Compliance Management, made easy
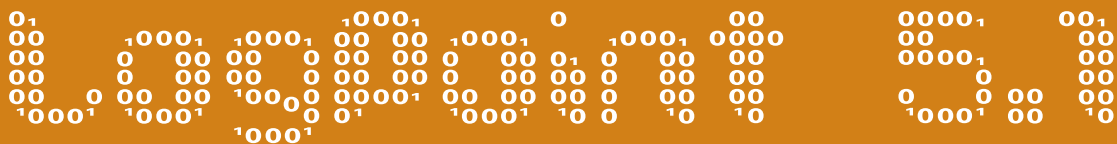
logpoint 5.1

logpoint

LogPoint 5.1:
*Protecting your data,
intellectual property
– and your company*

Log and Compliance Management in one solution

Managing security infrastructures to meet compliance requirements can be an easy, efficient process – with **LogPoint.**

Compliance Management – a daunting task

Security compliance requirements are normally a highly time-consuming and expensive task. Companies must not only interpret audit requirements and controls, they must also face the huge task of managing extreme volumes of log data – all the while facing multiple regulations at federal, state, and industry levels.

Not only are these mandates costly and complicated, failure to comply can result in huge financial losses from fines, notification costs, legal issues and damaged reputations.

Log Management – a blessing in disguise

Nonetheless, regulatory compliance has been designed to help you maintain thorough security intelligence and adequately report on your security environment. Both

are necessary for protecting your enterprise, no matter what type of organization you are. Though these important regulations vary, they all require the collection and storage of event logs.

Log management is clearly the foundation basis for meeting compliance, but it is also the first step towards a truly effective security strategy. Sometimes a company will choose to implement multiple complex and costly security solutions. By taking the right choices and focus on the core issues, you will be surprised how quickly you can reach compliance requirements.

LogPoint – quick, easy, efficient

With years of experience in Compliance Management, LogPoint has designed **LogPoint** to help you achieve your compliance obligations quickly, easily and efficiently.

Security regulations vary between industries, but share very similar basic

requirements. LogPoint can help you meet these day-to-day regulatory requirements by:

- **Automatic data collection** for all types of event data across the network
- **Storing event logs** for easy access to complete, secure audit trails
- **Rapid threat response** for identification, remediation and reporting
- **Alerting** of policy and compliance violations
- **Validating** that controls are in place and optimized
- **Correlating** volumes of diverse events – to uncover the core issue from the beginning
- **Documenting** incidents, including detailed auditable records
- **Out-of-the box and customizable** compliance reporting.

ISO 27001 Compliance

Information security best practices

Established by the International Organization for Standardization, ISO 27001 are regulations that provide best-practice recommendations for information security management. Importantly, ISO 27001 provide guidance to those responsible for initiating, implementing, and maintaining information security management systems, in an effort to:

- **Prevent unauthorized users** from gaining access to business systems and confidential company data
- **Safeguard** the accuracy and completeness of information and processing methods
- **Ensure necessary access** to information and associated assets for authorized users.

Security solutions
In order to establish an appropriate code of practice for information security management, in alignment with the ISO 27001 standard, security controls must be implemented across your IT infrastructure. Complying with Communications & Operations Management and Information Security Incident Management means that data must be monitored and analyzed throughout your network, systems, applications, and databases.

But in order to achieve these affordably and reliably, the right automated security solutions are needed, ones that offer:

- End-to-end data correlation
- In-depth analysis
- Detailed reporting that matches the ISO 27001 mandates.

LogPoint and ISO 27001
The stringent requirements for ISO 27001-compliance call for adopting a security compliance management strategy that employs both security information and event management (SIEM) and log management solutions. **LogPoint** offers both of these – allowing for the collection and analyzing of log data while enhancing your security practices to protect your applications and databases from insider threats. But it also delivers real-time actionable security and ISO 27001-compliant information throughout your enterprise.

The **LogPoint** SIEM solution can empower you to continuously manage risk while leveraging recognized security best practices — including ISO 27001 best practices.

More than a log management solution
Log management is clearly important for meeting ISO 27001 requirements, validating that proper controls are in place, and delivering the desired compliance results. But while other log management solutions simply collect, store, and report on raw event logs, **LogPoint** solutions offer more.

Thanks to multiple layers of patented correlation technology, log management transforms into in-depth log visibility across your organization. By correlating all logs, **LogPoint** provides a complete and

clear understanding of events, patterns, and trends in real time – so that attacks can be stopped before they reach important data.

The **LogPoint** solution can also perform historical analytical correlation of disparate events. Normalization and categorization capabilities deliver quick, actionable analysis of real-time event management.

Effective security compliance management
LogPoint is an effective security compliance management suite that can help you meet even the toughest ISO 27001 and security intelligence challenges, such as:

- **Decreasing time and resources** spent on compliance requirements
- **Monitoring and measuring** the effectiveness of PCI compliance controls
- **Providing information** to third-party auditors for compliance evaluations
- **Securely capturing and storing** event logs for evidence and enforcement
- **Correlating event data** from all your devices and applications
- **Delivering real-time visibility** into threats against compliance related assets
- **Immediate detection and alerting** of control and policy violations
- **Out-of-the-box and customizable** ISO 27001 reports and rules.

More information:
www.logpoint.com

logpoint

LogPoint 5.1:
Protecting your data,
intellectual property
– and your company

Sarbanes-Oxley Act (SOX) Compliance

SOX – security best practices & proactive risk management

The Sarbanes-Oxley Act (SOX) was designed to protect investors by improving the accuracy and reliability of corporate disclosures made in accordance with securities laws. SOX standards must be followed or companies face strict penalties for noncompliance.

SOX encourages auditors to take a proactive, risk-based approach in evaluating internal controls for a public company's financial reporting. All compliance-related data and applications need to be monitored and secured throughout an enterprise at both the application level and network activity level.

Adopting a true policy-driven security program, however, presents significant challenges. To meet SOX requirements, success must be tracked and proven in measurable risk reduction. Auditable internal controls must be established, including:

• Logs, incident reports, alerts, and IDM systems
• Application session information
• Across your entire organization on different platforms.

A properly implemented risk-based approach to auditing for SOX compliance can make SOX more manageable. It can also reduce the associated cost and help ensure the adequacy of controls and the integrity of financial reporting.

LogPoint SOX solutions

The **LogPoint** solution is a cost-effective approach to proactively managing risk across your network, systems, applications, databases, and user activities while enabling SOX compliance. It delivers reliable, end-to-end security monitoring and incident management processes around financial applications, data, and the IT systems that support them. By deploying an effective security compliance management solution, a company is equipped with a set of tools that allows it to meet SOX obligations.

Log management and beyond

Log management is an important foundation in a SOX compliance strategy. It enables the collection, storage, and reporting of event logs and proves that adequate controls are indeed in place. Yet log management is only one element in an effective approach to SOX compliance. **LogPoint** goes beyond merely collecting and storing event logs and leveraging advanced correlation capabilities – it prevents and mitigates even the most advanced threats.

SOX compliancy and secured infrastructure in one

With **LogPoint**, a company can achieve security best practices and continuously manage risk through:

• Data collection
• Log management
• Real-time monitoring
• Threat identification
• Rapid response
• Actionable reporting

LogPoint helps you meet SOX compliance, allowing you to:

• **Prove diligence** in managing information security risk, with detailed documentation that continually prepares for potential audits
• **Monitor and protect** financial databases down to the record level, securing data as it moves throughout applications
• **Centrally collect and store** audit trails from financial databases and applications, correlating them with network security devices
• **Respond rapidly** to material events such as a data breaches, notifying appropriate parties and taking remedial action.

PCI – the Payment Card Industry Data Security Standard

PCI mandates that merchants and service providers storing, processing, or transmitting credit card data must comply with a multitude of requirements. The consequences of not meeting compliance are costly and include fines, notification costs, legal issues and brand damage.

Effective PCI implementation

With the increasing constraint on budgets and resources, it is becoming more challenging for companies to implement effective PCI compliance programs – not to mention to ward off attacks and protect data. But companies can turn this challenge into their favor by elevating it from an ad-hoc exercise to an ongoing process – continually collecting data, monitoring, measuring, and reporting while at the same time, meeting compliance requirements.

LogPoint makes achieving and maintaining PCI compliance not only possible, it makes it simpler and more cost efficient than expected.

Don't just log – detect, stop, and remedy

"Checking the box" on PCI requirements and validating that proper controls are in place and effective require more than just plugging in a log management tool and forgetting about it. Unlike typical log management solutions that merely collect, store, and report on raw event logs, **LogPoint** adds a layer of security intelligence by employing multiple layers of correlation technology.

This means that event logs are not just collected and stored — even the most advanced threats can be detected and stopped. Should incidents occur, you can rapidly remedy them with integrated incident-handling capabilities that integrate seamlessly into other help-desk solutions.

LogPoint for PCI

LogPoint can help you meet even the most stringent PCI compliance obligations and unique security intelligence needs, including:

- **Decreasing time and resources** spent on compliance requirements
- **Monitoring and measuring** the effectiveness of PCI compliance controls
- **Providing information** to third-party auditors for compliance evaluations
- **Securely capturing and storing** event logs for evidence and enforcement
- **Correlating event data** from all your devices and applications
- **Delivering real-time visibility** into threats against compliance related assets
- **Immediate detection and alerting** of control and policy violations
- **Out-of-the-box and customizable** PCI reports and rules.

Conclusion

The examples provided demonstrate that it is impossible to comply with PCI requirements without having log data management processes and technologies in place.

Complete log data is a must for proving that you are up to date and compliant with security change management, access control and other required processes. When managed well, log data can protect companies when legal issues arise – for example, when processes and procedures are in question or when a forensic process is initiated as a part of an ongoing investigation.

The **LogPoint** log management solution goes beyond enabling compliance. It provides the opportunity to prove you are implementing and monitoring these processes – all the while giving you a powerful tool to protect and secure your company's data.

More information:
www.logpoint.com

logpoint

More information:
www.logpoint.com