USE CASE

Protecting Critical Assets from Data Breaches

When it comes to protecting a network, organizations need to defend critical IT assets from any potential threat – whether inside or outside of the organization. In many cases the source of the breach may not be aware of its culpability – such as the victim of stolen credentials, or a system running a Trojan horse programmed to automatically send confidential data to an unauthorized recipient.

The challenge is keeping an eye on all systems within a large, heterogeneous environment, accurately identifying improper or malicious user behavior, as well as detecting software-based breaches. While many of the systems already in place may be capable of detecting a specific category of events, it is critical to have the ability to identify any potentially malicious behavior.

LogRhythm can help monitor and protect critical IT assets:

	Controlling User Access	Protecting Critical Data	Identifying the Threat
CUSTOMER CHALLENGE	The larger the company, the greater the challenge in keeping track of individual users and identifying if and when an account has been compromised. Globally distributed workforces make it even more difficult to correctly identify compromised credentials.	Excessive data transfers may signify aberrant behavior, but determining whether transfers are suspicious or legitimate is difficult in an enterprise environment. Without backend correlation of all log and event data, many organizations have no way to tie large data transfers to specific assets.	Insider threats are not always tied to specific user behavior. In many cases they are perpetrated by malicious software that has either been intentionally loaded onto a machine or has been installed on a vulnerable system through an external attack such as a worm or Trojan horse virus.
LOGRHYTHM SOLUTION	LogRhythm can send out immediate notifications when an account is added or modified. Active Directory integration allows administrators to easily correlate authorized access with relevant activity indicating inappropriate behavior or compromised credentials.	LogRhythm's wizard-based toolset allows users to easily set up alarms to alert on data transfers meeting specific criteria such as size or frequency. Advanced filters provide additional granularity by allowing users to identify individual assets or specific time windows.	LogRhythm can automatically alert on suspect behavior on controlled servers and devices. This can include general activity such as non-whitelisted processes starting up, or specific blacklisted actions, including outbound file transfers or ftp services starting up.
ADDITIONAL BENEFITS	LogRhythm's data enrichment capabilities provide a valuable context layer that allows IT administrators to quickly identify suspicious behavior, such as a user accessing the network from a non-whitelisted location or a duplicate set of access credentials being created for a privileged user's account.	LogRhythm's optional agents include Data Loss Defender – providing additional security on critical assets by independently detecting and alerting on removable media usage. It can even prevent the transfer of data to an unauthorized device such as a CD/DVD or a USB thumb drive.	The simplicity of the wizard-based GUI makes ad hoc investigations highlighting event propagation a quick and effective process. Advanced visualization is a feature of any investigation, mapping all locations where that same activity is observed for comprehensive forensics and rapid response.