Huntsman®
Defence-Grade Cyber Security

On-premise Huntsman Enterprise SIEM:

Cost saving advantages for migrating customers

Following the acquisitions of the IBM QRadar cloud business by Palo Alto (a cloud native endpoint/XDR vendor) and LogRhythm by Exabeam (also cloud native and endpoint focussed) there is understandable concern about the future of the existing SIEM solutions, specifically the on-premise/software-based versions of both the QRadar and LogRhythm SIEMs.

SIEM users who specifically bought those solutions (in many cases instead of cloud-hosted endpoint solutions) are naturally worried about their chosen technology going end-of-life, lacking in investment or being steered towards the new vendor's cloud platforms that are focussed on endpoint detection, rather than the wider infrastructure monitoring and compliance coverage of SIEM.

This briefing note focusses on the cost savings and financial advantages of on-premise SIEM that existing users will be familiar with.

" Avoid the hidden costs of cloud-based SIEM "

1. For users who retain online/archive data for long periods cloud solutions can be expensive (for storage and extraction) or impose limits

Cloud solutions often impose data retention limits and/or don't allow data to be archived out (or they charge for it). This is not an issue with an on-premise SIEM like Huntsman where storage is only limited by what is available, and archives can be kept indefinitely.

2. Users with unusual or bespoke data sources may not be able to adapt standardised cloud-based systems to ingest this security information

They may be unable to do it locally and need expensive professional services. In extreme cases the customer might have already gone through this pain with an existing solution and will have to repeat it for the (different) cloud service they are forced to adopt. Huntsman can ingest any data source and reuse knowledge gained from past efforts to ingest data into other platforms, often improving on the approach.

3. Users will have to learn/adapt to a different new technology

While not impossible, there are costs and time commitments involved. Moving to a similar solution – i.e. from one SIEM to a different SIEM like Huntsman is easier than moving to an E/XDR or UEBA platform as they are closer in operation and architecture.

“ Nobody wants to buy a second endpoint solution ”

4. Users have a SIEM as the cornerstone of their SOC and may have XDR already

Several end-user organisations and MSSPs have a SIEM solution alongside an endpoint technology. The SIEM is the cornerstone of their SOC and stores security information and alerts. The XDR does endpoint threat detection and passes alerts to the SIEM.

If the SIEM was replaced by a different endpoint solution, the organisation would have to choose or migrate between them or run both in parallel – with neither fulfilling the “SOC cornerstone” function.

The Huntsman SIEM can support endpoint alerts from downstream threat detection solutions (UEBA/EDR/XDR) as a platform for SOC operations. It also has inbuilt threat detection and UEBA functionality.

“ Channel support deficits will hamper support ”

5. Resellers/VARs will cease support for on-premise SIEM products

Resellers who currently sell SIEM products (appliances or software licences) will prefer capex/support/maintenance revenue rather subscription-based cloud services. The acquisitions of traditional SIEM solutions will affect renewal opportunities, future upgrades for customers and change the revenue and commission to subscriptions rather than one off.

Some resellers may opt to cease support for solutions like LogRhythm and QRadar leading to less choice and high costs for customers needing ad hoc professional services or ongoing support and maintenance contracts.

Huntsman SIEM is architecturally and functionally equivalent to a LogRhythm or QRadar SIEM and can be licenced as a capex purchase with support or as a subscription model to compete with cloud offerings. Learning Huntsman SIEM for sales, installation and support purposes is a smaller leap that to go from an on-premise SIEM to a cloud-based XDR.

Talk to your reseller about engaging with Huntsman to offer the Enterprise SIEM solution, or contact Huntsman directly for a price to replace your existing solution and move to a direct support model from our local, expert, security-cleared team.

Contact Huntsman Security for a free migration consultation

Huntsman Enterprise SIEM is a solution delivered on premise, on hardware or virtualised, or for deployment in a customer’s own private cloud. It provides easy migration and a stable upgrade path for users of traditional SIEM platforms who are worried about the cost implications of data storage, movement or migration to/from cloud-bases SaaS platforms.

e ukinfo@huntsmansecurity.com t +44 845 222 2010 huntsmansecurity.com

Huntsman®