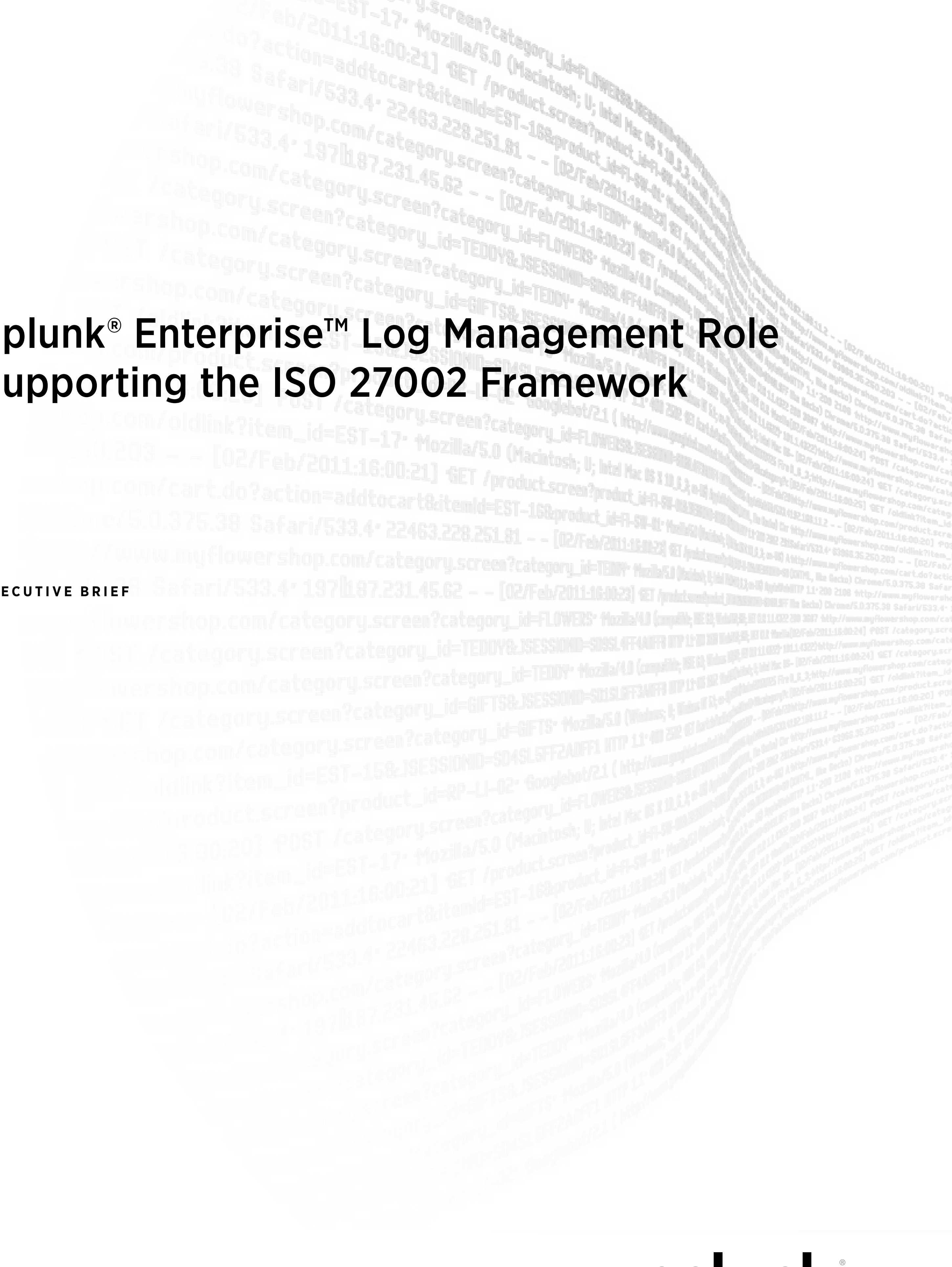
# Splunk® Enterprise™ Log Management Role Supporting the ISO 27002 Framework

EXECUTIVE BRIEF



Businesses around the world have adopted the information security standard ISO 27002 as part of their overall risk reduction strategy. The ISO 27002 framework can be used to reduce risk for businesses large and small and it is particularly useful for businesses that operate in multiple countries and need to be compliant with many in-country regulations. The ISO 27002 framework provides specific guidance for securing enterprise and organizational data.

Splunk® Enterprise™ enables enterprise security compliance across IT operations, the application management lifecycle, the data management lifecycle and security. Splunk Enterprise is a single system that supports all of these disciplines and gets everyone looking at problems through the same "data lens." The result is operational and security intelligence with a focus on the issues that most concern the business: reputational risks, risks to core business functions that affect top-line revenues and compliance risks that affect reputation and the bottom line.

Splunk software as a big data solution for security and an engine for machine data serves four primary functions that support ISO 27002:

- Collects, stores and monitors log data throughout its collection, transportation, use and disposal
- Helps protect the integrity of the log data making it useful as a definitive record of human-to-machine and machine-to-machine activities
- Provides data masking capability coupled with role-based data views
- Provides security intelligence through analytics and statistics to provide insights into system and human behaviors that can add risk to an organization

See the chart below for the specific ways that Splunk supports key ISO 27002 areas for information security management.

| Key ISO 27002 Area | How Splunk Supports ISO 27002 |
|---|---|
| **4.1 Assessing security risks** | Splunk is an engine for machine data that indexes large amounts of IT data and has analytics and visualization capabilities. Security and business teams can protect the most valuable company assets using Splunk. Once the parameters for "normal access" to critical company data is defined, Splunk Enterprise can be used to watch for access pattern anomalies based on access type, timing and the location of a given user accessing the data.<br>Splunk can classify specific application and host data—and can generate automated searches and alerts to help minimize business risk. |
| **6.1.1 Management commitment to information security** | With the ability to monitor for both known and unknown threats, Splunk Enterprise supports a management strategy that is focused on information security at a strategic level. For public companies this can mean listing cyber threats as a risk factor in the SEC 10-K document and listing their methodology for monitoring for malware that may remain hidden in the architecture for long periods of time. |
| **6.1.2 Information security coordination** | Splunk Enterprise supports automated reports for specific security team members or executives. Also, the Splunk App for Enterprise Security supports workflows for assigning tasks to specific people, event re-classification, and recording and setting policy for specific discovered threats. |
| **6.1.3 Allocation of information security responsibilities** | See 6.1.2 above. In addition, Splunk and the Splunk App for Enterprise Security provide tracking for specific security tasks related to security incidents and the metrics and monitoring of resolved security events. Splunk and the App for Enterprise Security can pull information from asset data bases to track data asset ownership. |
| **6.1.8 Independent review of information security** | Splunk support digitally signing (or hashing) of data to prove data integrity. Many users facilitate audit requests by simply teaching the auditor how to explore data with Splunk. |

| | |
|---|---|
| **6.2.1 Identification of risks related to external parties** | Splunk can be used to monitor data coming from third parties to ensure that data integrity and records are complete. Splunk can also be used to monitor the performance of third-party service providers for SLA violations. Splunk can monitor transactions between in-house and third-party systems for performance and completeness of transactions. Splunk can monitor and provide metrics for email and web security systems. |
| **7.1.1 Inventory of assets** | Splunk can perform asset discovery and monitor asset management systems for changes. Splunk can perform configuration reviews by monitoring file changes and system performance. |
| **7.1.3 Acceptable use of assets** | Splunk can monitor patterns of use and user behavior to determine if employees are using their time effectively or if they are a risk to the company. |
| **7.2.2 Information labeling and handling** | Splunk allows for meta-data to be added to data coming from specific systems to label the data or system as critical to the business. Splunk can monitor for changes to the configuration of the asset and the data contained on it and watch for changes that occur outside prescribed change windows. |
| **8.1.1 Roles and responsibilities** | Splunk supports role-based access-control so access to information is granted based on a user's specific role. Activity analysis can be performed using Splunk to ensure the separation of duties between individuals and/or established roles. User accounts in Splunk can be tied into Active Directory or LDAP for single-sign-on (SSO). |
| **8.2.2 Information security awareness, education and training** | Splunk can be used to monitor eLearning systems to confirm employee compliance with security awareness training. |
| **8.3.1 Termination responsibilities** | Splunk can be used to monitor terminated employee user accounts to verify that all accounts for a particular user have been closed. It can also watch and alert if process was not followed or if an account that should have been suspended suddenly becomes active. |
| **8.3.2 Return of assets** | Splunk can monitor several systems to determine if a terminated employee's company assets were returned. |
| **8.3.3 Removal of access rights** | Splunk can monitor the process of removing access rights, for example when an employee moves between departments or is terminated. Splunk can also monitor user access to Active Directory. If a user is added or removed, Splunk can notify IT operations of the change so they can verify that it was authorized. |
| **9.1.2 Physical entry controls** | Splunk can be used to monitor physical access to facilities and monitor established access patterns for unauthorized access. Data from Active Directory, physical access data and VPN data can be correlated to determine if a user has 'tail-gated' into the building. |
| **9.1.4 Protecting against external and environmental threats** | Splunk can accept data in any format including data from building HVAC systems to measure temperature change and monitor for related physical threats. |
| **9.2.1 Equipment sitting and protection** | Splunk can accept and monitor data from RFID systems and GPS information, so it can monitor and track the use of (RFID/GPS tagged) company trucks or equipment to protect against theft. |
| **9.2.6 Secure disposal or reuse of equipment** | Splunk can monitor inventories of hardware throughout its lifecycle. For example, it can track the disposal of hard drives and provide an audit trail for each step in the process. |
| **9.2.7 Removal of property** | See 9.2.1 Above |
| **10.1.2 Change management** | Splunk can be used to monitor changes to systems and when they occurred and who performed the work and why. This is useful when tracking emergency verses scheduled downtimes for particular systems. Risk can be assessed by the number of unauthorized changes and can be tracked over time to document the increasing or decreasing level of risk to the business. |

| | |
|---|---|
| **10.1.3 Segregation of duties** | See 8.1.1 above |
| **10.1.4 Separation of development, test and operational facilities** | Splunk allows access to production system logs for troubleshooting without needing to log onto production systems. This is a key audit requirement and prevents unauthorized changes to systems. |
| **10.2.1 Third-party service delivery** | If a company has access to log data from their service provider, SLAs can be monitored with Splunk. Also, the lifecycle for data hosted by third parties can be monitored up to the point of disposal. SLAs can be trended over time to support service acquisition decisions. |
| **10.2.2** | See 10.2.1 Above. |
| **10.3.1 Capacity management** | Splunk can monitor CPU utilization and other hardware performance information within a physical or virtual infrastructure. It can monitor thresholds over time to measure signs of performance degradation. Partial hardware failures such as fan breakdown or memory failure can be detected and monitored to support resource planning and acquisition decisions.<br>Services can be monitored for performance of transactions across the IT architecture. This data can inform investigations of the service delivery architecture and enrich customer satisfaction metrics. Splunk supports benchmarking against normal performance and alerting on all parts of the IP stack. |
| **10.3.2 System acceptance** | Splunk can drive decisions on system development as the ease of troubleshooting applications drives log formatting and revealing in log data what helps to diagnose problems. Splunk used during the QA process can benchmark performance differences between product releases. |
| **10.4.1 Controls against malicious code** | Splunk supports the search for 'known' and 'unknown threats' Splunk monitors all aspects of anti-virus deployment, host configuration, email security, and web security products, and next-gen firewalls. These are known threats as reported by signature and rule based systems.<br>Splunk can augment this data with DNS, DHCP, Physical Access data, Active directory log data, packet capture, and Flow data. Watching for time-based patterns that include geo-location data in this data can provide knowledge of malicious insider and persistent malware. Large data sets encourage creativity. Security can become more aligned with the business by focusing security on the most important data assets to the business. |
| **10.5.1 Information backup** | Splunk can easily monitor data storage solutions for performance and data integrity. Splunk works with different data classifications to properly maintain regulatory compliance and corporate disposal processes. |
| **10.6.1 Network controls** | Splunk supports role-based access controls for different network teams. Splunk can monitor HTTP, HTTPS, SSL VPN and application layer protocols from AppFlow or other load balancing data. Splunk can provide metrics for performance aspect of network hardware, configuration changes and network performance. Splunk can use log data to monitor data in transit for fidelity. |
| **10.6.2 Security of network services** | See 10.6.1 and 10.4.1 |
| **10.7.1 Management of removable media** | Splunk can be used to track the use of removable media for use increases, which may indicate the need for employee security awareness training. |
| **10.7.3 Information handling procedures** | Splunk can add meta-data for classification to facilitate data information categorization and management. |
| **10.7.4 Security of system documentation** | Monitoring system operations and configuration in accordance with system documentation and performance specifications. |

| | |
|---|---|
| **10.8.4 Electronic messaging** | Monitor log data form key management and storage systems. Splunk can monitor the authentication process. Splunk can monitor instant messaging communications and key pieces of text for compliance. Splunk can monitor twitter feeds to understand customer sentiment and reputational issues. |
| **10.9.1 Electronic commerce** | Splunk can monitor and report on all aspects of the customer transaction watching for indicators and patterns of fraudulent activities and transaction errors. |
| **10.9.2 Online transactions** | Splunk can monitor applications for incomplete from data and application error handling capabilities |
| **10.10.1 Audit logging** | Splunk can monitor security systems for changes to their configuration in change windows and monitor user behavior. Splunk can pervade a definitive record for compliance audits. |
| **10.10.2 Monitoring system use** | Splunk monitors account usage patterns determining the need for access by users. Splunk monitors the aspects of specific IT services to understand usage. |
| **10.10.3 Protection of logged information** | Splunk can monitor hosts to monitor for attempted deletion of system log files. Splunk can ensure proper disposal of log data. |
| **10.10.4 Administrator and operator logs** | Splunk monitors all user activities and provides a complete log of Splunk activities. Visualizations of trended data can reveal usage patterns |
| **10.10.5 Fault logging** | Splunk can monitor and trend application faults over time creating development team accountability. |
| **10.10.6 Clock synchronization** | Splunk can monitor systems to ensure they are synchronized using the NTP protocol. |
| **11.1.1 Access control policy** | See 10.4.1 and Splunk can monitor the behaviors of usurers that have highly privileged account access to highly sensitive business data.<br>Splunk supports HIPAA, SOX, and FFIEC, NIST 800-53 and other privacy related regulations and internal control framework objectives. |
| **11.2.1 User registration** | Splunk can monitor the entire process of user registration and monitor for out-of policy user additions and procedure violations. |
| **11.2.2 Privilege management** | Splunk can monitor privilege changes and monitor change metrics and access escalations. |
| **11.2.3 User password management** | Splunk can monitor changes to files including the /etc/password file for compliance with change requirements. Splunk can monitor how rapidly change is made across monitored hosts. |
| **11.3.1 Password use** | Splunk can monitor for hosts where no password is used for authentication. |
| **11.3.2 Unattended user equipment** | Splunk can monitor for host inactivity and monitor data indicating the password screen saver is in use or doesn't launch within a specific length of time. |
| **11.4.2 User authentication for external connections** | Splunk can monitor VPN usage for remote access. Splunk can correlate local system access information with VPN usage and physical access data to monitor for stolen credentials. |
| **11.4.5 Segregation in networks** | Splunk can monitor traffic between networks and watch for non-allowed traffic for network segregation. |
| **11.5.2 User Identification and authentication** | Splunk can monitor the process of user authentication. The Splunk App for Enterprise Security can correlate all the access identities of a particular user to track and report on user behavior across the IT architecture. |
| **11.5.4 Use of system utilities** | Use of system utilities is monitored through the use of their own applications logs in Splunk. |

| | |
|---|---|
| **11.5.5 Session time-outs** | Splunk can monitor open sessions and alert abnormally long or open sessions. |
| **11.6.1 Information access registration** | Please see 12.2.1 – 12.3.1 |
| **11.6.2 Sensitive system isolation** | Splunk can be used to add meta-data and enrich data with classifications by type and criticality and sensitivity for risk reporting. |
| **11.7.2 Teleworking** | Splunk can monitor remote access to systems via VPN log data and watch for abnormal patterns. |
| **12.3.2 Key management** | Splunk can monitor software check-in systems for access and separation between development and QA teams. |
| **12.4.1 Control of operational software** | Splunk can monitor access, configuration and performance of operational software. |
| **12.4.3 Access control to program data** | Splunk can monitor software check-in systems for access and separation between development and QA teams. |
| **12.5.1 Change control procedures** | Splunk can monitor systems for change and for violation of change control polities and procedures. |
| **12.5.2 Technical review of applications after operating systems** | Splunk can monitor for changes to log formats and increases in application error rates. |
| **12.5.4 Information leakage** | Splunk can monitor for abnormal patterns in system activities data and watch for signs of advanced persistent attackers and malware. |
| **12.6.1 Control of technical vulnerabilities** | Splunk can monitor the 'half-life' of vulnerabilities in the IT architecture and report on them as metrics for patching systems. It can also monitor system uptime metrics. |
| **13.1.1 Reporting information security events** | The Splunk App for Enterprise Security provides security event management alerting and reporting. |
| **13.2.2 Learning from information security incidents** | The Splunk App for Enterprise Security provides a complete record of the incident classification and ownership changes with all comment records. These records can be searched by date and by text search. |
| **13.2.3 Collection of evidence** | The Splunk App for Enterprise Security can take log data and security events and store them in an encrypted format using a free app on Splunkbase. |
| **14.1.1 Information security in the business continuity management process** | During testing, application performance data can be monitored and analyzed to streamline software development and time to market. Where there are problems, Splunk can monitor risk and report on delayed time to market and lost revenue (sales). |
| **15.1.4 Data protection and privacy of personal information** | See 10.4.1 and 11.1.1 |
| **15.2.1 Compliance with security policies and standards** | Splunk can automate the auditing of data integrity, availability and confidentiality across the enterprise to ensure compliance with security policies. Splunk can automate forensic investigation and run scripts to automate security-related actions. |

## Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.