5.2

LogPoint 5.2 delivers cutting edge features in the SIEM market space

When collecting logs from systems and applications, LogPoint extracts key events from the logs. These events are stored in cutting-edge NoSQL and search is carried out using Big Data technologies.

This enables LogPoint to collect more than 10.000 events and search in millions of logs per second on a single server - even on low-scale hardware!

LogPoint supports the use of SSD and hybrid disk-drives to enable even faster performance, enabling complex analysis and correlation of multi-million events per second.

SEARCHES

When searching for security events, LogPoint demonstrates unparalleled performance – However, performance is less valuable without context.

LogPoint delivers a rich and easy to use search syntax. Supporting the syntax are thousands of pre-defined searches, correlations and classifications of events - delivering the intelligence directly to the security or operations analyst.

Expanding further on the capabilities of searches in LogPoint; with version 5.2, it is now possible for operators to pass search results to custom-developed scripts inside LogPoint. This allows operators to conduct DNS-lookups of an IP address and extend the normalization with the resolved hostname. LogPoint will even let operators write their own Python scripts and can pass one or more field-value to the script and append the reply from the scripts in the logs.

REPORTING & DASHBOARDS

With the latest version of LogPoint, more than 1.000 new reporting and dashboard-elements have been added.

LogPoint now has hundreds of elements for detecting anomalies in the network.

LogPoint delivers real-time dash-boards to identify malicious traffic and deviations from the norm.

This enables both security and network operators to focus on remediating instead of searching for issues!

COMPLIANCE

LogPoint 5.2 supports GPG13 (Good Practice Guide) out-of-the-box, enabling organizations to use LogPoint as a turn-key solution for achieving compliance and improve the company risk profile.

With LogPoint for SAP, organizations achieve full anomaly detection, critical changes to master-data, correlations on business violations etc. out of the box, with easy customization and expansion.

LogPoint delivers one common language for security intelligence – across the entire enterprise landscape of IT.

IMPLEMENTATION

Implementing LogPoint is simple. The product is shipped in a virtual appliance, physical appliance or as a piece of software, allowing organizations complete flexibility in deployments.

LogPoint does not rely on specific hardware, but runs on commercial-off-the-shelf solutions, SAN/NAS/Local storage - mix and match it however you see fit.

Because the solution is hardware-agnostic, organizations are able to orchestrate storage for LogPoint that is both cost-effective and performance-optimized.

SCALING

Scaling and distributing LogPoint across data centers, within geographical regions or across the globe is considered easy - a couple of clicks and full-scale replication and clustering is primarily enabled. Searching, reporting and alerting through billions of logs from around the globe is a simple as identifying which systems to include in the search, if you are unsure then select all the systems and let our lightning fast indexing service find the relevant events!

LICENSING

LogPoint is licensed on the number of devices sending logs to the system. This means organizations can scale to as many LogPoint servers as needed, while maintaining transparent cost-projections.

LogPoint scales with the needs of any enterprise.

LogPoint. SIEM. But different.

Plain and simple has never been so unique

SIEM. But different.
When it comes to Information Security, LogPoint is easy to use, agile by design and intuitive by nature. Find out about more about how your enterprise can benefit from the LogPoint difference.

Contact us for more information:

logpoint

LogPoint A/S
Aldersrogade 6A
2100 Copenhagen O

E-mail: info@logpoint.com
Telephone: +45 7060 6100