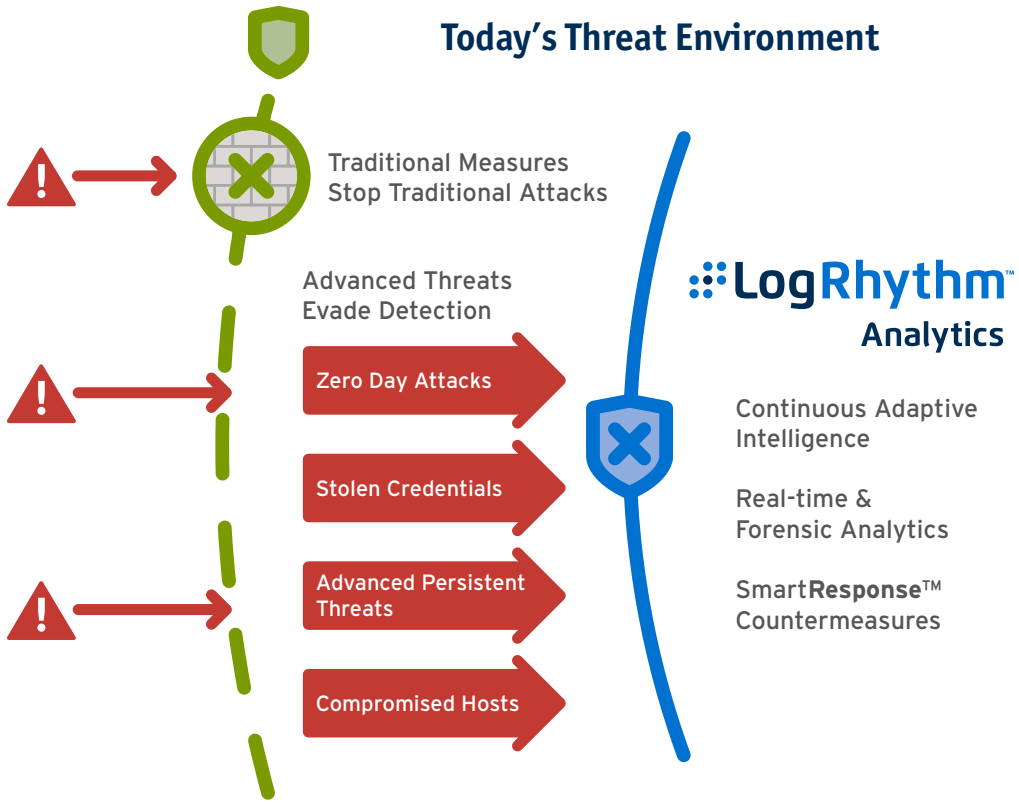
TECHNOLOGY INSIGHT

Analytics-Driven Defense

Most organizations have a layered security architecture in place. But even with this "defense in depth" approach, an alarming number of high profile breaches are occurring. Despite a heavier focus on preventative technologies, as well as extensive time and resources spent on hardening systems and applications, organizations are still missing the behavior patterns associated with attacks. Today's threat landscape demands a more modern, integrated approach.

LogRhythm's Analytics-Driven Defense combines the power of continuous monitoring with machine analytics and powerful forensic search capabilities to deliver an intelligent, 360 degree view of all critical activity on the network. Powered by LogRhythm's Security Intelligence Platform, Analytics-Driven Defense empowers organizations to detect and respond to attacks as they are happening, before they result in costly breaches.



LogRhythm Analytics

Real-time Analytics

LogRhythm's AI Engine uses powerful, machine-driven analytics, leveraging a variety of techniques to analyze the data from multiple dimensions. It performs advanced correlation against all data for sophisticated pattern recognition to identify suspicious or malicious activity. AI Engine also establishes automated behavioral and statistical baselines to identify what activity is normal on the network. This includes a unique ability to automatically establish whitelists of normal activity that can be used to immediately detect abnormal activity for accurate threat detection.

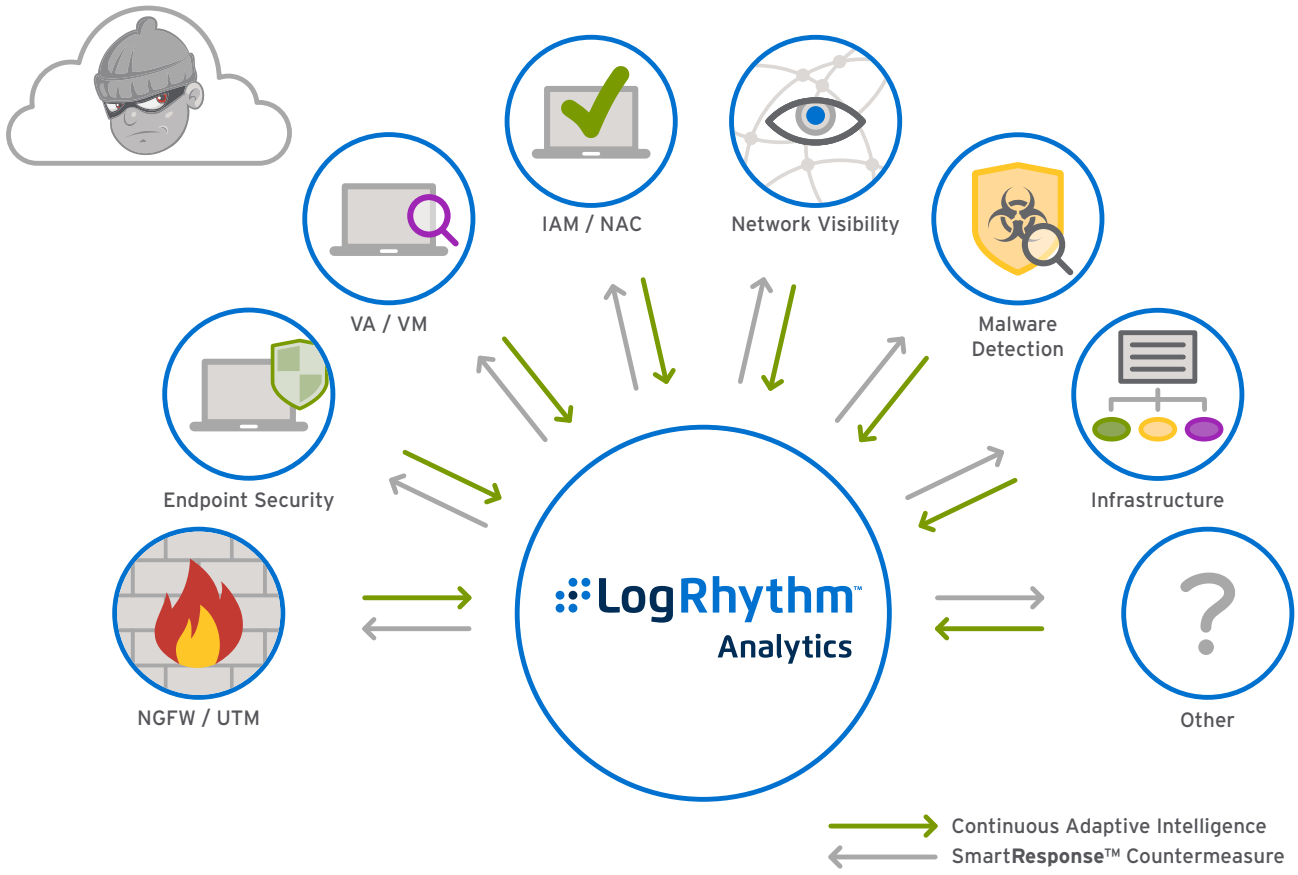
Forensic Analytics

LogRhythm provides powerful search and visualization tools to drill down and pivot through critical data, delivering quick and easy access to the forensic intelligence required to understand the origin and scope of even the most advanced threats. Every aspect of LogRhythm's advanced, HTML5-enabled user interface has been designed with the end-user in mind, making it easy to not only see what's happening in the environment in real time, but to quickly drill down into important event details for immediate analysis and rapid incident response management.

Smart**Response**™

Once an attack has been detected, it's critical for an organization to respond quickly to prevent a breach from taking place or mitigate damage if a breach has been discovered. The final step in the Analytics-Driven Defense approach to protecting the network is provided by LogRhythm's Smart**Response**™ feature. Through integration with partner technologies, such as next generation firewalls (NGFW), identify and access management (IAM) platforms as well as many other key technologies, Smart**Response**™ plug-ins take instant action to defend against breach attempts. It does so through intelligent, process-driven remediation that allows administrators to execute any script-based action, such as adding an attacking IP address to a firewall ACL or disabling a compromised user account, in response to any alarm. Smart**Response**™ remediation also comes with an optional, built-in approval process that can require up to three levels of authorization prior to taking action.

Analytics-Driven Defense



The following use cases outline how LogRhythm's Analytics-Driven Defense capabilities deliver enterprise threat detection and proactive response to defend against targeted attacks.

Compromised Credentials

Challenge Organizations need to correlate user profile data against actual user behavior to detect abnormal activity indicative of compromised credentials and internal threats.

Detection LogRhythm incorporates data from IAM platforms and correlates this data against all other machine and event data to create a baseline of normal user behavior. Real-time analytics immediately expose behavior deviating from the baseline such as concurrent VPN connections from two or more unique hosts within a short timeframe.

Defense Smart**Response**™ plug-ins automatically instruct IAM platforms to disable the user's account and signal integrated endpoint security solutions to add the suspicious hosts to watch lists.

Data Theft

Challenge Enterprises need to quickly detect unauthorized or suspicious data transfers to or from rogue IP addresses to avoid sensitive data loss, expedite forensic investigations, and prevent future data exfiltration attempts.

Detection LogRhythm analyzes data captured by NGFWs to correlate file access on classified servers with data movement to foreign or unknown IP addresses. When this activity is observed, a Smart**Response**™ plug-in automatically sends the observed traffic to an integrated network visibility tool for immediate packet capture to identify the contents of the suspicious data transfer.

Defense Smart**Response**™ plug-ins automatically add the suspicious IP addresses to the firewall ACL to prevent future network access and instruct IAM platforms to disable the user's account.

Malware Detection

Challenge Increasingly sophisticated malware combined with social engineering tactics are making it easier for attacks to bypass traditional, reputation-based security tools and trick end users into executing zero-day exploits.

Solution LogRhythm receives real-time security updates from malware detection tools that identify malicious files on the wire. LogRhythm performs advanced correlation and behavioral analytics on this event data to help identify which devices, hosts, applications and users have been targeted and/or successfully impacted.

Defense To prevent malware from propagating, LogRhythm Smart**Response**™ plug-ins initiate immediate protective action by integrating with infrastructure technologies and IAM solutions to isolate infected files and disable compromised accounts.