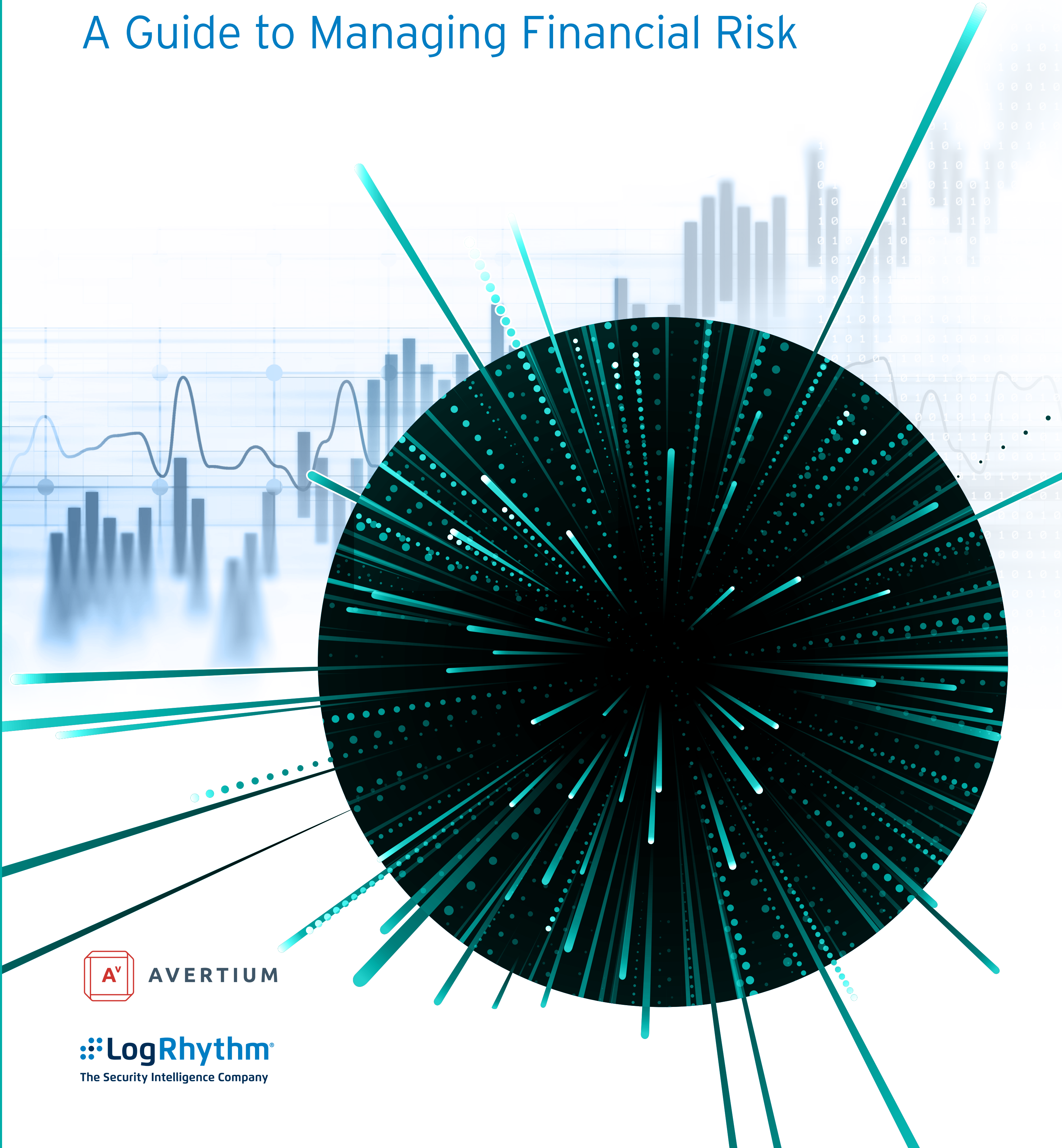
Budgeting for a Modern SIEM

A Guide to Managing Financial Risk



AVERTIUM

LogRhythm®
The Security Intelligence Company

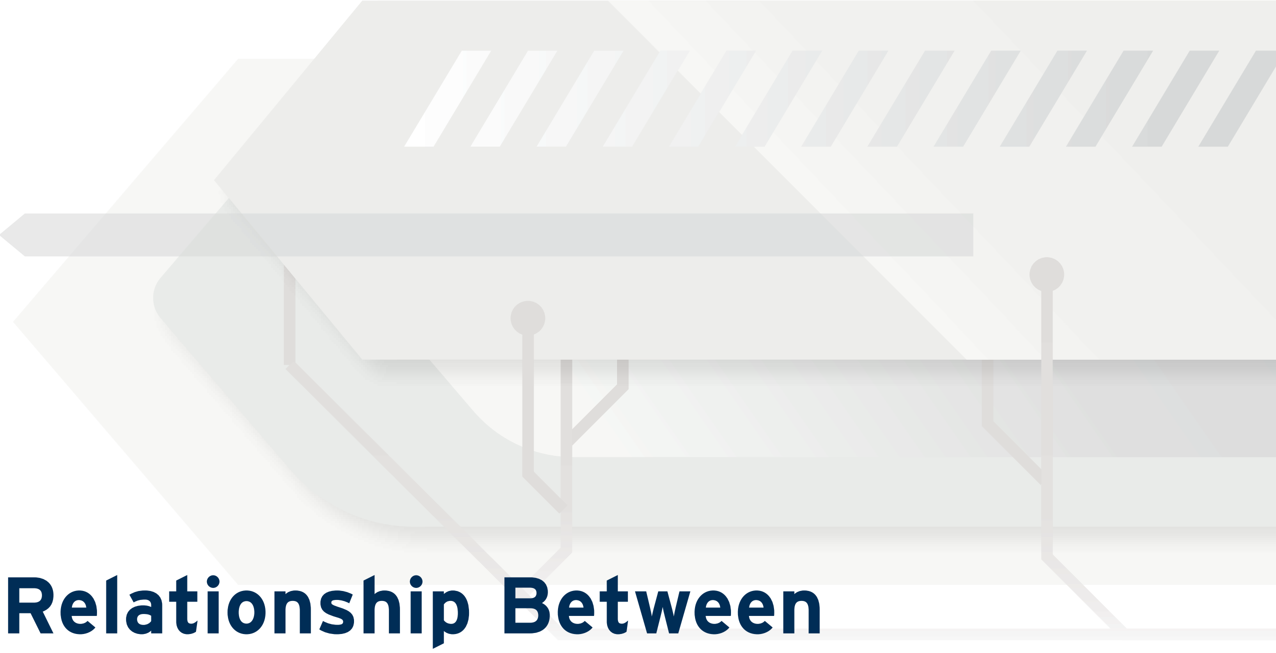
TABLE OF CONTENTS

For CEOs, growth is a welcome challenge — it's an indicator that business is healthy. But growth also poses a real challenge for CISOs for two reasons: First, when budgeting for a security information and event management (SIEM) system, CISOs are often faced with a tradeoff between limiting security threats and the cost of security operations. Second, larger businesses are a more attractive target for cyberadversaries.

Faced with an unpredictable cost expenditure, CISOs historically had to make tough decisions that increase the enterprise's risk exposure: Which logs do we collect and analyze? How long do we keep them? How do we balance current needs versus future company growth? How do I maintain flexibility when making a multi-year commitment to a SIEM platform?

> Faced with an unpredictable cost expenditure, CISOs historically had to make tough decisions that increase the enterprise's risk exposure.

There's no doubt, big data volumes are unpredictable and growing at an exponential rate. But there is hope. CISOs and CFOs don't have to live with the pain, frustration, and unpredictability of consumption-based pricing. In this guide to SIEM pricing models, we educate today's SIEM buyers on how to mitigate the security and financial risks associated with business growth.



The Relationship Between Business Growth and Security

Business growth has a direct impact on an enterprise's security posture as well as on the security organization itself. Growth can take different forms and represent varying degrees of risk, depending on the nature and maturity of the enterprise.

Increased Headcount

Business growth is often associated with a growing workforce. If sales increase, then so too must the employee base in order to maintain service levels. Inevitably, more people mean more data. Each employee results in an increase of network traffic and an increase in log and machine data generated by network devices as well as the many systems they use to do their job. That's more data to process and analyze as part of the normal course of security operations.

Growth can also cause the employee base to extend beyond the four walls of the existing location. The business may open remote offices or expand into new geographic areas. These new locations require new IT infrastructure and security systems, all of which generate additional data and expand the enterprise's attack surface.

There's also the issue of the people themselves. Each new employee increases the company's risk exposure. Each is, in essence, another threat vector. They can be an insider threat with malicious intentions, or an unknowing vulnerability easily exploited through social engineering, for example. The security organization is responsible for ensuring that new employees receive the appropriate training and understand the company's security policies and processes, but that doesn't always mean compliance with company procedures. The only way to be certain that employees are applying their training is to monitor behavioral changes in their user data with user and entity behavior analytics (UEBA).

Business growth results in larger workforce, revenue, and infrastructure. Without proper security coverage, this can expose an enterprise to greater risk of cyberattack.

Enterprises often hire contractors and freelancers to augment staff during times of rapid business growth or to bring innovative products and services to market. While these independent third parties can help reduce labor costs, they also present a security risk. Contractors and freelancers walk a fine line between trusted insider and insecure stranger. Security and IT teams must actively monitor and manage contractors' access to sensitive systems to ensure they do not exceed their access rights or introduce a threat into the environment. Depending on the maturity of the enterprise's hiring practices, the security team may not receive notifications of new contractors and freelancers – further increasing the risk posed by these individuals.

Infrastructure Growth

Business growth for a modern, digital enterprise often leads to IT infrastructure growth. For example, if an e-commerce website experiences a steady increase in traffic, the IT organization may deploy additional web servers. If the company's customer base grows significantly, it might be time to upgrade the database. Or lines-of-business may need to adopt new applications or systems to manage business processes that were previously fluid or manual when growth was negligible or stable. In short, business growth results in a growing IT environment.

The impact of infrastructure growth on security is similar to that of a growing workforce. The additional networking and computer equipment add to the volumes of data generated by the environment. That data is critical for understanding how the systems are operating and for detecting and stopping malicious activity. Meanwhile, each system and piece of hardware must be secured properly to prevent them from becoming a threat vector.

Increased Revenue

It's an unfortunate fact: the more an enterprise is worth, the bigger a target it becomes. No enterprise is immune from a cyberattack, but business growth attracts attention – some you want, and some you don't. Savvy cyberadversaries pay attention to what's going on in the business world. They read the news and monitor social media. Motivated by financial gain, business growth indicates an enterprise is a lucrative target.

There's another issue related to increased revenue and business growth that bodes well for cyberadversaries. An enterprise undergoing rapid growth is often in flux – there's a lot of activity and a sense of urgency as the workforce responds to the influx of business by onboarding new employees, signing new contracts, and so forth. Meanwhile, marketing and public relations teams often publicize financial milestones in press releases or on the corporate blog. This is a prime opportunity for crafty cyberadversaries who are looking to commit fraud. They can leverage the general air of urgency within the enterprise along with the information they find online to conduct a savvy phishing attack targeting the upper echelon of your enterprise.

The Modernization of IT

The enterprise data center is undergoing significant change thanks to modernization initiatives. These changes represent a form of business growth, as the IT environment grows bigger and more complex and dynamic.

As part of digital transformation, many enterprises are replacing legacy hardware and software with current offerings. These systems typically have more features and advanced capabilities, such as automation and analytics. Oftentimes, new IT solutions are easier for employees to use and for administrators to manage. However, there is a downside to modernizing IT. The logs from the latest digital tools and systems contain more data than their legacy equivalents. This data can be valuable to help protect the enterprise, but the SIEM must process and store it.

Similarly, moving infrastructure, systems, and applications to the cloud also impacts data volumes. Cloud-based IT assets tend to generate more data than the same assets hosted on-premises. Because the IT organization gives up some control over these assets when they move them to the cloud, the log data is vital for maintaining visibility of the environment and properly securing the assets off-premises.

Finally, business growth can come in the form of net new technology. Think, for example, of digital transformation, artificial intelligence (AI), the Internet of Things (IoT), and robotic process automation (RPA). Each of these requires updated technology systems with their own supporting infrastructure. Whether it's deployed on-premises or in the cloud, the new technology stack introduces an influx of valuable log data. As enterprises experiment and innovate with these technologies, it's important that they can monitor them and keep them secure.

Regardless of the type of growth your enterprise is experiencing, it is likely to become a larger, not smaller, target. Furthermore, one form of growth is likely to be accompanied by another. You never want to fall behind on your security coverage.

Regardless of the type of growth your enterprise is experiencing, it is likely to become a larger, not smaller, target … You never want to fall behind on your security coverage.

The Risk of Business Growth

Business growth generally elicits excitement from executives, but for CISOs and the security organizations charged with protecting the enterprise, business growth has a dark side.

"Chief information security officers and their teams should be focused on protecting their companies from damaging cyberthreats, armed with the visibility and data to do so effectively," said James Carder, CISO and VP of LogRhythm Labs. "They shouldn't be worrying about how much data they're consuming and how that will reflect on their overall bill."

Unfortunately, that is often the reality for CISOs and security leaders of growing companies. Protecting the enterprise against advanced threats is challenging enough – now CISOs also have budget constraints to keep them up at night. Security organizations whose enterprises are undergoing rapid growth have a high likelihood of exceeding their SIEM budget. It's difficult to project future SIEM budget needs, especially if the enterprise is undergoing diverse types of growth, as is often the case. Faced with exponentially growing log and machine data, security organizations often have no choice but to cap the volume of log data that their SIEM is processing and analyzing.

Security Risks

Reducing the volume of data that you send to your SIEM may be a logical way to fix a financial problem that's only going to grow – after all, the data isn't going to get smaller. The problem is that this approach introduces security risk that the enterprise definitely cannot afford.

"When you're trying to manage data consumption, potentially limiting intake into your SIEM, you lose visibility – putting your company at significant risk," said Carder.

Data is your window into the inner workings of the IT environment; excluding data from the SIEM creates a blind spot. Any activity could be taking place there, and the security team would be none the wiser. Furthermore, there's no "right" system to exclude, because you don't know what you don't know. It's difficult to make that choice ahead of time because you don't know which data is most important until you need it. The very log data you choose to exclude from the SIEM could contain the only clue that there's been a security breach. But you'll never know if the data isn't available in the SIEM for analysis.

Some security organizations determine which log data to exclude from the SIEM based on the value of the asset generating it. If the asset is of high value – say, the customer database – the SIEM processes the log data. If the asset is of low value – for example, a project management application used by marketing – the team might choose to leave that data out. The organization might also identify attack scenarios in an effort to prioritize data, but security professionals cannot predict the unknown. A low-value server may have a zero-day vulnerability. Or an employee may misuse IT assets, putting a low-value asset at risk. Or an attacker may breach an unmonitored, low-value asset and move laterally into high-value assets without warning.

Bottom line: organizations can't afford to treat medium- to low-value assets as if they aren't high priority.

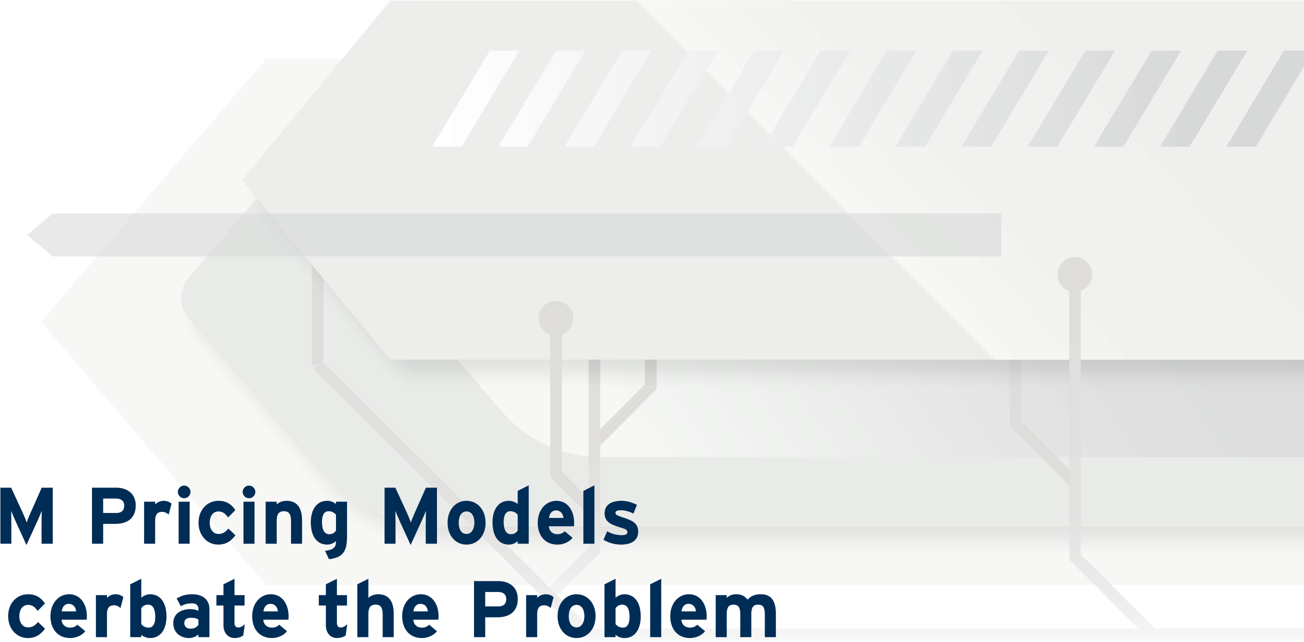
A SIEM analyzes current data in relation to historical data. So, the choices you make today about which data sets to exclude will impact your ability to detect threats in the future.

How do you know what data will be important to you six months from now? Simply put, you don't.

Excluding data hamstrings your ability to fully understand the scope of an attack. Effective threat investigation requires that you capture and analyze all data.

That brings us to another critical issue associated with log and machine data and your SIEM. Security organizations invest a lot into their security infrastructure. Excluding any data lowers the efficacy of the tool. It can't provide you with a complete picture of what's happening in your systems. The incomplete data, as a result, increases the time to detect and respond to threats. But, again, you still don't know what you don't know! You can't confidently answer questions like how long has this malicious activity been taking place? How much damage was actually done? Will you have the information you need to answer questions that your board/shareholders will have if you face a breach?

How do you know what data will be important to you six months from now? Simply put, you don't.



SIEM Pricing Models Exacerbate the Problem

SIEM vendors don't help. In fact, the two most common subscription models only make the data-versus-budget problem worse. Historically, vendors have charged based on capacity. Their customers pay a certain amount per message, gigabyte, or event per second, for example. It's easy to see how an organization can exceed its SIEM budget considering business growth under this pricing model.

Recently, some vendors have adopted a user-based pricing model. Under this model, customers pay a certain amount of money per user, per year. It doesn't matter how much data each user generates, the organization still must buy per user. This alternative to capacity-based pricing has generated a lot of buzz in the SIEM industry because it presents a more direct, easy to understand way to size a SIEM. However, user-based pricing doesn't promise any more stability than capacity-based pricing, because employee headcounts are likely to increase with any business growth.

There are some scenarios where either user- or capacity-based pricing work well for enterprises. These are, primarily, instances where companies aren't experiencing rapid business growth. Capacity-based pricing is good for companies that can safely predict how much data they will process based on previous years; and user-based pricing is appropriate for companies that can safely predict how much the workforce will grow.

Neither of these subscription-based pricing models are conducive to business growth, and you don't have to do the math to see why.

In addition to the disadvantages already mentioned, under either model, enterprises lose affordability and predictability. Security organizations face the hard decision of what data goes unprotected and at what price. Not only are they increasing the enterprise's security risk by excluding data from the SIEM, but they're also reducing the ROI they realize from the tool. If they don't process all the data, they're not seeing the full the value of the SIEM.

Fortunately, there is another, better option for enterprises undergoing rapid growth.

Comparing SIEM Pricing Models

A new SIEM pricing model stands to disrupt the industry and transform how growing enterprises manage their SIEM budget: unlimited data processing.

A SIEM license for unlimited data processing is an insurance policy against unpredictable or rapid and unknown growth. It removes data ingestion restrictions, giving security organizations the freedom to ingest all data to fully protect the enterprise no matter what kind of growth the future brings. It doesn't matter how much data the SIEM processes or whether the data originates from the cloud or on-premises. It's all included in one predictable price.

For instance, the LogRhythm True Unlimited Data Plan sets a fixed subscription price for the SIEM. During the subscription term, an unlimited amount of data may be processed regardless of infrastructure growth or employee/user growth.

A SIEM unlimited data processing plan is based on the idea that CISOs shouldn't have to weigh risk against budget. Nor should they have to make difficult decisions about what data they will and will not protect. Now, they don't have to.

"SIEM data consumption is an uncontrollable cost that most CISOs can't afford. With LogRhythm's new True Unlimited Data Plan, we're alleviating this issue for the CISO so they can focus on what matters – protecting their company," said Carder.

Like the consumption- and user-based SIEM pricing models, the SIEM unlimited data processing plan isn't perfect for everyone. It is ideal for organizations that have variability in the volume of their log data and/or the size of their user base and whose executives value a predictable budget. The unlimited data processing plan allows these organizations to purchase a SIEM with a predictable price model independent of the other fluctuating costs resulting from business growth.

At last, CISOs have flexible and predictable licensing arrangements that allow them to focus on protecting the organization – and celebrate new growth milestones with the rest of the business.

A new SIEM pricing model stands to disrupt the industry and transform how growing enterprises manage their SIEM budget: unlimited data processing.

The table on the following page compares SIEM pricing models.

Comparing SIEM Pricing Models

SIEM pricing isn't a one-size-fits-all solution. Depending on the factors your company is facing, there may be one model that is better for your organization than another. The below table takes a look at some common factors that may influence your SIEM contract and how each pricing model best solves those factors when it comes to budget.

	CAPACITY-BASED	USER-BASED	UNLIMITED
Digital Transformation Initiative	Good	Better	★ Best
Seasonal Business	Good	Good	★ Best
Fixed IT Infrastructure	★ Best	Better	Good
Expanding Compliance Requirements	Good	Better	★ Best
Steady Employee Count	Better	★ Best	Good
High-Growth Business	Good	Good	★ Best

CONCLUSION

Your business must be able to grow without compromising security.

If your business is experiencing rapid growth – whether as a result of increased headcount, growing IT infrastructure, or IT modernization – then you need a modern SIEM with unlimited capacity and a fixed price. LogRhythm is the only dedicated SIEM provider to offer a True Unlimited Data Plan so you do not have to make difficult decisions about protecting your organization based on cost. At LogRhythm, our goal is to make it easy to keep company data safe – no matter what the changing scale.

Learn More About Unlimited Data

About Avertium

Avertium is one of the largest cybersecurity services providers to the mid-to-enterprise market. Forged out of three award-winning cybersecurity services companies, each with a unique perspective on the security landscape, Avertium brings enterprise-level security to the many mid-sized and larger organizations that don't have access to comprehensive, specialized protection. Avertium is a LogRhythm **Service Authorized Partner** with experience in deployment, management and configuration, etc.

More than 1,200 organizations in industries ranging from financial services and manufacturing, to technology and healthcare benefit from Avertium's managed security, consulting and compliance services delivered with more rigor, more relevance, and more responsiveness. The company's dual security operations centers are located in Arizona and Tennessee.

Avertium.ShowNoWeakness.™

Avertium | avertium.com | hello@avertium.com | 1.877.707.7997