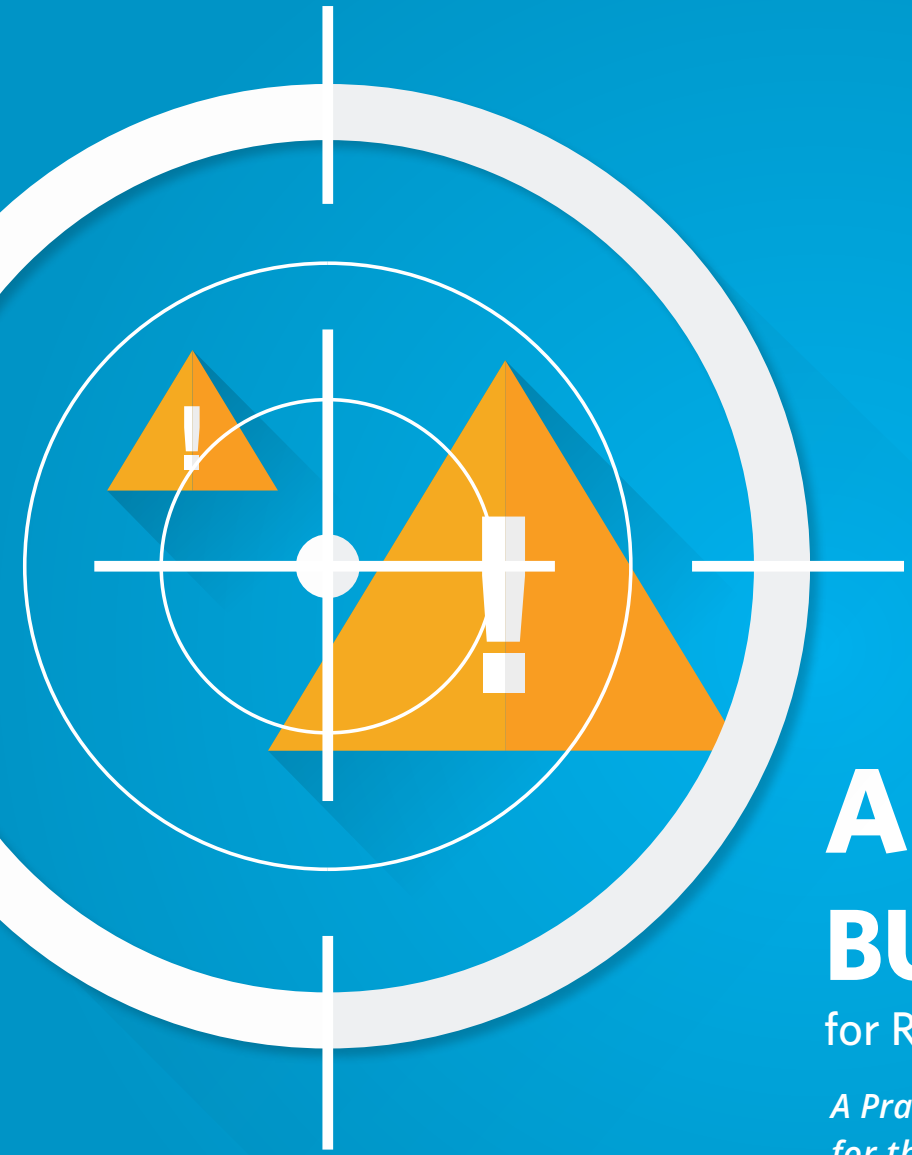
solarwinds



A SIEM BUYER'S GUIDE

for Resourced-Constrained Security

A Practical, No-Nonsense SIEM Buyer's Guide for the Tightly Resourced Security Department

A SIEM BUYER'S GUIDE

for Resourced-Constrained Security

A Practical, No-Nonsense SIEM Buyer's Guide for the Tightly Resourced Security Department

PERFECT SECURITY — a geographically distributed team of security analysts that make up an organization's Security Operations Center (SOC). They consistently stay on top of every potential threat and deploy a governance and policy management program that makes compliance an afterthought — because you will pass that audit. Sounds great! **But unless you're in the top 1% of security departments, that's a dream and the reality is drastically different.**

In 99% of organizations, the security story looks like this: **there's you** (and maybe a few others) trying to stay on top of security updates, manage security products, and deal with basic block and tackling. You would like to see and do more of what's needed to achieve sufficient IT security — **but there just isn't time or budget.**

Another time-draining and costly effort for the 99% security department is vendors. The bulk of security management vendors sell to the 99%, but spend most of their time serving the 1%. What does that mean? Huge license costs for complex products with advanced functionality that is designed for large implementations, but is seldom used.

Security Information and Event Management (SIEM), technology that collects, analyzes, stores and reports on security related events, has long promised to provide automated "SOC-in-a-box." A virtual army of security analysts, actionable intelligence, situational awareness, continuous compliance — the buzzwords and intentions go on and on. But over the years, failed deployments, consultant money pits and "there just isn't the time to use it" challenges have cast doubt on SIEMs' ability to truly fulfill its value promise.

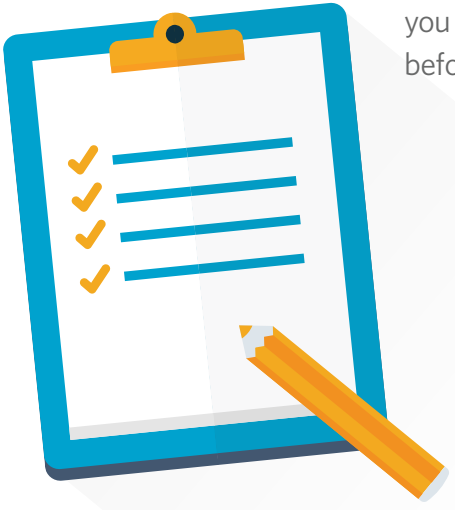
This guide has been designed by SolarWinds® Security experts to help the 99% security department get the critical security and compliance capabilities they need without falling into the enterprise SIEM money pit that they can't afford.

The following steps guide you through the process of purchasing an **efficient, cost-effective SIEM product** that will accommodate your security needs based on your company size and budget.

STEP 1 *Embrace the possibilities of SIEM*

Most organizations perceive SIEM as expensive and time consuming. While this might be true with enterprise SIEM products, the technology exists to help organizations just like yours benefit from this type of security. While you may not have a SOC and an army of security analysts, a good 99% SIEM provides intelligent automation to emulate those functions without endless maintenance. To start, know that it is possible to strengthen your IT security with intelligent monitoring, alleviate manual compliance reporting processes, and ultimately sleep better at night—without going beyond your budget or manpower. While an actual true, redundant SOC infrastructure might be out of reach, better and more efficient security and compliance doesn't have to be.

STEP 2 *Match the SIEM potential with your reality*



The promise of SIEM automation and security visibility is possible. But distractions lie ahead that you need to prepare for. Arm yourself against vendor-induced confusion by clearly identifying what type of help you want from a SIEM and how you need to interact with it. Here are some key questions to answer (in this order) before you embark on your budget-championing and vendor-selection journey:

- What are my objectives for adopting a SIEM? These can include compliance reporting, internal monitoring, stronger attack recognition capability, IPS alert validation, and incident response management. It is important to clearly identify your most important use cases because SIEM has infinite possibilities. Knowing your most important objectives will save you time and help you avoid vendor distractions during the selection process.
- How will I and others interact with the SIEM? If you're in the 99% overstretched security function, this question is crucial. Chances are you'll want to set up the SIEM as a virtual SOC—having it churn through data while identifying and prioritizing security issues for follow-up. If this is your intent, put an emphasis on out-of-the-box content, easy tuning, easy investigations, and powerful visualization.

STEP 3 *Choose vendors who "get" you*

Most SIEM vendors focus on enterprise-level organizations so their SIEM products and solutions are often too costly or challenging to manage for small IT security departments. During your buying process, look at the potential vendors' websites. If most of their marketing materials and messages are about big data, SOC operations, highly customizable risk management engines, or "enterprise" anything, they are likely not a good match for your needs.

Instead, look for vendors that focus on virtual SOC deployments for smaller security programs. This will take some research, but finding the right vendor for your purposes will be worth the effort. SIEMs that focus on the 99% offer more bang for the buck in extended features that reduce risk and accommodate more of your compliance requirements, such as USB blocking technology and extended remediation capabilities.

STEP 4 *Don't get distracted by edge use cases*

SIEM products have a lot of appealing features. The configuration possibilities and use cases of SIEM are endless. Many vendors use this to their advantage by selling edge use cases as core needs. There's no question that a highly customizable system might be useful at some point, but it's also important to be realistic about the level of customization and subsequent time commitment required. If you're struggling just to maintain the level of security you need with your given resources, focus on the basics. You'll accomplish what you need — and you'll still get a lot of the cool stuff out of it.

STEP 5 *Beware of SIEM "Alternatives"*

Unfortunately, SIEM has gotten a bad name among many in the security community — particularly those in the 99% organizations. This is because vendors, using the more-is-better pretense, commonly sold complex, enterprise-class products to smaller companies that didn't have the budget or manpower to support and manage them.

Due to the growing anxiety over security, smaller companies with limited budgets turned to one of the numerous SIEM "alternatives" that have sprung up. These vendors marketed their different approaches to security use cases to those companies who were burned by buying an enterprise SIEM they couldn't manage. If you're considering one of the SIEM alternatives, evaluate the log management and IT search vendors based on your need for intelligence, ease-of-use, ease of deployment, and manageable license costs. Otherwise, that alternative could result in needing expensive consulting, coding talent, and time to finish "rolling out your own" SIEM. These products are not tuned and optimized to get the real time intelligence needed from heterogeneous data sources. Many of the SIEM alternative vendors are talking about big data. Therefore, if you heed step 3 by choosing vendors that "get" you, you're already safe.

STEP 6 *Make Action a Priority*

So far, we've just focused on defining use cases and avoiding common distractions and money pits. Now it's time to focus on the question, "Once you see an issue, what should you do?" Most SIEM technologies point out issues that a fully resourced SOC following their well-planned, multi-step incident response process can respond to. But for the tightly-resourced security program, there isn't enough time for this kind of process. In addition to the intelligence, efficiency, and automation that SIEM can provide, a SIEM with action shrinks response time and reduces risk. Evaluate and place a priority on value-added functions that can block, quarantine, and actively protect your organization — both automatically and on demand. And make sure that those functions don't require buying a lot of that vendor's other products to make it work.

HOW SOLARWINDS CAN HELP

SolarWinds is the only SIEM vendor that's fully dedicated and focused on the 99% security department. We achieve this by emphasizing usability, ease of deployment, and out-of-the-box value while avoiding complexity through providing the features and functions that security programs like yours need. We make all this easy to purchase by keeping our license costs down — and you won't pay for features you don't need. We also add the ability to block USBs, audit databases, and actively respond and quarantine to provide a central point of security monitoring, investigations, and incident response. Download a trial of our product today or watch a demo to see for yourself at www.solarwinds.com/lem.

solarwinds
The Power to Manage IT