Practical Architecture for Any Enterprise

::::LogRhythm™

Many organizations may have the same reasons for obtaining a log management/SIEM solution, but each has a unique set of operational circumstances governing specific requirements and the scope of implementation. A network might be highly segmented due to security policies or geographic distribution, mandating specific collection capabilities. Or an organization might be constrained by budget and staffing limitations, requiring an incremental approach to rolling out a deployment.

Whatever the reason, architecture plays an important role in determining the long term success of any log management/SIEM implementation. A true enterprise architecture has to meet multiple potential requirements, from flexible collection capabilities to an easily scalable architecture. IT executives need to be assured that the solution they invest in today will be able to accommodate their organizational needs tomorrow.

LogRhythm offers enterprise architecture options that can support IT environments of any size, with easy implementation, scalability and usability for rapid time-to-value.

Flexible Collection	Rapid Time to Value	Easy Expansion
CUSTOMER CHALLENGE		
With widely distributed networks, collection can be a challenge for many reasons. Requirements for secure data transmission, guaranteed collection and minimizing bandwidth consumption can be difficult without flexible collection options.	Few organizations have the budget or manpower for an expensive and protracted implementation. They need to know that the log management/SIEM solution they choose will be quick to install, easy to manage and scalable to meet future requirements.	Whether related to budget or practical operating constraints, many organizations use a phased approach to roll out enterprise solutions. However, it is important that they can leverage their initial deployment in any future expansion.
LOGRHYTHM SOLUTION		
LogRhythm provides multiple options for collecting log data from remote locations, including optional System Monitor agents, dedicated Site Log Forwarder appliances, and standard agent-less collection. All options are centrally monitored and managed through a single interface.	LogRhythm's straightforward design and turnkey appliances make installation a quick and easy process. Centralized management through a simple interface and a self-maintaining database keep operating overhead minimal.	LogRhythm's building block architecture and enterprise scalability allows organizations to expand at their own pace. As requirements exceed existing capacity, expansion is as simple as plugging in a new appliance as a simple addition to their initial investment.
ADDITIONAL BENEFITS		
System Monitor Lite and Pro agents come with additional, fully-integrated capabilities. Available features include file integrity monitoring, network connection and user activity monitoring, and independent process monitoring.	LogRhythm uses the same wizard-based process for operating all features, maintaining a consistent look and feel. This enables a steep learning curve and easy adoption for rapid time-to-value.	LogRhythm offers High Availability options that are architected with the same practical operating considerations. Deployment is available on a per appliance basis for maximum flexibility and convenience.