

logpoint

COMPLIANCE MANAGEMENT

One of the most common motivators for initiating a SIEM regime is the need to tick all compliance boxes.

But how can you assure a SIEM solution will cover all the bases? What should you look for to assure you will always meet your enterprise's specific compliance requirements?

SIEM. BUT DIFFERENT.

Compliance Management

EASY IMPLEMENTATION

Tactical SIEM projects that are aimed at satisfying one single requirement – such as compliance – often face extreme time limitations.

When the need to meet compliance requires that your organization's IT team focuses on implementing a SIEM tool, it is clearly crucial that this tool is easy and simple to implement.



Compliance Management

EFFICIENCY

LogPoint offers you the highest level of out-of-the-box compliance within the shortest timeframe.

This means that your security team can spend time on what is important: pin-pointing which systems should be included under the “compliance umbrella” and which data should be monitored and reported.

Building blocks

LogPoint’s reports have been specifically developed to cover the broadest spectrum of regulatory domains. An enterprise can easily select those specific areas that should be included in its reporting, or modify these elements when needed – instead of crafting custom reports from the ground up. It offers a catalogue of various building

blocks – including descriptions and documentation – for organisations to choose from according to their individual requirements. Block by block.

The LogPoint approach

LogPoint monitors the key system objects and components found in any enterprise, including networking equipment, servers, applications and databases.

By monitoring and correlating from a common language, LogPoint provides a simple, transparent view into business events. It also delivers the accountability and manageability that security events need to assure not only that regulatory compliance requirements are met, but that these events can be handled efficiently.

LogPoint’s flexible architecture and features mean that security resource time can be spent on vital daily business operations.

LogPoint.
*Plain and simple
has never been
so unique.*

LogPoint provides intelligent insight into:

- Who did what, why and when.
- A complete, transparent overview of the business processes.
- An analytical engine needed to automatically and manually make sense of an event.

Out of the box

LogPoint also delivers a complete set of compliance reporting elements for regulatory domains such as:

- PCI-DSS
- SOX
- ISO27001 and ISO27002
- HIPAA
- FISMA
- BASEL-II

Additional security

In addition, LogPoint provides a range of more detailed security monitoring reporting elements, including:

- DSAG SAP Security guidelines
- Extensive infrastructure reporting with data from Next Generation Firewalls
- Enterprise Mobile Device Management reporting domains

Wide-reaching benefits

SIEM is often initially implemented as a tactical, point-solution for Compliance Management. But a sound SIEM programme can wind up providing you with additional key insights and security intelligence in the process – quickly turning a SIEM installation into a strategic means that can be applied to the broadest benefit of your enterprise.

SIEM. But different.

When it comes to Compliance Management, 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