



CYBERSHark WHITE PAPER

SIEM IN THE CLOUD:

COST-EFFECTIVE SOLUTIONS FOR TAKING CONTROL DATA OVERLOAD AND SCALING SECURITY

**Security is everyone's concern, but
it's our business.**

WWW.CYBERSHARKINC.COM

INTRODUCTION

Increasingly, both private and public institutions are realizing that to ensure the security of their IT operations, it is prudent to consider the merits of outsourcing their IT services. This new focus is now a key factor driving the explosive growth in cloud computing. The cloud computing model offers organizations the ability to:

- **scale IT smoothly and cost effectively, without the periodic need to retool and build up expensive base-I level infrastructure,**
- **re-architect systems and networks for growth, add staff, re-negotiatesoftware licenses, and**
- **proliferate security systems to monitor the increased data flows and ever-expanding points of vulnerability.**

Organizations that look to the cloud are looking for standard services delivered according to a pricing model that scales in a linear way with their consumption of those services. They also want to know that the services being provided are delivered securely, that their data is protected, and that the entire process can meet the rigors of any regulatory compliance requirements. A host of new technologies are making cloud computing possible. New virtualization techniques

allow providers of cloud computing to distribute computing power to the need more efficiently. High-bandwidth networks with protocol prioritization and optimization enable more business to be done off-

premise. New application-aware, business continuity technologies assure clients that cloud computing is resilient and business uptime will be preserved. Web- based applications enable software-as-a service (SaaS). And full-featured, remote systems management tool sets enable outsourcers to monitor and trouble-shoot systems and network problems in real-time.

(continued)




INTRODUCTION (CONTINUED)

Nevertheless, not every technology vendor understands the nature of cloud computing and reflects that understanding in their offerings. Many don't fully grasp the uniqueness of the outsourcing business model and how costs should scale evenly with service consumption. This is reflected in awkward or irrelevant pricing schemes extended to the cloud services provider. Not every vendor has architected their product to support multi-tenancy, sharing resources while maintaining logical partitioning by the client. Not every vendor scales gracefully, which forces providers to continually add gobs of new compute-power for small increments in service growth.


Finally, many vendors haven't thought through the need for client reporting that is distinct from management reporting. Here at CYBERSHARK, we understand cloud computing, and what is needed for our customers to be successful. As the pioneer and leader in Security Information and Event Management (SIEM) technology, CYBERSHARK is transforming all security related data – from the core to the edge to the cloud – into actionable security intelligence. We're providing organizations and providers of cloud computing with a whole new breadth, level, and quality of security decision support, putting the right information into the right people's hands at the right time to ensure compliance, reduce risk and assure business continuity.



GROWTH OF CLOUD COMPUTING



One of the key drivers of cloud computing is the runaway acceleration in our collective creation of data. In 2010, 161 exabytes of digital information were created. This is the rough equivalent of 3 million times the information contained in all the books ever written. Or, viewed another way, the equivalent of 12 stacks of books, each extending more than 92 million miles from the earth to the sun. This is a phenomenal amount of data, yet it's just a drop in the bucket. By the end of 2016, Cisco estimates that the annual global IP traffic will pass the zettabyte threshold. So if you thought an exabyte was pretty big – try stacking up 1000 of them to make a single zettabyte.




Yet all of this content lives somewhere and there are organizations and businesses that are legally responsible for the security, privacy, reliability and compliance of much of that data. As you can imagine, the resulting impact on IT resources is massive. So how are companies coping? In many cases they are outsourcing much of their IT responsibilities and looking to the cloud for solutions.

Forbes magazine believes that 2016 will be the year that the cloud will solidify its role as an innovation engine for business. Viewed as both the latest IT strategy buzzword and a gateway to new things, the cloud is perhaps best known for its ability to help companies contain costs.

The ease by which cloud-based services can be adopted as well as the clear economic benefit – for both the consumers and the providers of cloud computing services – are helping to drive the growth.



SECURITY SERVICES AND CLOUD COMPUTING



Security Information and Event Management (SIEM) is a vital component of what a cloud security services provider can offer its customers.


SIEM technologies enable outsourcers to deliver an extensive portfolio of security services, with SIEM providing a top layer of supervisory analysis and intelligence across the portfolio that provides much needed context and support for decision-making. SIEM transforms noisy, low-level security event information generated by firewalls and intrusion protection systems (IPS) devices into alerts that can be readily comprehended by security analysts.

SIEM uses data aggregation and event correlation algorithms and applies these to event logs generated from security devices such as firewalls, proxy servers, IDS and IPS devices, and antivirus software. SIEM products also normalize data – that is, they translate Cisco and Check Point Software alerts, for example, into a common format so the data can be correlated by a single system. The best SIEM vendors work with hundreds of different devices allowing the managed security service provider to pick best of breed and still consolidate the security intelligence with SIEM.

Regulatory compliance is another key value for SIEM in the Cloud. Customers operating under the guidelines of PCI, HIPAA, FISMA, NERC/CIP, GLBA, and more, need SIEM in their practice. According to a Forrester survey of 1,335 security decision makers, 32% buy SIEM technology for compliance and reporting, followed by 21% for incident investigation and 13% for log management.



SIEM IN THE CLOUD



Like network management software, SIEM tools generally consist of specialized servers or agents that function as data collectors, and one or more specialized servers for doing data analysis, correlation, and database functions with reporting.


SIEM is a natural fit to the outsourcing model. SIEM typically requires significant data storage that client organizations are challenged to provide; has high scaling requirements with respect to event collection; provides third-party device data interoperability that outsourcers can leverage across multiple customers; often requires a 24 x 7 security operations center approach, and may involve a compliance mandate – such as PCI DSS or HIPAA – with tightly defined technical requirements where outsourcers can demonstrate core competency across multiple customers in the same vertical.

According to Forrester Research, with compliance demands growing, such as Payment Card Industry Data Security Standard (PCI DSS), SIEM products are gaining considerable attention, and providers of cloud computing are positioned to become the primary providers of SIEM.

A fully realized SIEM solution can be both difficult to configure and costly to build. While some of the largest organizations have the budget and the intellectual capital available to build a SIEM solution of their own – most do not. Once again – the cloud has enabled a solution – SIEM in the Cloud.



SIEM IN THE CLOUD



CyberShark is a cloud-based security and compliance service that allows Managed Service Providers (MSPs) to deliver enterprise-class security information and event management (SIEM) to small business customers at an affordable price. CyberShark's scalable, multi-tenant software platform comes backed by a team of expert security personnel and uses the latest threat intelligence data to identify potential security breaches in real-time.

With CyberShark you can focus on building a sustainable SIEM services business that doesn't require you hire more security analysts or invest in expensive infrastructure. And your SMB customers? They can reduce risk and respond to threats faster while achieving compliance and ensuring business continuity.

CYBERSHARKS' technology powers the SIEM backbone of many of the world's leading MSP's and Remote Operations Centers. For organizations who want to "quick-launch" into the managed security services business, CYBERSHARK global MSP partners can private-label these services.

For providers of cloud-based security services, expanding the customer base can be challenging given the difficulty of managing every customer securely and cost-effectively - especially since each customer has unique service and compliance requirements. To address these diverse requirements, cloud-based providers need an infrastructure that is secure yet flexible, and can effectively scale to support all types and sizes of customers, without customizing the platform each time. CYBERSHARK technologies are sensitive to these unique requirements, and offer a range of compelling benefits highlighted below:

(continued)



Account Segregation System -

CyberShark is the market's only cloud-based SIEM solution that employs a multi-tenant architecture with comprehensive permission and segregation system that allows service outsourcers to keep each customer's data protected and separate, providing privacy, protection and integrity. Segregation of customer data is also extended to customer device types and to analyst teams. Analyst permissions can be tailored to allow/prohibit specific customer, device types or specific devices within customer.

Account Visualization System -

Visual representation of security information such as graphical dashboards and event graphs that illustrate dependencies help an analyst to more quickly and definitively identify an incident. Standard reports and templates can be customized for the needs of individual accounts (or for multiple accounts). Dashboard visualizations are layered allowing drill downs to get increasingly detailed views on any targeted element.

Virtual Account Views -

Providers of managed security services can offer customers their own virtualized view of security information. This can be customized, scheduled and accessed through a web-based report portal.

Advanced Correlation -

CYBERSHARK identifies suspicious patterns that would otherwise go unnoticed. Multi-dimensional correlation delivers unparalleled security visibility by tying together diverse security activities across the cloud provider's customer base. CyberShark allocates a full correlation engine to each cloud customer. Correlation functions include rule-based analysis, vulnerability correlations leveraging scanner data, plus statistical, and historical analysis.

(continued)



Customer-Based Alerting -

Security analysts cannot be effective watching a plethora of security events across multiple customer networks stream by their screen at high rates of speed. CyberShark enables security analysts to do more consultative, preventative, higher-valued work on behalf of their accounts, knowing that should any malicious activity occur, they will receive an automated alert relevant to that particular customer

Remote Updates and Patch Management -

All updates and patches appropriate to apply to deployed CYBERSHARK technologies, either on customer premise or in the cloud, can be delivered or installed remotely from a master “provider” machine that automates the process.

Compliance Audit Framework and Reporting -

CYBERSHARK provides an integrated security audit framework to facilitate regulatory compliance reporting. The framework provides the ability to create status reports that are relevant to the major regulations such as PCI, HIPAA, FISMA, etc. It includes:

- Knowledge-base guidance that details what the regulated customer must monitor and include in their reporting.
- Detailed, step-by-step instructions for configuring, aligning, and monitoring devices and other resources affected by the relevant regulation.
- Advanced correlation rules and report templates needed to speed deployment.



Multi-Device Coverage

CYBERShark integrates natively with hundreds of network and security devices, applications and databases. CyberShark is capable of connecting to most devices out-of-the box, and most importantly, these connections don't require installation on the actual devices. We connect and collect third-party device information non-intrusively.

CYBERShark also understands the cloud computing business model and can construct licensing that is sensitive to the unique requirements. Further, our SOC One professional services organization can provide comprehensive support to help implement and customize a SIEM environment tailored to the needs of the security service provider.

COST EFFECTIVE SUPPORT FOR EXPONENTIAL INCREASES IN DATA

CYBERShark has been working with some of the biggest names in cloud computing for many years. Supporting them with SIEM technology is our core business and we are good at what we do.

Our ability to securely segregate multiple data streams and customize reporting not only gives providers of cloud-based security services the opportunity to develop standard offerings that can be replicated for other customers, but also allows them to develop new, distinct offerings that can generate incremental revenue without further capital investment. Each customer will understand that the service being provided is relevant to them, and this can differentiate the cloud provider in the marketplace. We are the only SIEM technology vendor that "powers-the- cloud" in a way that supports exponential increases in data flows with modest increments in infrastructure costs. Our multi-tenancy and federated architecture put cloud providers in a position where they can grow their security business without experiencing spiraling costs.



ABOUT CYBERSHARK

CYBERShark is a pioneer of security and compliance solutions deployed and operated on premise, in the cloud or "as a Service" by providers of all sizes, government agencies and individual enterprises. Through our patented multitenant security information and event management (SIEM) technology, CYBERShark delivers unparalleled security visibility, prevents costly downtime and achieves and maintains compliant operations at a lower cost to operate.

To learn more about CYBERSshark MSSP solutions, visit: www.cybersharkinc.com



CYBERShark and the CYBERShark logo are trademarks of CYBERShark, Inc.

Other third-party trademarks are the property of their respective owners. © 2021

CYBERShark, Inc. All Rights Reserved.

