SIEM FOR SMALL BUSINESSES

Alternative solutions for endpoint management & security

Interfocus
A KYOCERA GROUP COMPANY

Light SIEM
Doesn't Mean
Light Security

SIEM Alternatives Might Be Right for You

Security Information and Event Management (SIEM) is a well-established cybersecurity solution that can often be too costly and complex for small and medium-sized businesses to deploy. To make matters worse, once businesses get SIEM up and running, they often realize that they don't have the IT staff or capabilities to use it effectively.

Cybersecurity solutions shouldn't break your budget or burden your staff. Finding an alternative, "light" SIEM option can ensure that you are still getting the benefits of a SIEM solution, but in a package and price tag that is easily manageable for staff and businesses of all sizes.

Interfocus
A KYOCERA GROUP COMPANY
Interfocus.us | Info@Interfocus.us

What Is SIEM?

The primary function of a SIEM is to collect and store all logs, alerts and event information in a corporate network. The information contained within a SIEM is invaluable when analyzing the source and impacts of security threats and incidents because it helps you:

- Monitor who is accessing your proprietary and private data through protected files, USB storage devices and printers
- Support investigations and forensic analysis when the inevitable security incident occurs
- Provide context and validation
- Identify suspicious events and malware on the web and in email

How does a SIEM help you do all of this?

In general, SIEMs provide:

- A complete dataset of information, events and logs about network activity that provides insights about threats and security incidents
- Real-time alerts based on the best and most complete set of information about network, application and hardware activity, speeding time to detect and respond to threats

These are great benefits—a reason that SIEM solutions are a “go-to” for many larger enterprises. However, when using a SIEM, you must configure it to know the specifics of the network itself and all of the other security tools included on your network. This is where the time, money and resources come in. You need to have an IT staff to set up the SIEM appropriately and monitor it to ensure that you are actually reaping the benefits of the solution. This takes time and money, and still doesn’t guarantee that you will be able to use the SIEM in the best way for you and your business.

What to Consider in SIEM Alternatives

Looking at alternative SIEM options doesn't mean you will be skimping on security or peace of mind. Instead, you need to think about how a solution is used. That way, you will know if you have the time and resources to deploy and manage the solution, and—ultimately—increase the safety of your data. When looking at options think about whether it has:

One Centralized Administration Dashboard

This helps you manage and update all endpoints and devices for a single user, a team or across your entire workforce.

Automatic Monitoring

The point of using a solution is that you can rely on it to automatically monitor the logs of a single application, a group of applications or all applications used by your business. Any solution you use needs to have this easy-to-use capability.

Simplified Policy Management

It should be easy to define, alert and report on user rights and privileges in regard to data access. Again, this is so it is not a drain on your IT resources or other staff.

Seamless Monitoring Behind the Scenes

Managing your security shouldn't take away too many of your valuable employees from their day jobs. It needs to be easy and seamless to manage your entire business network.

Real-time Administrator Alerts & User Notifications

You need to know when policy violations and security events have occurred. At the same time, your users need real-time notification when they are about to engage in risky behavior or if actual threats or incidents have been detected. All of these alerts need to be pushed out in "plain English" so that people aren't spending time or resources "decoding" what the solution is trying to tell them.

Interfocus
A KYOCERA GROUP COMPANY
Interfocus.us | Info@Interfocus.us

What Are Your Options?

As you consider alternative SIEM, evaluate your options with three questions:

1. Does it still provide me the benefits of a SIEM?
2. Does it cut down on the time I will have to spend managing the solution?
3. Does it cut down on implementation and management costs?

With that in mind, here are some options your company can explore instead of investing in a full-blown SIEM:

OPTION ONE

Build your own SIEM capabilities

using open source tools such as Hadoop. This option puts your IT team fully in control. You can narrowly define the functionality to address only those areas most critical to your risk and security: areas such as monitoring for data exfiltration, monitoring credential use and misuse, monitoring network connections, or something else. The option of developing a focused, single management capability can be very appealing to Small Businesses. However, proceed with caution. Having control of your capabilities still comes at a price. You or your team will be spending time and money to build and deploy the system. You'll also need to build custom integrations for the other IT tools that you use or create a plan designed to bring those into your infrastructure over time. For that reason, you need to carefully weigh the cost and benefits. You can spend a lot of time, resources and money becoming a development shop and creating a system that doesn't save costs or gain efficiencies in the long run.

OPTION TWO

Managed Security Service Providers (MSSPs) will deploy their own SIEM to your network. This is an option for businesses looking to reduce their initial cost for purchasing an SIEM solution. When looking at these options, though, you need to think through how you will manage the deployment time and costs. These are still part of the equation—even when using an MSSP.

OPTION THREE

Doing nothing is always an option, if you believe several things: that the risk to your business from cyber threats is minimal and can be managed; that your team will be able to rapidly aggregate and analyze network utilization logs in the event that you need to conduct forensics on a data breach; and that your audit and reporting requirements for external agencies are minimal, then you can postpone SIEM considerations until a later date.

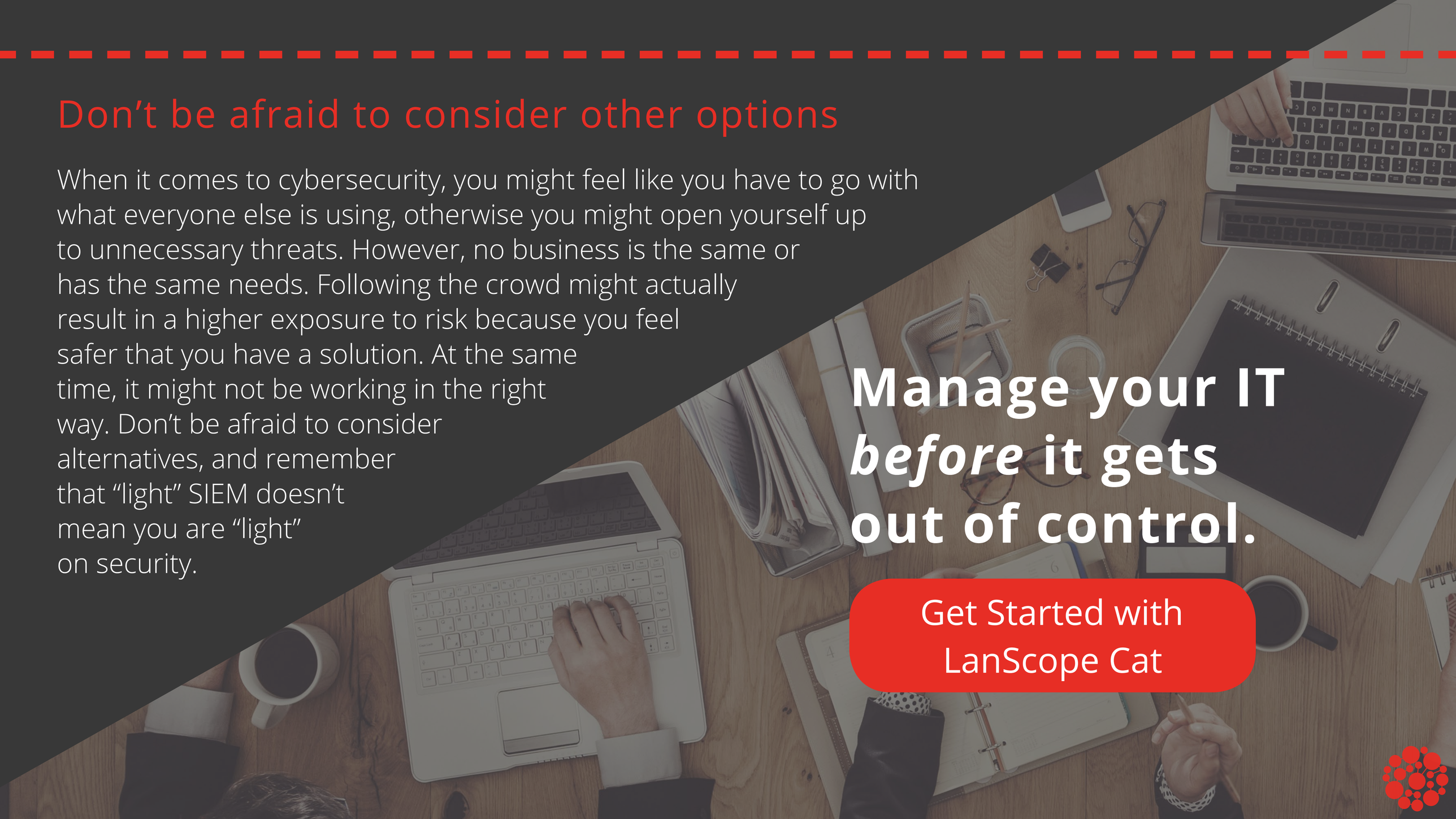
OPTION FOUR

"Light" SIEM Solutions offer you the same benefits as a SIEM, but are usually easier to use and come in at a lower price tag. For example, LanScope Cat is a SIEM alternative available in the US market. It still provides real-time threat detection and alerts. It logs the same type of data, has investigative capabilities and monitors endpoints, even USB devices. It does all this, but is also easier to deploy and manage with one centralized administration dashboard. In other words, a "light" option like LanScope Cat still gives you the SIEM capabilities, but will significantly cut down on your time and resources in managing your cyber risk.

Interfocus
A KYOCERA GROUP COMPANY
Interfocus.us | Info@Interfocus.us

Don’t be afraid to consider other options

When it comes to cybersecurity, you might feel like you have to go with what everyone else is using, otherwise you might open yourself up to unnecessary threats. However, no business is the same or has the same needs. Following the crowd might actually result in a higher exposure to risk because you feel safer that you have a solution. At the same time, it might not be working in the right way. Don’t be afraid to consider alternatives, and remember that “light” SIEM doesn’t mean you are “light” on security.



Manage your IT *before* it gets out of control.

Get Started with LanScope Cat

Interfocus
A KYOCERA GROUP COMPANY

Interfocus, a Kyocera Group Company, provides LanScope Cat, a unified endpoint management and security solution in the cloud that simplifies and automates how you control your team's devices in the workplace. LanScope Cat automatically inventories your PCs, laptops, peripherals and software licenses to provide visibility into how users interact with your proprietary data. LanScope Cat's dashboard and reporting capabilities are used by over 10,000 companies and 8.6 million users, protecting their digital data and assets and ensuring compliance with both internal policies and external regulations.

Start your free 14-day trial of LanScope Cat today!

INTERFOCUS.US

3565 CADILLAC AVENUE
COSTA MESA, CA 92626

INFO@INTERFOCUS.US