigeo.com