The Case for Asset Security

logpoint

Asset Security – a crucial investment

For companies of all sizes, across all industries, the ability to confidently select the most effective IT technology continues to be a major concern.

And in today's economic climate, businesses and organizations are facing a greater challenge when prioritizing just where their limited budgets should be invested in order to emerge from these uncertain times as strong, viable companies.

Those who deliver mission-critical network services and applications are feeling this pain the most.

Today's demands

Even with such adverse economical conditions, there is still a variety of requirements to be met, including:
- An evolving and increasing number of regulatory mandates
- The securing of assets against an ever-increasing number of threats
- Delivering security controls for existing and emerging technology solutions
- Ensuring that customer data is always intact and correct.

There will continue to be more difficult, financially-driven choices ahead – and organizations will continue to need to strategically select the solutions they will be deploying.

Proactive Monitoring

Fast and precise remediation. LogPoint is a rich solution with the ability to collect, analyze and monitor all events in an infrastructure – around the clock.

By utilizing this collected information, organizations can achieve a number of advantages and savings.

First and foremost, organizations can gain full transparency at all levels – optimizing IT operations and gaining higher availability, while at the same time reducing IT operational costs.

Quick & accurate

Should the IT operation still experience an interruption, **LogPoint** allows the organization to quickly and more accurately find the exact cause of the problem, begin the necessary remediation processes, and then monitor the components in question.

Errors, irregularities and poor performance can be a result of poorly configured systems, lack of patches and software updates, system changes and irregularities in the infrastructure, etc.

Personal dashboard

But these all can be monitored by **LogPoint** – and quickly reviewed, thanks to the personal dashboard. An organization will gain the possibility to prevent issues and improve IT operations – planning ahead instead of fighting fires.

Active & precise

In short, the IT operation will receive a decreasing number of events and fewer, but more precise, alarms. And, thanks to the built-in "active response engine", they can also count on immediate reaction and escalation, particularly for those very sensitive events.

2

Threat Management

Detecting complex, external attacks & overlooked internal fraud

Investigations of computer crime have shown that most organizations eventually will be exposed to internal or external attacks. Attacks are continuing to emerge, and are growing more complex and targeted – as well as more "silent", more efficient and harder to discover. This trend is impacting all industry across the board.

Limiting impact

LogPoint can help organizations avoid the impacts of such attacks, rejecting or aiding to the rejection of most of them. Thanks to built-in rules for aggregation and data correlation, attacks can be efficiently handled.

Cheating, deception and the manipulation of data is also becoming increasingly more sophisticated and complex. If the necessary control mechanisms are not in place, a company may suffer needlessly, unable to discover what is happening, much less whether it is internal or external.

Early warning

LogPoint can provide organizations with "early warnings" whenever such irregular transactions in enterprise systems and databases take place. This can prevent internal and external fraud and data tampering, providing a better protection of the true values – everything from trademarks to production plans, patents, business plans, and secrets.

Forensics, Analysis and Traceability

All businesses need one single log-data warehouse

Having all log data in one place enables a company to analyze all log data uniformly, allowing it to respond to all requests for notification and provide alerts for a given event or series of events across the entire infrastructure.

But at the same time, log data must be stored in accordance with best practice and in compliance with any regulations.

Mission critical

A company must be able to prioritize mission-critical systems and/or events so that the number of false-positives is reduced to a minimum. If a company can achieve higher security

efficiency, it can spend more time planning and achieving other critical IT security projects. **LogPoint** offers the opportunity for full traceability on all incidents coming from the infrastructure – and therefore the entire organization.

Efficient analysis

Authorities and auditing firms can be given the necessary documentation in the time the company must make an investigation or analysis of events or event patterns. In such cases, an organization can save expenses on consultants, cut down on their own time spent on the issue, reduce the loss in work hours, and direct this time on the key projects and operational tasks they should be focusing on.

> By utilizing this collected information, organizations can achieve a number of advantages and savings. First and foremost, organizations can gain full transparency at all levels – optimizing IT operations and gaining higher availability, while at the same time reducing IT operational costs.

> "It's official: Today's security managers are more worried about insiders leaking sensitive corporate data than they are about outsiders breaking in to steal it."
> – Source: Dark Reading, March 2011

> "Eliminating threats is impossible, so protecting against them without disrupting business innovation and growth is a top management issue."
> – James Kaplan, McKinsey

logpoint

Regulatory Burdens on Growth (Compliance)

Over the last few years, the burden of regulatory compliance has grown significantly heavier for nearly every industry. The list of regulations is long and potential penalties for non-compliance are significant.

This list includes:
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)
- Federal Information Security Management Act (FISMA).

Many of these regulations continue to evolve, having significant impact across all organizations.

Impact on bottom line

Penalties for non-compliance vary from industry to industry. However, a common sight across all industries is that non-compliance is significantly impacting the bottom line. As the financial penalties and inherent security risks become easier to quantify, organizations are becoming more acutely aware of the risks and costs of non-compliance.

Doing the right thing

Conventional wisdom dictates that organizations "do the right thing" and implement common sense controls to best protect corporate IT assets – not only to meet regulatory requirements, but also to protect mission-critical business data.

Recognizing that compliance with a policy or regulation often works on a sliding scale, **LogPoint** can provide:

- **Accountability**: Proof of who did what and when.
- **Transparency**: Providing visibility into the security controls, the business applications, and the assets that are being protected.
- **Measurability**: Metrics and risk reporting within a company.

Full solution

Having a monitoring and management solution that spans the network and security technologies in your environment can play a key role in supporting and validating compliance initiatives. **LogPoint** brings to enterprises, institutions, and government agencies the accountability, transparency, and measurability that are critical to the success of any IT security program tasked with meeting regulatory mandates.

Broad benefits

Specific benefits of a **LogPoint** solution include:

- Out-of-the-box compliance reports to assist meeting specific regulations, including PCI, HIPAA, NERC, GLBA,SOX and ISO2700x.
- An easy-to-use reporting engine that does not require advanced database and report writing skills – resulting in an improved ability of staff to produce required compliance reports on a regular basis.
- Delivery of compliant workflow and security controls – resulting in decreased financial risk to the organization for non-compliance.

Enhanced Controls

When an organization chooses to implement a **LogPoint** solution, it is given the opportunity to implement controls – which can become as automated as desired.

In principle, it is a company's own defined comfort zone that determines the extent to which imposed controls are to be implemented.

Based on our experience, typical controls include:
- Failed log on
- Successful log on
- System behavior
- User behavior
- Privileged users behavior
- Escalation of user rights
- File Access
- File Up / Download
- Configuration Changes
- Transactions
- Errors.

> "PayZone's goal was to meet the PCI DSS compliance mandate and replace a system that required too much work to implement and maintain. Under severe time constraints, LogPoint has enabled PayZone to deploy and implement a solution in an efficient and straightforward fashion..."
>
> – PayZone Case Study

> "Without LogPoint, identifying the source of the problem would take a fleet of guys going through the logs."
>
> – Bjarne Warming, Rambøll Informatik A/S

> "If we didn't have LogPoint to help analyze the mountains of application traffic coming into and out of our company network, it would have been nearly impossible to identify the anomalies that the company viewed as threats."
>
> – Insurance Company Case Study
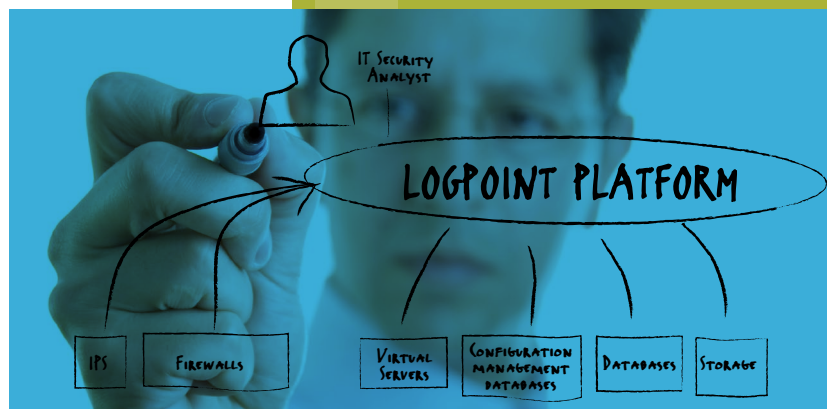
logpoint

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

When logs don't give you the answers …

LogPoint: uniquely incorporating Data Enrichment

When reviewing information found in log messages, not all the data needed is necessarily present. When data is not present in log messages, organizations often must introduce manual processes – possibly even routines for executing proper controls and spot checks in compliance with regulations or security controls.

Enhanced messaging

LogPoint makes it possible to enrich your necessary log messages with information coming from other sources, such as:

- Asset management databases
- Configuration management systems
- The internet
- Portals
- User directories
- Domain names
- Data categories

Data can be either static or based on sources where data is regularly updated (dynamic information).

Enriched data

Once the information has been enriched (or attached) to the log, it is possible to perform real-time analysis of all log messages, including the enriched data. It is even possible to include the correlation engine for very complex analysis – a process made very easy by **LogPoint**.

It is important to note that the data enrichment easily can be used for categorizing log messages.

An organization can benefit from lowered costs for security and operational controls by minimizing the manual controls and aftermath – not only performing limited spot checks, but also thoroughly analysis of all data.

Protecting Data and Intellectual Property (IP)

In a world where knowledge and intellectual property is becoming more and more essential for supporting continued growth and attracting new employees – and where it is constantly becoming more regulated – all organizations must focus on securing their IP accordingly.

This requires reviewing data, users and systems. **LogPoint** enables an organization to review these elements, avoiding data loss by notifying or alerting the right people at the right time of any behavior or pattern deviation.

Four solutions in one

LogPoint combines log management, security information and event management, network analysis and file integrity in a single solution.

This not only decreases cost of ownership, cost of deployment, and cost of operation. The intersection of all **LogPoint**'s surveillance feeds (logs, events, and network flows) actually yields more accurate data for an operator, more granular forensics for an incident response manager, and more complete reporting for auditors.

Visibility

Network and security teams are converging (or at the very least collaborating) in all types of enterprises. A key value proposition for a **LogPoint** solution is the ability to delivering visibility to match this operational convergence – while enabling full monitoring capabilities across the network and security fabric.

Automation of manual processes and routines

A core part of the **LogPoint** solution is its log management features which automate the collection and analysis of information across the entire IT infrastructure. **LogPoint** supports hundreds of heterogeneous systems, including network solutions, security solutions, servers, hosts, operating systems, and applications.

The solution is easily extended to support proprietary applications and new systems that are deployed as an IT landscape changes. Further automation includes powerful, real-time correlation that prioritizes security incidents for security operators, as well as detailed auditing and reporting to meet the security information needs of regulatory auditors and security professionals.

Optimization of staff's efficiency

Most IT staffs are already stretched to their limits, a condition unlikely to change any time soon. When incidents occur, reviewing the log data has traditionally been a manual process. **LogPoint** automatically reviews all log data across servers, databases, applications and heterogeneous networks without the need for specialized personnel.

LogPoint prioritizes all threats in advance – optimizing a staff's efforts and effectiveness in protecting the organization against potential risks and threats.

LogPoint also allows the company to offer better and more accurate customer and user support, thanks to real-time analysis, advanced search and alert capabilities.

Cost efficient

The out-of-the-box functionality found in **LogPoint** minimizes the time and effort to operate the overall security solutions, freeing up time for other important security projects.

When comparing **LogPoint** with proprietary solutions, typical costs for developing, maintaining, debugging, support and more seem to altogether disappear – and a company can enjoy increased functionality coupled with better tools that provide optimal security and support for the business.

Supporting growth for all businesses

The architecture, packaging, and out-of-the-box features found in the **LogPoint** solution mean it is uniquely capable of scaling to specific business needs. From the largest corporations, with thousands of devices and millions of events per day, to small colleges, hospitals, and regional utilities. Logging, monitoring, and analysis needs are met with a single appliance.

A comprehensive security management program typically develops and grows over time. In many cases, an organization will implement a log management solution at the outset to meet a specific security or compliance objective – but will quickly need that initiative to evolve along with advancing capability requirements.

LogPoint can easily be expanded to match even the largest and most diverse requirements in any organization.

More information:
www.logpoint.com

logpoint