

To SIEM or Not to SIEM?

How to determine the right security
technology for your business.

Understand which next-generation,
market-leading Splunk solution is right
for you.

Contents

Challenges in the IT Security Domain	4
The Effect of these Challenges on Tool Selection	5
Managing Security with Splunk Enterprise	8
The Next Layer – Splunk Security Essentials	9
Splunk ES as a SIEM	10
Splunk's App for PCI Compliance	13
User Behavior Analytics (UBA)	14
Achieving Ongoing Value	15
Can Your Organization Afford to Minimize Security?	15
How Aditum Can Help	16

Challenges in IT Security

Security is top of mind for IT and security professionals and it should be top of mind across organizations. The trouble is that many organizations don't place high value on security until **after** a major security incident occurs.

After an incident, financial losses and damage to a company's reputation are difficult to overcome. Despite the risks imposed by insider threats or external attacks, many companies still fail to invest in strengthening their security posture. Why?

Small to mid-size organizations may not have the resources, bandwidth, or subject matter expertise to effectively manage the security practices and tools they have (or should have) in place.

Larger organizations, even those with security teams or SOCs face similar challenges but on a grander scale. In addition, there are too many threats coming in from too many sources of data feeds to be able to triage and investigate these issues without the right tools to overcome resource and bandwidth limitations.

What is the best way to mitigate these risks and challenges?

We suggest taking an iterative, progressive approach to maturing your security teams, processes, and tools.

From a tools perspective, organizations turn to a set of security-focused devices and applications to detect threats and notify IT or security personnel when these incidents occur.

Typically, these tools start as point solutions – firewalls, endpoint antivirus, identity management, or email malware filters.

As an organization's security processes mature, they will inevitably incorporate more proactive monitoring techniques – vulnerability scanning, intrusion detection/prevention systems, or industry-specific threat intelligence feeds.

Eventually, many security-focused organizations deploy a SIEM solution to aggregate data and perform advanced correlations from all of these point solutions to deploy real-time monitoring, incident response, user monitoring, threat detection, and security analytics through a single system.

Organizations often face challenges in tool deployment because they have not created a foundation of people and processes to support the tool. It's critical **to build up to** your desired security end state, including the use of advanced tools such as a SIEM.

To SIEM or Not to SIEM?

Deciding whether your organization is ready to benefit from the higher level of protection a SIEM has to offer requires careful consideration. On one hand, there are significant benefits to deploying a SIEM solution. On the other hand, your organization needs to be ready for it.

There are significant business benefits of SIEM solutions, including:

- Near real-time detection of and response to security incidents
- Reduced risk of noncompliance
- Greater value realization across all underlying security technology / systems
- Less time-intensive and more comprehensive reporting
- Reduced capital and operational costs via tool consolidation

Despite these clear benefits, many organizations consider a SIEM just another security tool in the toolbox and – often wrongly – assume they are ready for it. It's also important to note that many security challenges can be addressed without moving to a SIEM, but with other security apps and tools. It's a matter of determining which tool best matches your organization's security processes, needs, and goals.

There are several key factors which can be used to determine the best security technology for your organization.



In this e-book, we'll review:

- Top challenges faced by IT security teams,
- The effect of IT security challenges on tool selection,
- Splunk's various security-related solutions,
- How Splunk can build value for your organization and help your security processes mature.

You'll gain the knowledge you need to select the right Splunk deployment for your organization's current state and learn how to move to the next level of security maturity.

Effect of Challenges on Tool Selection

Many security practitioners would argue that when it comes to security, having a SIEM in place is the only way to go. That's because a SIEM, without fail, significantly increases visibility into vulnerabilities, deviant behavior, and critical security threats.

SIEM tools are able to do this because they correlate logs that were previously in siloed data stores (the various security point solutions throughout the enterprise). More data sources + correlation of that data = the application of security analytics that eliminates security blind spots, and perform that detection much quicker.

This improved availability of data and data correlation ensures more rapid triage of security incidents. For instance, **studies of 1,500+ Splunk customers found that incident investigation time can be reduced between 70% to 90%.**

This enables:

- Faster mean time to resolution for security incidents
- Increased volume of incidents a security team can investigate
- More time for proactive threat hunting activities

Despite the clear benefits that a SIEM delivers to significantly enhance an organization's security posture, not every organization is ready to deploy a SIEM such as Splunk Enterprise Security (ES).

Let's examine **5 questions** to better understand what type of tool is right for your organization:

Question 1: What problem(s) are you trying to solve?

You must understand the security use cases that you want to address prior to deploying a SIEM. As important, **how many** security use cases are you trying to address? If you are only trying to solve one problem – for instance, gaining visibility into Windows security event logs – a SIEM would be overkill. If you have a large number of security use cases to address, a SIEM starts to make much more sense.

Question 2: How large is your security team?

An organization with a smaller security team, or no security team in place, would be crushed by a SIEM. Managing the generation and investigation of alerts could overwhelm a smaller team. This will increase the risk that these alerts – many of which will be critical – will become “white noise” and may eventually be ignored due to alert fatigue.

On the other hand, if you have a team of security analysts (or SOC) in place to handle events and tune the system, it makes much more sense to have a SIEM in place.

Effect of Challenges on Tool Selection

Question 3: What security tools are currently in place?

A SIEM primarily aggregates and correlates data from other sources. The more security tools that an organization is using, the greater the benefit of the SIEM to provide end-to-end monitoring. Organizations with limited or incomplete security data sets – for instance, just firewalls, anti-virus, and Active Directory (account activity) data -- will not realize as much benefit from a SIEM as organizations with additional security tools (and data sources) in place such as vulnerability scanners, network intrusion detection, packet sniffers, threat intelligence feeds, or password crackers. Organizations with all of these tools in place would gain tremendous value from the correlation a SIEM can provide.

Question 4: How security-focused is your company?

Risk reduction, compliance, and the creation of a more secure organization comes down to culture. This is driven at the executive level and cascades down through leadership to the staff level. When your security team needs to install monitoring software on someone else's equipment (developer's application servers, network infrastructure, user desktops, etc.) do they get pushback? Is the request met with a lack of urgency? An uncooperative culture makes a SIEM deployment, while certainly not impossible, much more difficult. Conversely, a security-focused culture where everyone works together to meet overall organization security goals can drive the success and value of a SIEM deployment.

Question 5: Are your security policies well-defined and documented?

The foundation of IT security is the existence of proper security policies. These policies feed into security tools, including your SIEM. What are the most sensitive targets in your environment? What are the most accessible or likely targets? Your security policies should be designed to defend your business priorities. A successful SIEM takes these priorities and makes them actionable. If it is a priority to prevent unauthorized access to information, your SIEM should monitor for brute force attempts, impossible travel logins, or terminated user login. Without a security policy in place, actionable rules can't be built into a SIEM tool, including downstream responses.



Splunk's Security Solutions

If you're focused on improving your organization's security posture, chances are you're considering Splunk as a tool that can help you meet this goal – the Gartner Group named Splunk “Market Leader” in the research firm's latest [2017 Magic Quadrant report for SIEM](#) .

For those that may not be overly familiar with Splunk, it's worth pointing out that “Splunk isn't *just* Splunk.” Splunk provides numerous security products and it's essential to understand which one is right for your business.

Splunk Enterprise – Splunk's flagship product, sometimes referred to as “Splunk Core” or “Core Splunk.” This is the platform that serves as the foundation of any Splunk deployment.

Splunk's Security Essentials (App) – A free app available on Splunk's app market, [Splunkbase](#). Security Essentials provides over 300 security uses cases for your team to explore. More importantly, it provides a prescriptive path to help you understand which data sources are most critical to ingest as your security processes begin, develop, and mature.

If you're trying to improve your security processes, but don't know where to begin, Security Essentials is an excellent first step.

Splunk Enterprise Security (Splunk ES) - A **Splunk ES** – A full-feature premium (paid) app built on top of Splunk Enterprise. This is Splunk's analytics-driven, next-generation SIEM platform.

Splunk's App for PCI Compliance – Another premium app built on top of Splunk Enterprise to help organizations meet PCI DSS 3.2 requirements.

Splunk User Behavior Analytics (UBA) – An independent platform that integrates with Splunk Enterprise and leverages advanced Machine Learning models to identify threats.

There are hundreds of additional security-related apps available on [Splunkbase](#) . These apps are typically tied to specific security use cases (ransomware, fraud detection, etc.), data sources, or products (Palo Alto Networks, Cisco Security Suite, or Proofpoint). Most of them are completely free and all of them are designed to be installed on top of Splunk Enterprise. Close to 250 of these security apps are built and maintained by Splunk, while many others have been developed by the larger Splunk community.

Which Splunk security solution is appropriate for your organization? This, in large part, depends on the 5 key factors discussed earlier. In the next section, we'll examine each Splunk security offering in light of these factors.

Security with Splunk Enterprise

Splunk Enterprise is Splunk's flagship product. It is an analytics platform for machine data; it allows you to ingest any data source you'd like and then analyze and report on that data in ways that were not possible with legacy solutions.

Machine data, including the log data being collected by an organization's hardware and software that is the basis for IT security, has unique characteristics that pose major challenges to reporting and analytics - the "3 V's" of big data: Volume, Variety and Velocity of that data. Splunk Enterprise's core value is its ability to overcome these challenges of machine data and provide security analytics that were previously not possible.

Splunk's flagship Splunk Enterprise product is not, however, a SIEM in and of itself. What this means is that while users can benefit from Splunk's power to analyze large volumes of machine data and report and alert on that data, the use cases themselves - including security use cases - need to be built after the platform is deployed. This is unlike Splunk's ES product (discussed in greater detail below) which is a SIEM and has 60 pre-built security use cases, out-of-the-box.

Is Splunk Enterprise (as opposed to Splunk's SIEM solution, Splunk ES) the right security solution for your company's current security posture?

Understand your readiness by comparing your current security state to the scenario below:

- ✓ You have a small number of specific security use cases.
- ✓ No dedicated security team exists, or a small team.
- ✓ You're using a small number of security tools, such as a firewall and antivirus protection.
- ✓ There aren't a large number of data sources to correlate.
- ✓ Your organization hasn't crafted specific security policies to inform threshold setting and provide actionable steps to be taken in the event of security incidents.
- ✓ Security culture is still in an immature state.
- ✓ Your organization doesn't yet understand the value of a robust security program.

If these scenarios match your organization, Splunk Enterprise can help your existing team address security threats extremely effectively, without overwhelming your staff as a complete SIEM solution might at this state.

While it's not a full SIEM, **Splunk Enterprise will provide unmatched visibility into your environment and significantly improve your security team's ability to quickly investigate incidents.** It's a positive and necessary step in the right direction for your organization's security culture.

The Next Layer – Security Essentials

If your organization has already deployed Splunk Enterprise and wants to improve its ability to correlate threats and monitor security events, Splunk's Security Essentials app is a good next step. Splunk Security Essentials is a free app that can be deployed on top of Core Splunk (Splunk Enterprise).

This app has over **300 working examples of anomaly detection** leveraging advanced SPL techniques (Splunk Processing Language) which can be tweaked to fit your environment's specific needs.

Security Essentials provides out-of-the-box security correlation searches with use case functionality across access, data, network, threat, and endpoint domains.

Perhaps most importantly, the latest version of Security Essentials is highly prescriptive. Oftentimes the biggest challenge to monitoring security threats lies in knowing what to do first, or next. Security Essentials mitigates this challenge by providing a sequence of the critical data sources to ingest. It's a clear prescription for improving your organization's security posture.

While Security Essentials will pinpoint areas where threats may exist, it does not provide the investigation and resolution tools that are available using a more robust SIEM tool such as Splunk ES.

When does it make sense to deploy Splunk Security Essentials?

- ✓ You want to improve security but you're not sure where to start or which data sources are most important.
- ✓ You want to utilize Core Splunk for security but do not have the time or resources to develop security use cases in house.
- ✓ You have enough Splunk knowledge to support yourself using this app. As a free app, there is no support for Splunk Security Essentials.
- ✓ You're interested in building a business case for improved security.
- ✓ Your organization must comply with security regulations like HIPPA, PCI, and GDPR.

It's important to realize that your organization may eventually need to make the move to Splunk ES in order to eliminate security blind spots and make investigations more efficient. In fact, some organizations choose to use both Security Essentials and ES together.

Security Essentials provides excellent security use case examples and guidance for improving your security practices. And if your organization's eventual goal is to move to Splunk ES, Splunk Enterprise and the Security Essentials app will help users better acclimate to using Splunk before making the move to ES.

Splunk as a SIEM – Splunk ES

Splunk ES is a SIEM – it is a robust, next-generation security analytics platform that has complete out-of-the-box functionality for Security Analysts, Engineers and Executives. Splunk ES is a licensed, “premium” app that is installed on top of Splunk Enterprise.

When is your organization ready for a SIEM such as Splunk ES? If your organization is facing a large volume of security-related threats detected by a large number of point security tools and data sources, and has the people and policies in place to anticipate, recognize, and investigate security events, you’re ready to utilize a SIEM platform such as Splunk ES.

Most security practitioners would go further and say you’re not only ready to deploy such a platform, but that you only start to achieve optimal risk reduction when a SIEM is in place.

“Instead of merely watching events after they occur, an IT organization should anticipate their occurrence and implement measures to limit vulnerability in real time.”

- [Six Capabilities of an Analytics-Driven SIEM](#)



It’s important to realize that not all SIEMs are created equal. Based upon increasing volumes of machine data, legacy SIEMs such as IBM’s QRadar and HP’s Arcsight are falling behind both in their ability to ingest data from all of the necessary sources and to quickly report on that data, among other issues.

Splunk ES offers many robust SIEM features, including:

60 pre-built correlation searches (Splunk ES version 4.7.4)

These out-of-the-box correlation searches are common security use cases that fit in to nearly any environment. They include capabilities like finding brute force access attempts, identifying malware activity, finding matches against indicators of compromise (IOCs), or discovering network activity to or from known bad sources.

Splunk as a SIEM – Splunk ES

Risk Scoring

Splunk ES assigns risk scores from 20 (informational) to 100 (critical) to any asset or identity relative to the severity of activity discovered in correlation searches. The Risk Analysis dashboard within Splunk ES displays these risk scores and other risk-related information.

Investigation (Workflow)

Splunk ES has built-in capabilities for workflows tied to notable security events (referred to in ES as “investigations”). Each notable event becomes a task; this task is an event that must be assigned, reviewed, and closed. ES allows for collaboration across a security team. It also enables documentation of the progress or stage of the incident, what has been done, including the searches that have been run, what results were returned, and all information related to any particular investigation and post-incident reporting. This all occurs within a single pane of glass.

“Splunk ES is our single pane of glass that allows us to do incident management as well as investigation from one pane.”

- [CISO, Manufacturing Company](#)

Adaptive Response

Adaptive Response (AR) provides an automated (and semi-automated) way to remediate security events. For example, if Splunk ES detects a recurring infection on your network, you can easily create an AR script to kick off the response that should occur.

AR is a Splunk-led industry-wide initiative that is supported by and across many other leading security technology vendors.

AR is all about automated remediation. Some examples of AR:

- Quarantine of a server that is infected with malware
- Triage of a security event to a different IT team, including the creation of a ticket in non-Splunk ticketing systems used by other teams (for instance, ServiceNow)
- Automatically look up or ping a suspicious IP

Adaptive Response is a framework that allows bi-directional integration across security products. It not only helps organizations to find security threats, but also to quickly and thoroughly investigate and respond to them.

Splunk as a SIEM – Splunk ES

Machine Learning

Splunk ES (via their Extreme search feature) allows for the building of dynamic thresholds on event data. This feature helps move from static, user-configured thresholds to a contextual, dynamically updating model.

Instead of alerting on all outbound data transfers greater than 1 MB, Extreme Search provides a framework that lets you aggregate data transfer rates over time and put them into context (for example: low, medium, and high). Now you can configure your alert to trigger whenever outbound data transfer rates are “high” where “high” is a dynamic threshold based on a statistical aggregate of your data transfer rates.

All of these features work in concert:

- Correlation Searches and Risk Scores work together to generate notable events
- The severity of the notable events is determined by Risk Scores tied to an organization’s assets and identities (for instance, servers can have classifications such a high, medium and low severity, as can users)
- Notable events naturally feed into Splunk ES investigation tools
- Extreme Search provides a framework that allows you to easily move from static to dynamic thresholding.

Equinix was overwhelmed by more than 30 billion raw security events generated every month. With Splunk Enterprise Security and Splunk Cloud, **the security team can now reduce the 30 billion raw security events down to about 12,000 correlated events, and then to 20 actionable alerts**, thus providing actionable security intelligence and the foundation for a dedicated SOC.

[Learn More](#)

With the exception of some of the correlation searches, **the features above can only be found in the Splunk ES SIEM tool**; they can’t be found in Splunk Enterprise or the Security Essentials app. Splunk’s Security Essentials app helps with built-in correlation searches, but only Splunk ES offers full SIEM capability with the functionality outlined above.

It’s worth noting that these features could be built within Splunk’s core Enterprise product, but that would take an inordinate amount of development time, and Splunk ES already affords this functionality as an out-of-the-box SIEM tool.

Splunk App for PCI Compliance

The Splunk App for PCI Compliance is a licensed “premium” app that is installed on top of Splunk Enterprise. It is a Splunk developed and supported app designed to help organizations meet PCI DSS 3.2 requirements.

Like other Splunk apps, it provides out-of-the-box functionality. In this case, the capabilities cover the real-time status of PCI compliance technical controls.



The Splunk App for PCI Compliance:

- Identifies and prioritizes any control areas that may need to be addressed
- Allows organizations quick response to auditor reports or data requests
- Provides out-of-the-box searches, dashboards, reports, incident response framework, and integration with employee and asset information
- Gives visibility into system, application, and device activity relevant to PCI compliance

Splunk User Behavior Analytics (UBA)

For organizations looking to find not only the “known bad” but also the “unknown bad,” there is Splunk User Behavior Analytics (or Splunk UBA). Splunk UBA is installed on separate infrastructure and acts as an advanced machine learning analytics engine against the data stored in Splunk. **Splunk UBA is a tool for high-maturity organizations that are ready for more proactive security solutions.** Splunk UBA can help detect many types of suspicious and malicious activity, but is focused primarily on insider threat detection.

It's critical to realize how exposed organizations are to insider threats:

A whopping **69% of enterprise security executives reported experiencing an attempted theft or corruption of data by insiders during the last (12) months**, according to Accenture's 2016 survey of over 200 enterprise security professionals

The Ponemon Institute, an independent research firm in the privacy, data protection and InfoSec space, reported [that 43% of businesses need a month or longer to detect employees accessing files or emails they're not authorized to see.](#)

Similarly, the SANS Institute claims that nearly a third of all organizations still have [no capability to prevent or deter an insider incident or attack.](#)

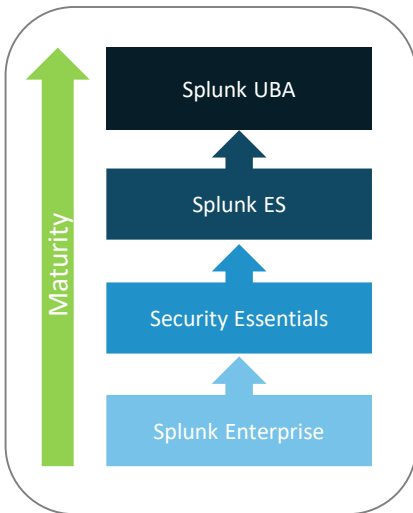
Insider threats are a serious challenge for organizations that need to be addressed, but in many cases, organizations may not find immediate value from adopting a solution like UBA unless they have already achieved a certain level of security maturity. Solutions like UBA make very specific correlations and to do this effectively requires complete and accurate data. Are you sure you have security events from ALL of your domain controllers, firewalls, IPS, etc.? Are you sure the events are being assigned the correct timestamp (so they can be correlated over time properly)? If these data sets are not properly configured, you will fall into the classic data science problem of “garbage in, garbage out.”

Another barrier is developing environmental context. For many newer security teams, the basic architecture of critical systems is not well-documented and each security incident generated by a tool like UBA will become a whole project in itself. For example, if UBA detects a vulnerability scanner sweeping subnets it will fire an alert for scanning activity. In a mature environment, the source IP can be looked up quickly and the analyst would determine this was a vulnerability scanner. In a less mature environment, the analyst may be forced to track down the assignment of the IP, uncover the physical location of the device, find the owner, and confirm that the device is a vulnerability scanner. The more of this context that is available ahead of time, the greater the value of alerts from UBA.

Achieving Ongoing Value

As Gartner indicated in its [2017 Magic Quadrant report for SIEM](#), one of the key strengths of utilizing Splunk for security use cases is that **Splunk provides organizations with room to grow.**

By beginning with Splunk Enterprise, layering on Security Essentials, and then growing into Splunk ES and UBA, organizations can improve security posture over time by adding new applications, data sources, and correlations. **Each new source of data and correlations across this data lead to increasing levels of risk reduction.**



The ability to take a phased approach to SIEM deployment helps IT and Security organizations fully realize the value of the solutions in which they invest.

Consider the following when building your business case for improved security:

- ✓ How many critical events happen in your organization each year?
- ✓ What is the Cost to IT for an average security incident (security analyst salary * number of analysts * time to resolve)?
- ✓ What is the average cost to your firm for lack of compliance (for example, PCI compliance, etc.)?
- ✓ What is the impact of a security incident on your brand's reputation? Consider how you might quantify this for your business (drop in revenue, lost customers, stock price, etc.).

An evolutionary approach enables security teams to build the strong policies, processes, and security domain expertise that are necessary to underlay the technology platform. This is key to gaining the highest level of risk reduction and business value from security initiatives.

Many stakeholders are concerned about the cost of a SIEM. When faced with the consequences of a security breach, can your organization afford to maintain an immature security posture? Can your organization afford to minimize security?

Aditum Can Help

Examining whether you are ready for a SIEM, can effectively stand one up and drive meaningful tool adoption and, most importantly, gain significant value from that tool, requires the right subject matter expertise. This expertise is a combination of IT security domain expertise as well as SIEM expertise.

Aditum's professional services team has decades of combined experience with both. This expertise ensures that:

- ✓ Security use cases that will capture the highest level of protection to your organization are addressed
- ✓ Correct data sources are being targeted for your businesses' use cases, which ensures critical data correlation and meaningful reports, dashboards and security alerts
- ✓ Your security team will be able to hunt down more security incidents and more meaningful incidents
- ✓ Tools such as Splunk are configured to be scalable and maintainable

Aditum's professional services team has the both the security domain expertise and Splunk expertise to ensure that you get the most out of your SIEM.

We look forward to any opportunity to help harden your security posture and to grow your security capabilities and culture.



Stay Connected with Aditum

Improve your security posture and learn how to get more from Splunk.

Call: (727) 240-3176

Visit: www.aditumpartners.com/contact-us

References

The State of Cybersecurity and Digital Trust, 2016

Accenture

https://www.accenture.com/t20160704T014005Z_w_us-en/acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf

Data Theft Rising Sharply, Insider Threats Cited as Leading Cause

Varonis

<https://www.varonis.com/learn/ponemon-2016/>

Insider Threats and the Need for Fast and Directed Response

SANS Institute

<https://www.sans.org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-37447>