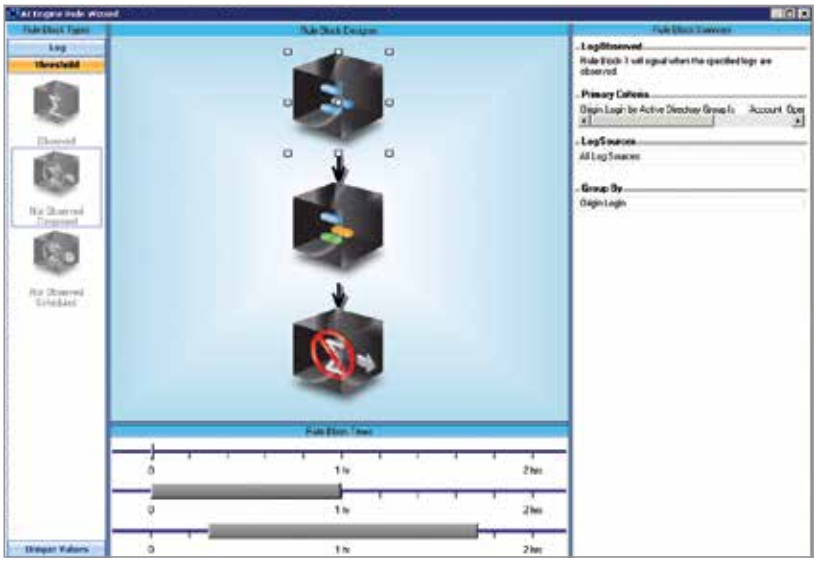
PRODUCT OVERVIEW

Advanced Intelligence (AI) Engine™

LogRhythm

LogRhythm's AI Engine is a fully integrated component of the LogRhythm platform, delivering automated, continuous analysis and correlation of all activity observed within the environment. With a uniquely flexible and comprehensive approach, it delivers real-time visibility to risks, threats and critical operations issues that are otherwise undetectable in a practical way. AI Engine is correlation that works.



With over 900 preconfigured, out-of-the-box correlation rule sets and a wizard-based drag-and-drop GUI for creating and customising even complex rules, AI Engine enables organisations to predict, detect and swiftly respond to:

- Sophisticated intrusions
- Insider threats
- Fraud
- Behavioural anomalies with users, networks and endpoints
- Compliance violations
- Disruptions to IT services
- And many other critical actionable events

Comprehensive advanced correlation

Unlike legacy SIEM solutions, AI Engine leverages its integration with the log and platform management functions within the LogRhythm platform to correlate against all data – not just a pre-filtered subset of security events. Seamless integration also enables immediate access to all forensic data directly related to an event.

AI Engine rules draw from over 70 different metadata fields that provide highly relevant data for analysis and correlation. This metadata includes the dynamic Risk Based Prioritisation (RBP) value assigned to all machine data, enabling the AI Engine to build trends and expose statistical anomalies based on the risk level associated with specific activity on the network. Whether detected by out-of-the-box rules or user-created/modified rules, AI Engine identifies and alerts on actionable events with tremendous precision, supporting security, compliance and operations use cases. AI Engine can also be used to cast a wide net through generalised correlation rules for broader visibility that accommodates changes in event behaviour.

Multi-dimensional analytics

LogRhythm has combined enterprise-wide advanced correlation and pattern recognition with automated behavioural and statistical analysis to deliver the industry's first Multi-dimensional Analytics capabilities. By combining advanced statistical and heuristic analysis with behavioural whitelisting, LogRhythm enables organisations to automate the process of learning what constitutes "normal" behaviour on any combination of attributes tied to users, hosts, applications, or devices. Integrating these capabilities with advanced correlation and pattern recognition eliminates three significant problems for users of 1st generation SIEMs: the inability to accurately define what constitutes "normal" activity, a deluge of false positives that reduce understanding of meaningful events, and uncertainty due to false negatives.

AI Engine delivers

- Advanced correlation against all log and machine data
- Generalised and targeted threat management and compliance automation suites
- Automated behavioural and statistical baselining
- Immediate access to underlying forensic data
- Extensive out-of-the-box advanced analytical rules
- Unparalleled ease of use

AI Engine in action

AI Engine's numerous predefined advanced correlation rule sets are configured to run out-of-the-box and act as templates for easy customisation. All rules within AI Engine can be quickly modified through a highly intuitive GUI to address the unique requirements of any organisation.

Secure

A single event is not always enough to indicate a breach or show the true reach of a security incident. AI Engine automatically generates behavioural whitelists of "normal" activity to help identify suspicious behaviour patterns and automatically identify and alert on potential threats and breaches. For example, malware can invade and spread through an organisation quickly, exposing data and weakening security faster than administrators can react. In many cases, the extent of the damage is unknown.

Examples:

- Malware is detected on a host, followed by multiple outbound attacks from that infected host.
- Suspicious communication from an external IP Address is followed by data being transferred to the same IP Address.
- A user logs in from one location, and then logs in from another city or country soon afterward.
- RBP score assigned to firewall logs steadily increases from 50 to 90 over the course of an hour.

Comply

AI Engine enforces continuous compliance by generating events when specific policy violations occur. These include protecting cardholder data or Protected Health Information (PHI) from unauthorised access and actively monitoring privileged user behaviour.

Examples:

- Five failed authentication attempts followed by a successful login to a database containing ePHI, followed by a large data transfer to the user's machine, all within 30 minutes.
- A file containing credit card data is accessed, followed by an attempt to transfer information from the same host to a USB thumb drive within 10 minutes.
- Multiple new accounts are created, granted escalated privileges, and then access critical data in a short period of time.

Optimise

Advanced correlation offers substantial value for operational insight and IT services assurance. Slight variations in specific activities or a particular sequence of typically common operations events may indicate critical operations issues.

Examples:

- A backup process is started, but no log is generated, indicating that the backup completed.
- A critical process stops and doesn't start back up within a specific timeframe.
- A large group of servers shuts down, followed by a smaller group of servers starting back up.
- High I/O rates on a critical server, usually only observed after-hours during backup procedures, are observed during normal business hours.

AI Engine deployment options

As a fully integrated component of any LogRhythm deployment, AI Engine can be deployed as a dedicated, high-performance appliance, installed as software on dedicated customer equipment, or deployed on multiple virtualisation platforms, including VMware ESX, Microsoft Hyper-V, and Citrix XenServer. High-performance appliances can process tens of thousands of logs per second and billions of logs per day. AI Engine possesses a horizontally scalable architecture, allowing for simplified, incremental expansion of the deployment to meet the processing volume requirements of any enterprise. All instances of AI Engine are centrally managed through the LogRhythm client console.

CITRIX XenServer vmware Windows Server 2012

Appliance Line	Max Processing	CPU	Memory (Expandable)	Storage	Chassis	Power	Ethernet	Dimensions	Weight
AIE5400 	30,000 MPS*	16 Core	128 (256) GB	1 TB	1U	100-240V	Broadcom 5720 (4 x 1GB)	H4.28CM x W48.24CM x D67.73CM	19.3kg
AIE7400 	75,000 MPS*	32 Core	256 (512) GB	1 TB	1U	100-240V	Broadcom 5720 (4 x 1GB)	H4.28CM x W48.24CM x D67.73CM	19.3kg

*Messages Per Second