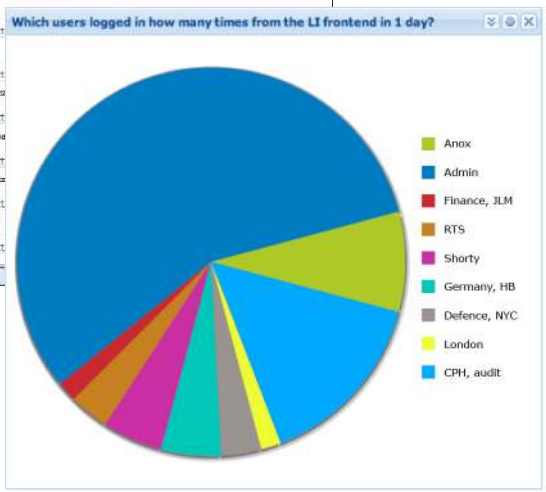
LogPoint 5 Product Features

Robust. Dynamic. Unparalleled.

logpoint

Enjoy ultra fast search capabilities – in simple and complex modes – optimized for 'Big Data'

Easily filter and display relevant topics, eg: 'Top 10 Denies'



LogPoint - transforming SIEM solutions into business value

Most organizations today realize and accept that a SIEM solution adds clear business value on several fronts, including:

- Automation of regulatory processes
- Improved efficiency in forensic investigations
- Increased troubleshooting turnaround time
- A widely improved security position

The **LogPoint** platform intelligently extracts events and incidents from the billions of logs existing in any IT infrastructure of any size. Filtered and carefully correlated results are displayed in easy-to-manage Dashboards that can be configured based on the specific roles and responsibilities of each user.

LogPoint collects and stores data – from any source

LogPoint provides a secure, centralized log archive that automatically analyzes log messages in real time. Log consolidation and safe storage of evidence provide a single interface for accessing and managing all information.

Once raw, unaltered log data collected from across the Enterprise is received, it is stored in archives subject to integrity checks per the log management standard (the NIST 800-92 SHA-1 hashing algorithm).

LogPoint analyzes and alerts automatically

The built-in intelligent log analysis engine automatically detects and notifies of all critical incidents. Events monitored can be very diverse and can include an ongoing attack, a compromised system, a system breakdown or user authentication, and much more.

LogPoint's powerful search engine

LogPoint has its own, unique search language – making it easy to search for specific information within the logs.

This includes an advanced labeling structure that allows for highly efficient log tagging. Any search – from simple to advanced – can be converted on the fly into a permanent Dashboard. Searches can also be reported for easy future reference. And the advanced log analytics make it easy to display data in the best possible fashion.

LogPoint Dashboards

Security Event Management is much more valuable if the information collected can be presented and found with little effort. **LogPoint** presents information through a structured overview, allowing you to quickly spot new trends and drill down any information.

LogPoint – simplifying auditing and compliance

LogPoint can help you achieve complete insight to your network, making it easy to meet common regulations thanks to built-in templates based on the most common compliance and security reports, including:

- PCI-DSS
- SOX
- HIPAA
- Basel-II
- ISO27001

LogPoint 5 – the next level in Asset Security

With LogPoint 5, LogPoint has launched the 5th generation of its SIEM platform – bringing asset security to an entire new level.

Enterprise ready

Thanks to unparalleled correlation, **LogPoint 5** can now analyze data across a diverse array of systems for true Enterprise-wide implementation.

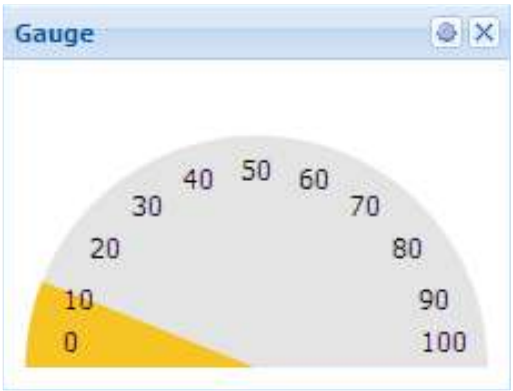
Dynamic data integration

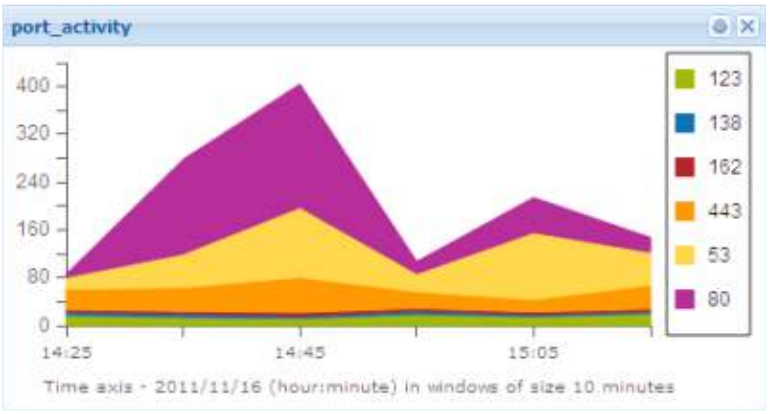
LogPoint's reliable logging solution is now matched with dynamic data enrichment capabilities, integrating external data such as enterprise databases, IT asset management information or even data from an Internet portal.

Requirement ready

LogPoint 5 is built to satisfy any requirements mandated by:

- Compliance
- Threats & Forensics
- IT operation visibility





LogPoint displays data in easy-to-read gauges and diagrams.

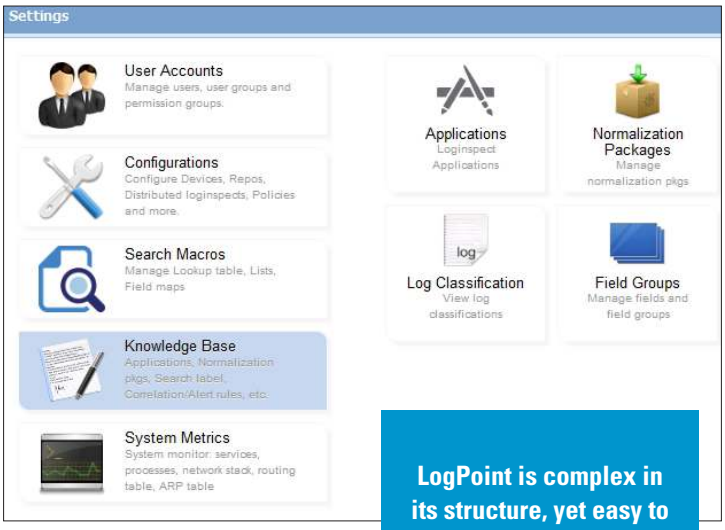
LogPoint – Your dedicated security partner

LogPoint is dedicated to delivering customer-focused applications within IT security, particularly Security Information and Event Management (SIEM).

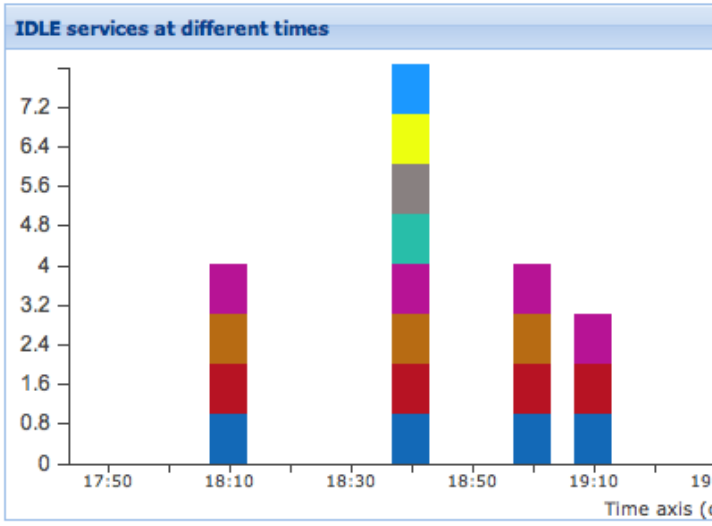
We have a long history of partnering with our customers, listening and continuously adapting to match their needs.

Our software solutions are characterized by ease of deployment, ease of use, ease of management and outstanding global support.

logpoint



LogPoint is complex in its structure, yet easy to configure and manage.



Out-of-the-box implementation

Risk Assessment

Confidentiality, Integrity, Availability (CIA). This well-known model enables operational implementation of a calculated threat impact score. It can be based on your personal risk analysis, placing focus on the most important events as aligned with, e.g., an internal IT security strategy.

Dashboard – for ease of control

Based on web 2.0 design models, **LogPoint**'s advanced Dashboard technology allows users to individually configure the Dashboard to reflect desired views based on a user's role in an organization. The Dashboard displays critical Events and Security Incidents in real-time.

Data Enrichment

LogPoint makes it possible to enrich your necessary log messages with information from other sources, such as CMDBs, the Internet, Portals or any other data source. This can be a static or dynamic process.

Application and database monitoring

LogPoint provides performance and availability metrics from any database log, including:

- Trigger alerts based on database activities and commands
- Detection of policy violations
- Inspection of application traffic content

Event Correlation

LogPoint's Event Correlation Engine can detect patterns of events, such as:

- Missing parts of a business transaction
- Mismatches between log messages and external data sources
- Brute force attempts
- Security incidents

Active Response Engine

LogPoint's Active Response Engine provides for automatic, valuable measures, such as:

- E-mails alerting to detected security incidents
- Automatic system triggers from specific events, such as blocking an IP in the Firewall, or shutting down users if suspicious security incidents occur
- Integration into existing ticketing and support systems

Rules and signatures via powerful application structure

At **LogPoint 5**'s core is a strong application structure that enables easy implementation of new security rules, Dashboards, searches, reports and more… ensuring that all customers are always up to date.

LogPoint can also adapt to other proprietary formats.

Out-of-the-box reporting

Common reporting templates for compliance such as PCI, SOX, ISO2700x, HIPAA and more are standard to the **LogPoint** solution – and can be modified or created from scratch using an intuitive **LogPoint** Report Wizard.

Built-in scaling

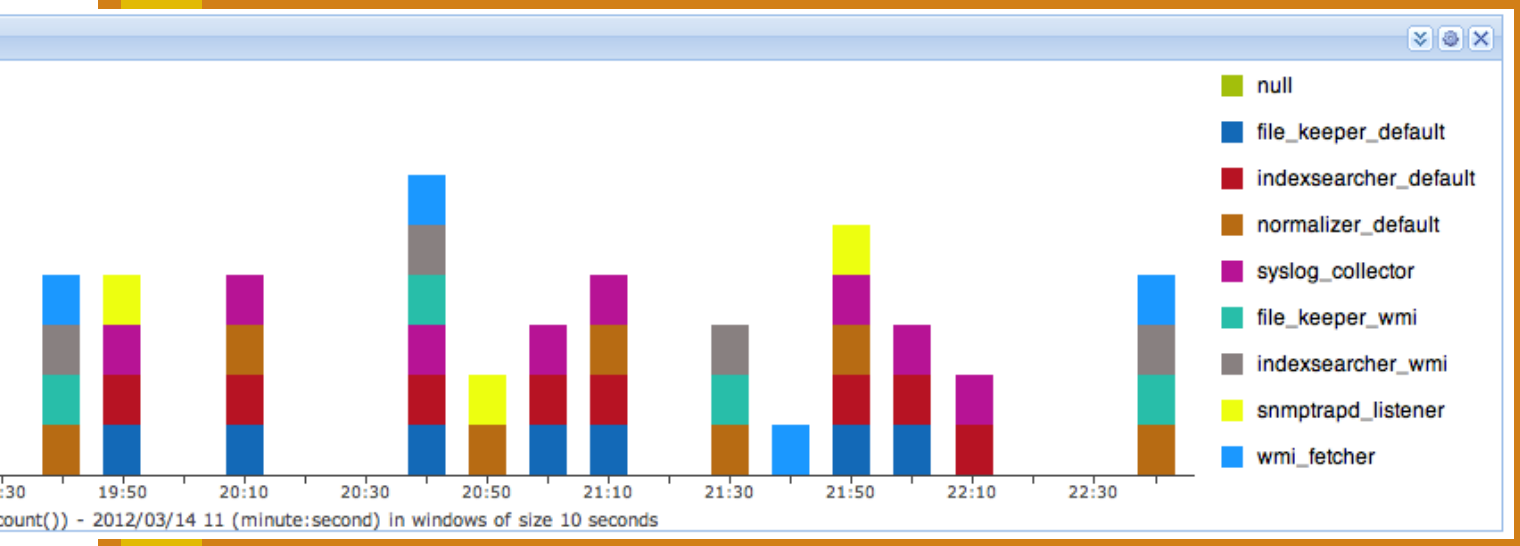
LogPoint offers built-in scaling architecture, enabling enterprise-wide implementation that combines any hardware and virtualized appliances. Searches and reports can include any subset of any distributed **LogPoint** servers across the network.

System requirements

LogPoint is delivered as a preconfigured appliance based on any common brand of hardware, VMware or HyperV – enabling ultimate flexibility in terms of deployment.

License model

The software is licensed through an annual subscription that includes all new upgrades, patches, signature subscriptions, and e-support through the LogPoint Ticket System.



LogPoint is a powerful SIEM tool with endless customizable search and monitoring functionalities.

Unique, heavy-volume data performance

Powered by NoSQL

Traditional relational databases have proven to perform poorly when processing heavy volumes of data. **LogPoint** is powered by the latest NoSQL technologies, better known as a 'document database'.

The **LogPoint** technology enables the receiving and real-time normalization of billions of logs a day – with techniques commonly used by Google, Amazon, Facebook and other heavy data companies

ISO 27001 Compliance

More information:
www.logpoint.com

logpoint

Corporate Headquarters
LogPoint A/S
Aldersrogade 6A
DK-2100 Copenhagen O
Denmark
Phone: +45 70 266 286
Fax : +45 70 266 287
E-mail: info@logpoint.com

More information:
www.logpoint.com