



10-08-2026

Change data

Change data refers to any recorded information about modifications made to configurations, policies, rules, or system settings. This data typically includes details about what was changed, when the change occurred, who initiated the change, and the impact of the change. Change data is critical for tracking, auditing, troubleshooting, and maintaining compliance in IT environments, especially in systems focused on security and infrastructure management.

Change data ensures accountability and helps organizations maintain the integrity and security of their systems while adhering to established governance and compliance frameworks. It ensures traceability and accountability for changes to meet regulatory requirements (for example, GDPR, HIPAA, and PCI DSS). It also helps identify the root cause of issues by reviewing recent changes.

Key components of change data include:

- **What was changed:** Detailed description of the modification (for example, policy, configuration, rule)
- **Who made the change:** The user or administrator responsible for initiating the change
- **When the change occurred:** Timestamps indicating when the change was made
- **Reason for the change:** Optional but often logged for auditing purposes
- **Impact of the change:** Affected systems, users, or processes
- **Approval information:** Record of change approvals (if part of a formal change management process)

Change data typically includes events on:

- **Firewall and security devices.** For more information, see [network firewall data](#) and [web application firewall data](#).
- **Endpoint detection and response (EDR) systems.** For more information, see [endpoint data](#).
- **Server configurations.** For more information, see [infrastructure data](#).
- **Intrusion detection systems (IDS).** For more information, see [intrusion detection data](#).
- **Network devices.** For more information, see [network router data](#) and [network switch data](#).
- **Cloud infrastructure.** For more information, see [cloud services data](#).
- **Backup and recovery systems.** For more information, see [backup data](#).

The Splunk Common Information Model (CIM) add-on contains a [Change data model](#) with fields and tags that describe create, read, update, and delete activities from any data source. This model is for administrative and policy types of

changes to infrastructure security devices, servers, and endpoint detection and response (EDR) systems.

Before looking at documentation for specific data sources, review the Splunk Help information on general data ingestion for [Splunk Enterprise](#), [Splunk Cloud Platform](#) or [Splunk Observability Cloud](#).

Add-ons and apps

- [Splunk Add-on for Microsoft Windows](#)
- [Splunk Add-on for Unix and Linux](#)
- [Splunk Connect for Syslog](#)

Splunk Lantern articles for the Splunk platform

- [Maintaining Microsoft Windows systems](#)
- [Managing an Amazon Web Services environment](#)
- [Managing Azure cloud infrastructure](#)
- [Maintaining *nix systems](#)
- [Automating Splunk Platform administration with a Continuous Configuration Automation framework](#)
- [Monitoring NIST SP 800-53 rev5 control families](#)

Splunk Lantern articles for Splunk security software

- [Configuring Windows security audit policies for Enterprise Security visibility](#)
- [Configuring Windows event logs for Enterprise Security use](#)
- [Detecting AWS suspicious provisioning activities](#)
- [Monitoring AWS S3 for suspicious activities](#)
- [Detecting ransomware activities within AWS environments](#)