Security Logs: 3 Reasons You Can’t Survive Without Them

One extremely important (but often overlooked) set of weapons in your security arsenal is your **security logs**. Why?

System and network logs can be the key to heading off an attack, responding immediately to a breach, and determining the critical details of a security incident after it has occurred.

It’s like finding “patient zero” in a pandemic—and having those answers safe and on hand can make all the difference in recovery times. However, hackers know this too and often target system logs in an attack.

Here’s a look at how you can protect them and why log data security is so important.

1. Security logs can help you proactively identify and characterize threats.

When it comes to protecting your data and applications, security logs can act as an early warning signal when something fishy occurs. Using appropriate log analytics platforms or log monitoring software, you can be alerted to anomalous user behavior, network events, or system access, which could point to a potential security incident or threat.

Some analytics platforms can parse log data to identify potential threats that more traditional security tools can’t detect. These early warnings enable you to proactively address the issue before it has a chance to

escalate. You can also use detection capabilities to test security scenarios and hypotheses, which then empowers you to identify and resolve security gaps or other vulnerabilities.

2. Security logs can help you detect and respond to attacks.

A log analytics solution can continuously monitor your security logs to help you become immediately aware of a security incident, whether it's unauthorized access, a violation of security policies, a change to data or system configurations without the right permissions, or an outright attack.

Your security logs will have the information you need to know regarding what's happening at the moment (or very shortly thereafter), so you can act right away to minimize exposure and mitigate the enormous financial and reputational implications of a serious breach.

3. Security logs can help you know exactly what happened after a breach has occurred.

Once you've identified and remediated a security breach, it's vital to trace the event back to where it started. Much like epidemiologists work hard to analyze populations and find "patient zero" during a viral outbreak, your organization will want to forensically review existing security logs to identify the person or device that infiltrated the system, see how they got in, learn exactly what they did and when, and determine whether the threat is ongoing.

This forensics task is a critical part of recovery after the event. Without it, your IT team won't know which systems are vulnerable or how to fix them.

Security logs can be a powerful cybersecurity tool—but only if they're activated and used correctly. Security experts say it's important to log everything on all of your systems. You don't know where a breach attempt will occur, so having logs across your **entire** infrastructure can save you in the future.

Having a solid log analytics solution is also key to getting the most out of security logs. In a single day, your servers, network, and end-user devices could generate hundreds of thousands or millions of log entries. One study found that the average enterprise will accumulate up to 4GB of log data a day. That data includes every transaction that takes place across your network, including information about users logging

on and off the system, server crashes, applications starting and stopping, files being accessed, and so on. It's too much data for any human to review daily.

Focus on putting the right analytics tooling on top of your security logging in three core areas: the network, endpoints, and end users. A good log analytics platform can monitor your daily volume of security log data and process it in real time to detect anomalies, identify potential threats and indicators of compromise, and alert IT to security violations. After collecting and analyzing the logs, it's important to have an orchestration tool that can enrich data that gets passed to your threat hunters so that they have a curated set of information to begin their review.

Security logs can be a powerful cybersecurity tool

Because your security logs contain such a wealth of data about potential security issues and activities, it's important to keep them well protected. Hackers know how valuable they are, so they can often delete or change them to hide their tracks.

To protect security logs, you can:

- Encrypt or password-protect them
- Make them append-only, which means a user can add to the logs but can't alter or erase what's already there
- Create copies of log files and store them across multiple environments
- Store log files on a separate system or server altogether
- Use unalterable audit logs to ensure accuracy
- Hide log files within the system
- Use write-once media to save log files

How Pure Storage and Our Partners Can Help

There are a lot of benefits to using Pure Storage® FlashBlade® or FlashArray™ to store your security log files. Both are all-flash, highly scalable, network-attached storage solutions. FlashBlade and FlashArray consolidate all of your log files and integrate seamlessly with even the most advanced log analytics platforms—including solutions from our partners, Elastic and Splunk. FlashBlade and FlashArray deliver faster time to insight at a lower total cost of ownership.

FlashBlade and FlashArray also have features that protect your security logs even further. By running the solution in our SafeMode™ feature with Splunk or Elastic log analytics, you ensure that your logs can't be deleted. That way, you can confidently recover after a security breach and will have the information you need to analyze the event and take action to prevent it from happening again.

Regardless of how many security solutions you deploy—whether it's network access control, data loss protection, firewalls, intrusion prevention systems, identity access management, cloud access security brokers, antimalware, endpoint detection, or all of the above—it's critical to have an action plan for detecting and remediating a security breach when or if it occurs. **Download *10 Questions to Ask Your CISO* to get your plan in motion.**