

# Splunk for Security

## The old way:

### Data overload blocks incident response.

If your organization is like most, you've deployed a wide variety of security technologies. Multiple IDS systems for "defense in depth," firewalls, web proxies, access control systems, and more. All this technology generates a huge amount of data, which is both a blessing and a curse.

You're overwhelmed by alerts and can't easily decide which require response. You ignore some - perhaps many - alerts, increasing the odds that real incidents are slipping through the cracks.

When alerts do get your attention, incident response proceeds slowly. You have to use multiple consoles and log into many servers to follow the trail of an attacker - one window to look at outgoing web traffic, another to look at authentication, another to look at DHCP leases. Analysis of a serious incident can take days, and until it's complete, you're in the dark. An attacker may have left backdoors open, critical data may have leaked, time-bombs may be ticking away.

Your investments in security management technologies are falling short. While they help correlate and prioritize alerts, they're slow and cumbersome to use on an ad hoc basis for incident response. More importantly, you need fast access to data that existing solutions don't support. To effectively track an attacker you have to see the configurations they changed, scripts they left behind, and database audit trails to see the data they viewed - so much more than just security events.

## The new way:

### All your data correlated in one place.

Splunk lets you search, alert and report in real-time on any user, network, system or application activity, configuration changes, and other IT data from one place.

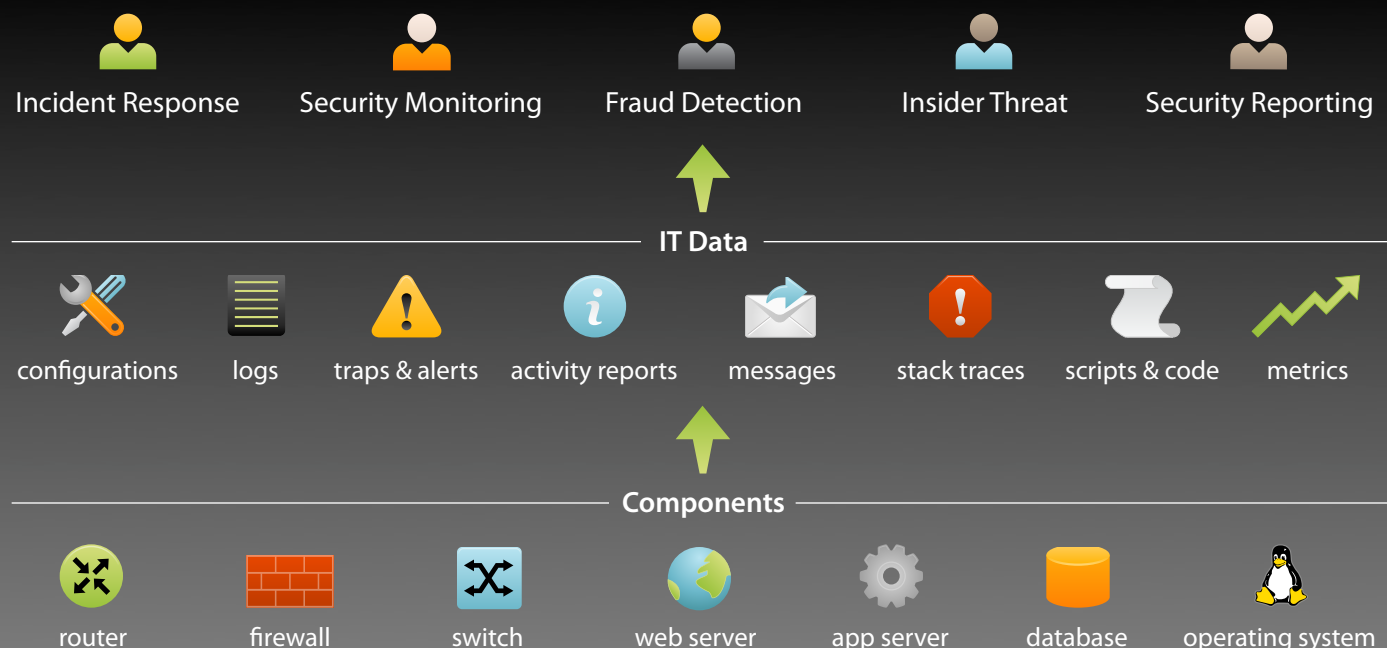
Eliminate the need for multiple consoles and follow the trail of an attacker from one place. Now you can perform more in-depth analysis and respond to incidents faster and more thoroughly, lowering your risk and exposure.

You'll have the complete visibility you've always wanted, but didn't think you could achieve.

#### Benefits

- Accelerate incident response
- Lower exposure and risk
- Identify unanticipated threats before exposure occurs
- Continuously observe the changing threat landscape
- Eliminate false positives
- Make your people smarter and more effective

## Solution at a Glance



# Using Splunk for Security

## Incident response

Splunk will be the first place you turn when you get an alert or a report of any suspicious activity. Just type the details you have into Splunk's search box - the source and target IP from an IDS alert, or the account ID of a customer who thinks their private data leaked. Splunk will instantly return every event with that search term across every application, host and device on your entire network. Initially, It might seem like a lot of data, but Splunk helps you make sense of it and bend it to your will. It automatically extracts and lets you filter on time and other fields, classifying events based on keywords and patterns, so you can quickly get a handle on all the activity. Then if you see an event of interest and want to follow the trail, just click on any term to run a new search pivoting on whatever you clicked on. Since Splunk can index any IT data - not just security events, and not even just logs - you don't have to leave Splunk to get the complete picture. You can search for and find processes an attacker may have running right now, processes they executed in the past, and see configuration changes they might have made - all from one place.

## Security monitoring

Splunk makes it easy to monitor security events across the IT stack. Search for traffic violations in your router and firewall logs, find access violations on servers and applications, or look for unauthorized or unsafe configuration changes. Make use of Splunk's trending, classification, and transaction identification capabilities to quickly identify more complex use-cases, such as suspicious transactions and patterns, or changes in network activity. Alerts can send notifications via email, RSS, SMS or trigger scripts for easy integration with your existing monitoring consoles. Alerts can also trigger automated actions to immediately react to certain conditions, like instructing the firewall to block future traffic from an offender.

## Fraud detection

Splunk gives you the power to make sophisticated fraud detection a reality. Use Splunk to monitor your web access, application and transaction logs to seamlessly apply fraud detection without costly modifications or add-ons to your existing applications. Since all activity and access logs are centrally available in Splunk, simple searches can pinpoint risky transaction patterns like high volumes, or large sums of money. You can even detect a single IP address accessing a large number of accounts - often the tip off to a phishing attack.

## Insider threat

Splunk equips you with the flexible analysis capability you need to detect insider threat of all kinds. There is no one type of event that identifies a malicious insider. You have to monitor your entire application stack; network traffic, operating system, database audit trails, and application, as well as transaction logs. Use Splunk to search for any type of access behavior. Generate visual representations of activity by a single user across all the applications and servers to identify outliers.

## Features

- Index any type of IT data from every source
- Search your entire infrastructure from one place
- Keep up with change - no models or rules to maintain
- Everyday use captures and shares knowledge of senior staff
- Distributed search across silos to enable holistic analysis
- Secure, policy-based remote access to IT data enables stricter production controls
- Turn any search into a proactive alert
- Powerful search language enables sophisticated correlation without hard to write rules
- Report on incidents and risk across multiple security products
- Share alerts and data with service providers and other tools
- Launch searches contextually from any existing console

## Security reporting

Splunk gives you a single place to generate reports across all of your IT infrastructure and technologies. Report on security events, performance statistics and configuration changes across all of your servers, devices and applications. Use trend graphs and summaries to identify anomalies and suspicious changes. Reports are interactive, allowing you to drill down to understand the cause and impact. Turn to Splunk to communicate the security posture of your infrastructure, review access controls, or keep watch over user behavior. Automate reporting on a schedule or generate ad-hoc reports for your customers, management, or peers. Put reports on dashboards to increase situational awareness by providing a real-time view into your applications and systems for stakeholders across your organization.

## Get Started Today !

Download your own free copy of Splunk today at [www.splunk.com/download](http://www.splunk.com/download).

Visit [www.splunk.com/security](http://www.splunk.com/security) for tips, tricks and applications to help get off the ground with Splunk for Security.