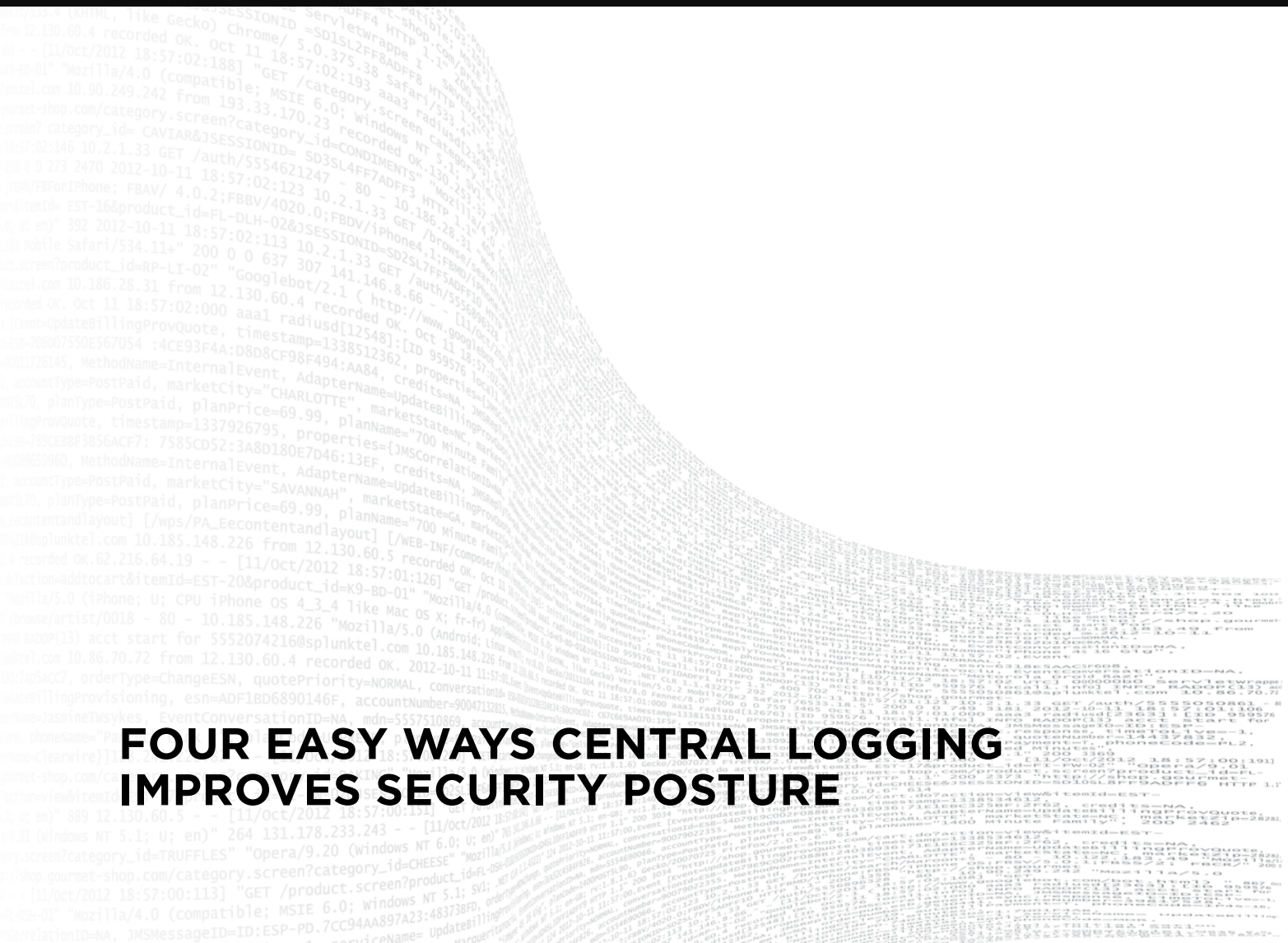
splunk>

WHITE PAPER

FOUR EASY WAYS CENTRAL LOGGING IMPROVES SECURITY POSTURE



Executive Summary

Most cybersecurity tools are designed to help identify, alert on, and in some cases prevent a particular type of malicious activity. Current technologies send alerts and may even prevent specific types of attacks, but the burden remains with the organization to figure out whether that alert is meaningful in a broader context, such as overall posture, and if and how that alert fits into a larger chain of actual malicious or attack activity.

Reliable central logging – also know as log management or log aggregation is the first critical step toward gaining visibility across a multi-layered security environment.

The Need for End-to-End Visibility

When organizations are attacked, it is critical to quickly understand the full extent of a breach to effectively remediate and minimize its impact. Organizations need tools to help them connect the dots and uncover all the interdependencies and relationships between seemingly incongruous activities. They need to see the complete chain of events that make up the attack so they can be understood. End-to-end visibility is critical to establishing security posture, efficiently investigating and acting quickly before damage can occur. This paper focuses primarily on security posture.

Security Posture Defined

Security posture refers to the overall status, or "strength," of an organization's ability to handle threats and defend assets, employees and other resources. Security posture can be used to help measure the effectiveness of planning and preparedness. It is a plan that details procedures and controls to protect an organization from internal and external cyberthreats.

Ideally, the view into security posture includes the entire organization's environment – including any and all IT systems and other digital assets that produce machine data. The broader the visibility into security posture, the more context security teams can gain to make better decisions on how to best respond.

What's the Challenge?

Security technologies offer a limited view of what is happening, based on where they are deployed, in the network or on the endpoint, and what they are optimized to look for, such as the initial infection (malware), propagation (network scans/probes), data exfiltration (command and control traffic), and more. In addition, a lot of relevant security information is contained in non-security devices throughout the organization, such as web servers, mail servers, DNS servers, identity infrastructures, applications and more.

PROBLEM	SOLUTION
Protect endpoint	Antiviruses: Symantec, McAfee
Protect network: Unauthorized traffic	Firewalls/Web Filter: Palo Alto, Cisco
Indicators of malicious activity	Threat intelligence
Control user access	Anthentication/2-factor: AD, RSA, Badges
Network attacks, stolen information, phishing	IDS/IPS: Cisco, Palo Alto Email filter: Cisco, Proofpoint
Unpatched systems, versions with bugs	Scanners/Patching: Nessus, SCCM

To understand the full scope of an attack, organizations must identify the significance of an alert, by collecting all potentially relevant data and determining how that single piece of information potentially relates to other activities on the network – many of which may be disguised as normal events.

Understanding the full scope starts with a good posture assessment. This means looking across the environment and the events occurring in the environment – without a central way to look across all these events, organizations can struggle to get end-to-end visibility of all an attack's activities, so those organizations can effectively mitigate all of the components of a threat.

Assessing Posture

In order to efficiently look across the entire environment, security teams can leverage the insights from event logs and other machine data. This concept of central logging assumes that all the relevant data is available in a single, reliable location for security teams to access.

Collecting all this information into a centralized repository enables security teams to ask questions to assess and validate posture, such as:

- How secure are my endpoints?
- What is happening on my network?
- Where do I need to patch?
- Do I have the right level privilege configured on my authentication systems?
- Is there any suspicious traffic going out?

There are four basic data sources that security operations can leverage to answer these questions and for immediate visibility of critical security activities. The data sources are:

1) endpoint
2) user/identity/access
3) network
4) threat intelligence

Four Ways to Improve Posture Quickly

Each of these can come in variety of formats and sources and each of these categories has sub-categories and a range of solutions that provide the data.

Let's take a look at these methods in depth.

Understanding Your Endpoints

Processes, File Info / Access, User Activity

What you discover:

- Frequency of application executions, unique applications
- Non-corporate approved applciations
- Known malicious executables

Benefit:

- Visibility into application executions
- Understanding of unknown applications – whom and where and frequency

Endpoint can be a critical component to find malware infections before damage is caused to business operations. Almost all organizations have Windows, Linux, and various other endpoint data they can leverage to gain critical insights – such as validating the method and source of infection, scoping the broader impact of an infection, and understanding how to prevent similar infections in the future.

Basic posture assessment methods for endpoint include using Windows Sysmon, Windows Event data, and activity logs from endpoint security systems such as antivirus, anti-malware, anti-spyware, and endpoint detection and response (EDR) solutions to discover key insights on the endpoint that could be related to malicious activity.

Access and Identity

Who, Why and Credential Abuse

What you discover:

- Credentials used in multiple locations, or shared by users
- Admin credential abuse
- Login frequencies, users moving around quickly
- Users failing authentications trying to discover internal/external resources

Benefit:

- Uncover unusual login patterns
- Track user behavior

User activity data can help identify potential malicious login activity to determine if deeper investigation is required. For example, user activity data can identify patterns of authentication failures, gain visibility into malicious access attempts, and to investigate and visualize patterns and sequences that help inform how best to remediate a threat.

Basic posture assessment methods for login activity can identify the who and the why for credentials if you just bring in security event information, specifically things that go to Active Directory and authentication to both endpoint and servers.

Network Activity

Detecting Exfiltration and Unusual Communication

What you discover:

- Who talked to whom, traffic volumes (in/out)
- Malware download/delivery, C2, exfiltration
- Horizontal and vertical movement

Benefit:

- Determine how threats got in
- Systems and endpoints communicating internally
- Detect intellectual property theft, insiders

Network event data can help security teams understand where and how an attack may have entered the network and how to remediate a threat. For example, network activity can help locate the attack vector and associated movement, verify whether command and control has been established, and also help identify the extent and impact of a compromise.

Basic posture assessment methods for network activity include bringing in security event information, specifically things that go to Active Directory and authentication to both endpoint and servers.

Threat Intelligence

Known and Early Warning Indicators

What you discover:

- High risk behavior and patterns
- Malware not blocked, malware and command & control activities
- Known indicators of compromise

Benefit:

- Detect intellectual property theft
- Detect insiders
- Compromised systems communicating internally
- Compromised endpoint

Threat intelligence is a compilation of malicious sites, file hashes, malicious IPs and more that are used to inform detection and investigation.

Threat intelligence can offer early warning indicators of malicious activities, detection of compromised traffic or watch-listed destinations. It can determine high risk behaviors and patterns. You'll also see malware that may not be blocked or command and control activities.

Get the Complete Picture

By starting with four basic data sources, security teams can quickly determine what's happening across the environment, such as unusual activity that hasn't been seen before or sudden changes in traffic and login patterns.

Organizations can use these security posture insights to better analyze their overall risk, and apply best-practice methods to answer basic questions about where to focus their investigations.

Enter Splunk

Splunk Enterprise can provide a fast and easy way for organizations to gain control of their security posture, using an iterative process that helps use a single source of truth across the organization.

Splunk enables better control over security posture, which in turn helps get to insightful answers quicker, such as to determine the root cause of an attack faster, validate the broader extent of impact and how best to remediate an issue.

Splunk's ad hoc data exploration and the platform's ability to look across all attributes of any data over all historical time, align directly to the methods needed by investigators and forensics analysts to answer the investigative questions they need resolved.

Interested in learning how to use Splunk to improve your security posture? Try these security techniques online now in a free, demo environment.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com