whitepaper

Controlling the Cost of SIEM

A Guide for Resource-Constrained Security Departments

solarwinds

whitepaper

solarwinds

Ask most security professionals about SIEM and you'll hear the words "expensive," "time consuming," and "difficult." At the same time, most agree that the benefits a SIEM can provide are essential to any security strategy—not to mention getting some relief in passing a compliance audit. The promise of SIEM is to provide continuous situational awareness, automate compliance reporting, and support the incident response process through root cause analysis and serve as an investigation platform. Unfortunately, due to the perceived negatives, smaller, more resourced-constrained security departments that most desperately need the automation and security improvements SIEM can provide don't believe that the benefits are within their reach.

There is good news though! All those negatives do still happen but only when an organization buys the wrong SIEM for their size and needs. SolarWinds® offers a lighter and lower cost SIEM that does away with enterprise SIEM complexity and cost issues. It's specifically developed for the resource-constrained security pro. This paper takes you through the economics of SIEM by outlining the various money pits and shortcomings of implementation and demonstrating how SolarWinds Log & Event Manager helps organizations get the power of SIEM without the cost.

Factors That Affect SIEM Cost

When looking at a SIEM implementation, the license cost can be just the tip of the iceberg. The majority of SIEMs are complex—having been developed for enterprise use—which means that a lot of additional work goes along with them. Potential additional costs for SIEM include:

Consulting

Many SIEMs (or SIEM "alternatives") require consulting for deployment. And, for some of the most complex SIEMs and SIEM "alternatives," consulting is required for basic customization.

Manpower to Manage/Tweak Data

Many SIEMs do not have self-managing databases, meaning that expensive DBA talent is required to configure the basic operation of the system. In addition, inefficient handling of the data can require constant tuning in and out of data.

Hardware

The SIEM application puts a significant amount of pressure on any database. Massive real-time insertion rates and simultaneous analysis and retrieval of data make it a performance-heavy application. Of course, more users requires more hardware. But what's often forgotten is that more features also requires more hardware.

High Support Costs

Most SIEMs are expensive, with average purchase prices of over $50,000. With the high license cost comes a big maintenance bill that has to be renewed every year.

EPS or Indexing License Expansion

The majority of SIEM license costs are based on "events per second." A popular, but complex SIEM alternative licenses products based on "Mb indexed per day." Gartner estimates that data volumes are doubling annually, meaning that license costs must also expand. And, to the previous point, so do support costs.

Add-On Components

SIEM vendors commonly push numerous add-on components with their products which increases costs for customers. Whether the charges are for individual connectors, content packages, additional analysis modules, or "apps," there will always be a new add-on that your sales rep encourage you to purchase.

whitepaper

Storage

A core function of a SIEM is to store log and event data for archive and historical analysis. Depending on the compression ratio and the method used, storage costs can be manageable or spiral out of control.

Types of SIEM Products and Costs

Over the years, the "old school" SIEM has been joined by a host of alternatives. The weighing of the aforementioned SIEM costs varies depending on the approach. These costs are established with the needs of smaller, resource-constrained security departments in mind. However, the costs do correspond with the company's growth and expansion.

Enterprise Traditional SIEM

Traditional enterprise SIEM products were designed for large security operations centers. However, as regulatory compliance needs grew, these SIEMs were sold to organizations that did not have the staff or resources to manage them. These SIEMs typically have a very high license cost (starting at $50,000) as well as numerous add-ons. Hardware, storage, and consulting are also high-budget requirements of these products. In addition, the complexity of the products require extensive training for staff to manage and use the SIEM.

SIEM Evolved from Log Managers

Many log management companies entered the SIEM market and gradually included SIEM-like functionality in their products. They also modified their pricing model—typically starting at $20,000 for the inclusion of SIEM functionality, increasing the costs with add-on features. The cost of these SIEMs (a common barrier to solving the SIEM challenge) is more difficult to quantify. However, the lack of advanced correlation capability, limited real-time awareness, and lack of built-in intelligence adversely impacts the health of security.

Security Analytics

Security analytics products are typically not SIEMs. They are products that record activity directly from the network and might combine these recordings with logs. Aside from license costs, storage is very expensive due to the all-consuming nature of these products. The additional benefits of recording everything on the network are typically weighed down by large-storage problems and sub-optimal event management.

IT Search/Big IT Data Management

These products got their start as a general IT Data Management and Search product. However, over the years they have marketed to the SIEM use case, and the overall costs for this approach continue to expand. The Mb indexed-per-day licensing model is a costly endeavor with large consulting fees for deployment and customization. Add-ons are also a factor with expensive "apps." The largest hidden cost with these products, however, is the large amount of time and extensive technical skills required to make this approach appear SIEM-like.

Change the Economics

SolarWinds allows resource-constrained security departments to change the economics of SIEM by providing a SIEM designed just for their needs. We've included the most critical capabilities of SIEM but have left out the bells and whistles that are seldom used and cause the most complexity. SolarWinds changes the economics of SIEM through:

No Consulting Required

We've designed our SIEM specifically for the tightly resourced department. That means making sure you can deploy it quickly and easily. Don't believe us? Download our free trial and see for yourself at **www.solarwinds.com/lem**.

whitepaper

No DBA or Extensive Care and Feeding

We've put a lot of effort into making our database self-managing. That means no expensive DBA resources or constant data management.

Hardware

We do require hardware because we've left out non-essential enterprise features that put more pressure on the database and the SIEM application. Still, our product requires a lot less hardware to run than the traditional, enterprise-level SIEM products.

Support Costs

Our support costs are lower because our pricing is much lower—typically 10-20% compared to other SIEMs. We're able to do this because we aren't spending enormous development budget to support large enterprise one-offs. This results in a significant cost savings that we pass directly to our customers.

Simple Node Based Pricing

You pay for only the number of nodes feeding the SIEM, not the event or indexing rate. This means that unless you decide to expand your implementation to a much larger number of systems, you don't incur additional license costs.

All In One

SolarWinds Log & Event Manager goes far beyond traditional SIEM. We offer extensive remediation, USB blocking, and database auditing.

Storage

SolarWinds Log & Event Manager minimizes overall storage costs by taking a straightforward, no-nonsense approach to providing better security and a high compression ratio.

Summary

Organizations of all sizes can realize the benefits of SIEM, but only by selecting the approach and the product that is best suited to their needs.

Learn More About or Download SolarWinds Log & Event Manager Today. Visit **www.solarwinds.com/lem**.