LogRhythm

5 business headaches that a cloud-based SIEM solves

If you are weighing the pros and cons of moving your security information and event management (SIEM) to the cloud, or you are under pressure to follow a cloud-first strategy, here are five business headaches a cloud-based SIEM can remedy.

1. Skills Shortage

More than
HALF
of companies report a problematic shortage of cybersecurity skills at their organisation. And it's getting worse[1]. There are **2.93 million unfilled security positions**[2] around the world.

Meanwhile
84%
of cybersecurity workers are open to offers of new employment[3]. Retaining the employees you have is essential.

How cloud-based SIEM helps

Cloud-based SIEM enables security teams to focus on threat hunting and resolving real threats, not on managing infrastructure problems or troubleshooting capacity issues.

With cloud-based SIEM, the infrastructure, capacity, patching and admin work is done automatically, leaving your security analysts free to focus on keeping your organisation safe. Plus, your analysts have more time to spend on work that matters to them.

2. Business continuity planning

If you are breached, can you keep your operations running smoothly?

In the last five years, more than
50%
of companies experienced an incident that interrupted operations[4] for at least eight hours or more.

Just 35 per cent of incidents are due to natural disasters – 45 per cent are down to operational issues and 19 per cent are caused by human error.

How cloud-based SIEM helps

Being cloud-based means your SIEM is available anywhere and at any time. If your business must relocate in response to an incident, your service needn't be interrupted by the move – so you maintain effective security.

And cloud storage of log data means it won't be lost if you lose access to on-premises logs.

3. Cost control

Spare a thought for your CFO.

On-premises software comes with a price tag. And, as a CapEx expense, it comes with a lot of headaches.

Large amounts of **upfront cash** are needed. **Predicting future capacity** needs is difficult. **Budget approval** can be a long and arduous process.

How cloud-based SIEM helps

Moving your SIEM to the cloud lets you shift from a CapEx cost to an OpEx cost.

A shift to the cloud means no costly, upfront investments in hardware. No wasted money caused by staffing for peak times, leading to underutilised staff. No costly software upgrades – you get the latest versions immediately, automatically.

Smooth out cash flows over time instead of requiring large capital outlays. And, when it comes to an OpEx, you may be eligible for possible tax and accounting benefits.

4. Invest in people, not infrastructure

Desks and chairs don't make your business more secure. Nor do server racks and air conditioning units. The right software and skilled staff do. But too often money and time must be pumped into hardware and infrastructure.

Many businesses spend large sums on building and running data centres, but the extra space alone doesn't improve security.

How cloud-based SIEM helps

Cloud-based SIEM lets you scale at pace. Which means you can focus your spending on securing your data and protecting your business.

With a cloud-based SIEM you can hire a highly skilled cybersecurity team that delivers strategic value for the business. It means you can focus on working with your data to protect your organisation, not on the operational aspects of storing and managing data[5].

5. Easy upgrades and patching, no hassles

Unpatched software represents a serious security risk. But staying updated is a huge time-sink and your SOC has bigger fish to fry. Employees are often irritated by having their work interrupted by updates and patches and can delay them for too long, or even decline them, unaware of their significance.

Should a highly skilled cybersecurity professional be wasting their time on patches and updates? They don't think so. A survey of security professionals found their preferred tasks[6] are:

Threat hunting
(55 per cent)

Resolving threats
(55 per cent)

Preventing threats
(54 per cent)

How cloud-based SIEM helps

Log monitoring, patching and policy enforcement must be done. Now, with cloud-based SIEM, the solution is simple.

With cloud-based SIEM, patches are applied automatically and without delay, cutting off one important attack vector at source.

Don't compromise.

You shouldn't need to compromise with cloud-based SIEM. A reduced feature set isn't a fair trade for flexibility and convenience.

With LogRhythm Cloud, get the power of the LogRhythm NextGen SIEM Platform with the ease and flexibility of a SaaS solution.

Maximise security team effectiveness

Delivering reduced mean time to detect (MTTD) & mean time to respond (MTTR)

Embedded security orchestration, automation and response (SOAR)

Comply with cloud-first initiatives

LogRhythm Cloud

The power of the LogRhythm NextGen SIEM Platform in the cloud

LogRhythm

[1] The cybersecurity skills shortage is getting worse:
https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html

[2] Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens:
https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0%5Ch

[3] What Employers Need to Know About Cybersecurity Jobseekers:
https://www.isc2.org/Research/Hiring-Top-Cybersecurity-Talent

[4] 17 Shocking Statistics about Disaster Recovery and Business Resiliency—Where Does Your Organization Stand?: Part 1:
https://www.datacore.com/blog/17-shocking-statistics-about-disaster-recovery-and-business-resiliency-where-does-your-organization-stand-part-1/

[5] If Everything is a Service, Why Do We Need Data Centers?:
https://www.datacenterknowledge.com/archives/2017/05/31/everything-service-need-data-centers

[6] Cyber Security Training: What CISOs Must Do to Mitigate Talent Churn:
https://blog.5nine.com/cybersecurity-training-what-cisos-must-do-to-mitigate-talent-churn