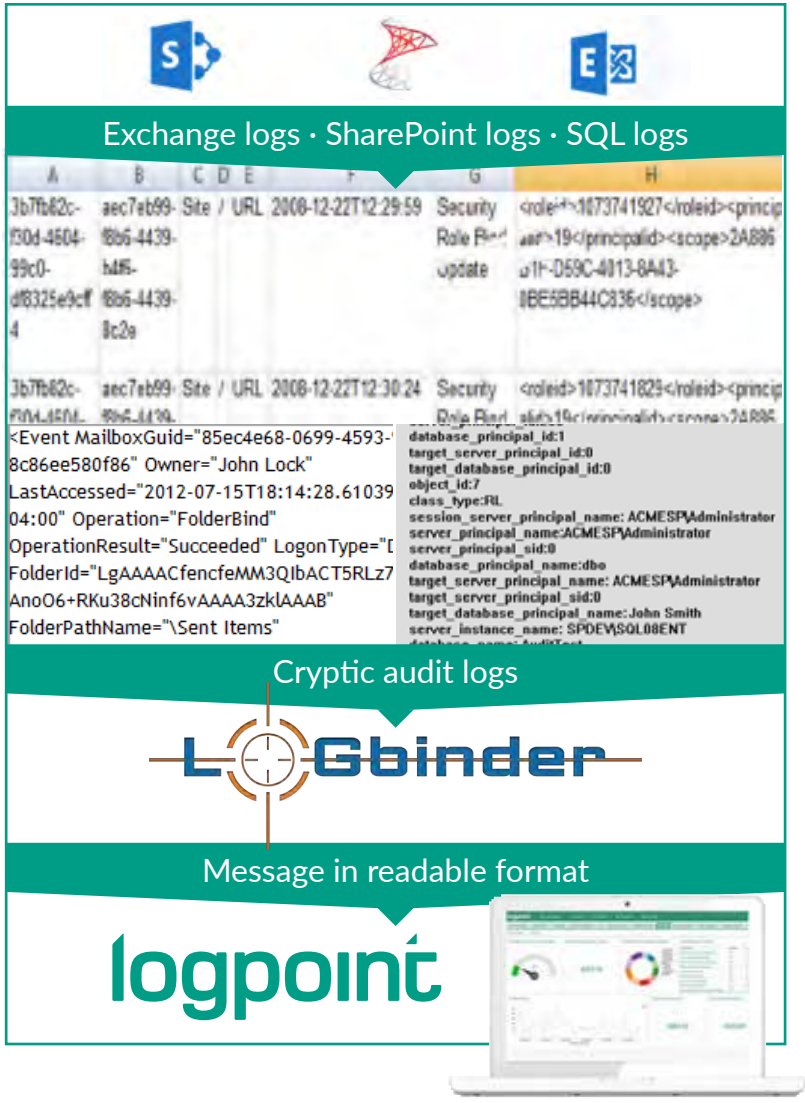
SharePoint, SQL Servers & Exchange

The information attackers are after and which compliance regulations attempt to protect often resides in applications like SharePoint, SQL Servers, and Exchange environments. One of the main challenges faced by organizations in this respect is that audit logs of these applications are not accessible or readable by ordinary log collection.

Integration Capabilities

To solve this challenge, LogPoint integrates LOGbinder collectors to extend the capabilities of our SIEM solution to consume and manage cryptic audit trails from applications, which might otherwise be inaccessible. With this integration, the audit data is translated into a readable format that is sent to LogPoint, which normalizes the data and thus enables you to easily monitor, report and alert on any suspicious events from these applications directly in your existing LogPoint interface.

The synergy adds to the effective SIEM capabilities of LogPoint and provides the user with simplified security operations, better security and compliance, enhanced accountability and audit trails at the crucial application layer.



LogPoint · Email: info@logpoint.com · Telephone: +45 7060 6100

Exchange Server Audit Logging Challenges

Microsoft Exchange contains confidential information, and thus, obtaining visibility into this prevailing platform is critical to security- and business risk management for most organizations. Especially taking into consideration today's ever-growing compliance burden and evolving threat landscape.

Log Types

Microsoft built the capabilities to generate numerous log types into Exchange. Many of these logs are utilized for operational analysis and capacity planning, and Exchange Servers provides audit logging as well – all of which can be analyzed using LogPoint.

Particularly three of these audit logs (message-tracking, mailbox auditing, and administrator auditing) contain security intelligence that is vital to protecting your organization. The message-tracking log is directly accessible by LogPoint's SIEM solution, and it can disclose who is emailing and to whom. Mailbox audit logs and administrator audit logs are fixed inside Exchange and stored in mailboxes and hidden folders. These logs convey who has accessed individual mailboxes and which actions have been performed. The latter is information solely facilitated by the integration between LOGbinder and LogPoint.

How Does It Work?

The LOGbinder add-on fills a critical gap in the analysis capacity of your Exchange environment, enabling the audit log, which can be interpreted by LogPoint. LOGbinder processes the native Exchange audit data from the organization's applications and translates cryptic codes, generating a 'decoded' Exchange audit log to the Windows event log, text file or syslog. Subsequently, LogPoint's takes over the log and enables collection, alerting, reporting, and secure archival of the information.

Supported Exchange Systems

The LOGbinder add-on can be installed on almost any server in your domain; there is no need to install it on any of your Exchange servers, thus preventing impact on production mail flow.

Install LOGbinder for Exchange on a server belonging to the same domain as your Exchange environment, which has to be Microsoft Exchange 2010 or later with service packs supported by Microsoft.

LogPoint · Email: info@logpoint.com · Telephone: +45 7060 6100

logpoint

SharePoint Challenges

As more and more information and processes move to SharePoint, it becomes critical to monitor and audit SharePoint activity. SharePoint's internal audit log requires the value-added functionality of our LOGbinder integration in 6 key areas:

1. SharePoint's audit log does not provide names of users or objects
2. SharePoint's audit log is buried in SharePoint's SQL server content database
3. SharePoint's audit log has no enterprise reporting
4. Windows SharePoint Services provides no interface for enabling auditing
5. SharePoint's audit log built-in trimming feature can delete audit events before they are exported
6. It is not possible to manage audit policy

How Does It Work?

Our integration with LOGbinder for SharePoint enables monitoring of the internal SharePoint audit log without making any changes to your SharePoint installation.

LOGbinder monitors the SharePoint audit log, and for each event, the cryptic code is resolved, producing a plain-English translation, which is then reported to the Windows event log – either the security log itself or a custom event log. Based on this process, LogPoint enables you to collect, monitor, report and securely archive your SharePoint audit logs.

Supported SharePoint Systems

The SharePoint add-on installs on your SharePoint server and allows you to quickly configure auditing on any or all of the server's site collections.

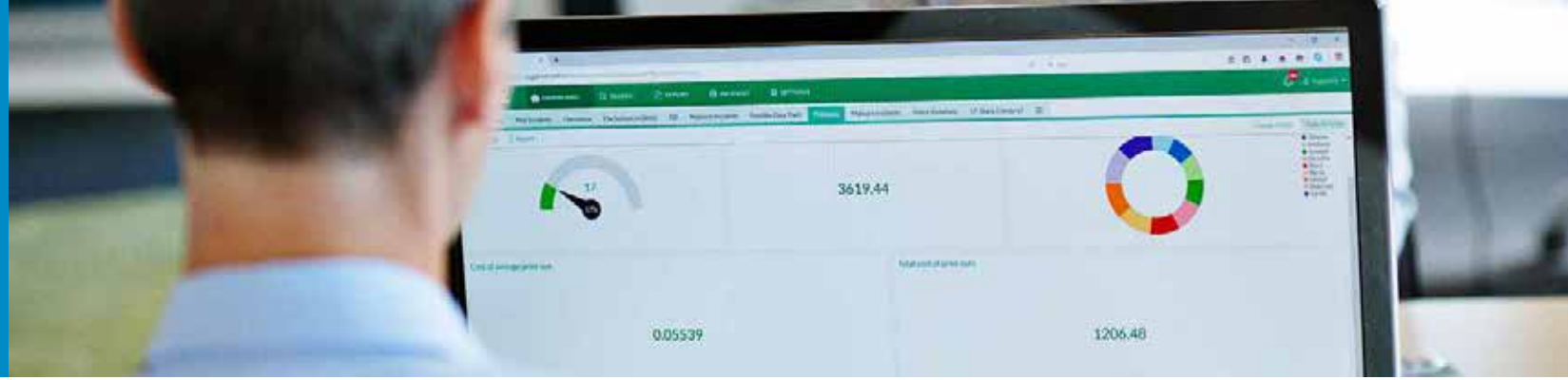
The Systems Supported:

- Microsoft SharePoint Server 2013
- Microsoft SharePoint Server 2010
- Windows SharePoint Foundation
- Microsoft Office SharePoint Server 2007
- Windows SharePoint Services 3.0

LogPoint · Email: info@logpoint.com · Telephone: +45 7060 6100

logpoint

SQL Server Audit Logging Challenges



SQL Server 2008 introduced a new audit logging facility, which is critical to enterprises storing sensitive information and/or processing significant transactions in today's demanding compliance environment. Nevertheless, the audit records generated by SQL Server audit are cryptic, and need additional refinement and processing before they can be relied upon as a usable audit trail and managed by LogPoint.

How Does It Work?

The integration with LOGbinder enables LogPoint SIEM to securely collect, alert, report, and analyze on the proprietary formatted SQL Server audit logs.

Overall, the integration between LOGbinder and LogPoint fills a gap between enterprise database servers and audit log management solutions as LOGbinder enriches the SQL Server's cryptic and generic audit messages to produce an understandable audit log, which then outputs to the Windows event log and is processed in LogPoint.

System Requirements

LOGbinder for SQL Server can be installed either on the SQL server itself or, to eliminate any impact on business database functions, you can deploy a separate server with LOGbinder for SQL Server, processing audit logs from multiple SQL Servers via shared folders. Required servers include: SQL Server 2008, 2012 or 2014, including the free Express Editions.

Integration & Licensing

LogPoint works alongside LOGbinder to build recommended alerts and reports into our SIEM solution. Thus, the partnership ensures our customers are off to an effective start with predefined dashboards, reports and alerts according to best practice within operations as well as security.

As a LogPoint customer, you can add the LOGbinder integration to your existing license. The integration is licensed depending on which particular integration you require (Exchange, SharePoint and/or SQL). Contact us today to learn more about how licensing is set up based on your specific needs and requirements.

LogPoint · Email: info@logpoint.com · Telephone: +45 7060 6100

logpoint