Monitoring the Hybrid Cloud: Evolving to the CloudSOC

Version 1.7
Released: January 7, 2015

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051
info@securosis.com www.securosis.com

Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

Copyright

Monitoring the Hybrid Cloud

Table of Contents

Introduction

As we wrote in The Future of Security, the collision of cloud computing and mobility continues to disrupt and transform security. We started by documenting the initial stages of this transformation, and we now turn our attention to implementation of controls as technology infrastructure adapts to our new automated and abstracted reality. That may sound like science fiction, but these technologies are here now, and we are only beginning to see how automation and abstraction ripple outward — transforming how technology services are provisioned, managed, and secured.

IT organizations need to accept their lack of control over infrastructure. In fact they often don't even know how the underlying systems are constructed — servers and networks are virtual and opaque.

Change is hard, and the security industry faces a distinct lack of control in a number of areas, which is enough to cause panic attacks. In terms of access, IT can no longer rely on ownership of or control over devices. Consumption occurs on user-owned devices everywhere — often not even through corporate-controlled networks. IT organizations need to accept their lack of control over infrastructure. In fact they often don't even know how the underlying systems are constructed — servers and networks are virtual and opaque. Compute, storage, and networking are now beyond the direct control of staff. You cannot just walk down to the data center to figure out what is going on.

As the mega-trends of mobility and cloud computing collide, security folks find themselves caught in the middle. The techniques used to monitor devices and infrastructure no longer work. There are no tap points, and it is often prohibitively inefficient to route cloud traffic through inspection choke points. Security monitoring needs to change fundamentally to stay relevant — even viable — in this cloud age.

This paper will dig into the new cloud use cases you need to factor into your security monitoring strategy and discuss emerging technologies which can help you cope. Finally we will discuss coexistence and migration to a means to monitor the hybrid cloud. You will be dealing with legacy infrastructure for years, so you will need to support this hybrid environment combining on-premise assets with stuff in the cloud.

The Cloud Is Different

For context on this disruptive innovation we borrow from our Future of Security paper's description of how and why the cloud is different. If you think these changes don't apply to you, think again. Every major enterprise we talk with today uses cloud services. Even some of the most sensitive and highly regulated industries, including financial services, are exploring more extensive use of public cloud computing. We do not see technical, economic, or even regulatory issues seriously slowing this shift. The financial and operational advantages are simply too great.

Defining 'Cloud': Cloud computing is a radically different technology model — *not* simply the latest flavor of outsourcing. The cloud combines abstraction and automation to achieve hitherto impossible efficiency and elasticity. This has created new business models and shifted the economics of technology delivery and consumption.

Cloud computing fundamentally disrupts traditional infrastructure because it is more responsive, more efficient, and potentially more resilient and cost effective, than the status quo. Public cloud computing is particularly disruptive, because it enables organizations to consume only what they need without the overhead of managing their own infrastructure, while rapidly adapting to changing needs at effectively infinite scale.

Losing Physical Control: Many of today's security controls rely on knowing and managing the physical resources that underpin technology services. This is especially true for security monitoring, but let's not put the cart before the horse. The cloud breaks the old model by virtualizing resources — including entire applications — into resource pools managed over the network. We give up physical control to standard network interfaces, effectively creating a new management plane of APIs and web-based management consoles. The good news is that centralized control is baked into the new model. The bad news is that this change is likely to destroy the traditional security controls you rely on. At minimum most existing operational processes need to change fundamentally.

> Holding onto the legacy security model would adversely impact the agility and speed with which we can do things in the cloud. Security needs to adapt to the new operations model — not vice-versa.

A New Emphasis on Automation: The cloud enables extreme agility, such as servers that exist only for minutes — automatically provisioned, configured, and destroyed without human interaction. Entire (virtual) data centers can spin up and go live with just a few lines of code. Scripts can automate what used to take IT staff weeks to set up physically. Application developers can check in a piece of code, which then runs through a dozen automated checks and is pushed into production on a self-configuring platform that scales to meet demand.

Security can leverage these capabilities too, enabling previously manual processes (like incident response and many security operational tasks) to be performed with much great speed and precision. Although the trade-off is that our old bottlenecks and fixed inspection points — including

mandated human checks — are gone because they cannot keep up. Holding onto the legacy security model would adversely impact the agility and speed with which we can do things in the cloud. Security needs to adapt to the new operations model — not *vice-versa*.

The cloud's elasticity and agility also enable new operational models such as DevOps, which blurs the lines between development and operations to consolidate historically segregated management functions to improve efficiency and responsiveness.

The cloud's elasticity and agility also enable new operational models such as DevOps, which blurs the lines between development and operations to consolidate historically segregated management functions to improve efficiency and responsiveness. Developers take a stronger role managing their own infrastructure, by programming and automating operational tasks through easily accessible APIs. DevOps is incredibly agile and powerful, but contains seeds of potential disaster for both security and availability, by condensing and eliminating many application development and operations checkpoints and failsafes.

Legacy Problems Fade: Some security issues which have plagued practitioners for decades are no longer problems in the cloud. The dynamic nature of cloud servers can reduce the need for traditional patching — you can simply launch a new fully up-to-date server and shift live traffic to and from it with an API. Network segmentation becomes the default because all new instances are in security groups. Automating reduces the need for as many skilled staffers to perform manual tasks. Centralizing resources improves our ability to audit and control, while still offering ubiquitous access.

Monitoring Needs to Change

The entire concept of monitoring depends on visibility. We need to pull logs and events from the network and security devices protecting your environment. What happens when you don't have access to those devices? Or they don't work like the familiar devices in your traditional data center? You need to reconsider your approach to security monitoring.

There are architectures and techniques to address this lack of visibility and device access, which we will discuss in the Solutions Architecture section, but for now suffice it to say that we need to instrument the other parts of the technology stack where we can.

But we won't get to this new model overnight. It may take upwards of a decade or longer to fully realize the promise of cloud computing for the masses. You'll need to support both traditional infrastructure and cloud-based resources for the foreseeable future. Moving forward one success criterion will be an ability to straddle both worlds and provide an end-to-end view of what's happening — regardless of where infrastructure and data actually reside.

We aren't saying you will move your entire existing SIEM and other monitoring technologies to the cloud now — or perhaps ever. But you will need some form of monitoring infrastructure in the cloud soon.

The cloud has created new business models and shifted the economics of technology delivery and consumption. We will continue to harp on the need for coexistence and consistency to reflect this hybrid reality. You need to ensure your monitoring infrastructure supports a smooth migration to the cloud, without compromising your ability to monitor or manage.

This is where the *CloudSOC* comes into play. *We aren't saying you will move your entire existing SIEM and other monitoring technologies to the cloud now — or perhaps ever. But you will need some form of monitoring infrastructure in the cloud soon,* so it is time to start thinking about how to architect it — to monitor infrastructure that resides in the cloud while taking advantage of the cloud's inherent advantages.

The Age of Analytics

Many of the security monitoring requirements identified in our SIEM 2.5 paper are still very much in play. These include detecting advanced malware attacks and figuring out whether mobile devices are accessing the right information within the environment. Those challenges are exacerbated by the hybrid cloud. Cloud systems generate lots of event data, and technology is available to perform advanced analytics on vast amounts of information, but these capabilities lag behind the latest threats, so you will need to carefully consider how to detect attacks in new environments. There will always be more security data to analyze, so ensure your monitoring environment can provide advanced analytics at scale.

Monitoring must provide end-to-end visibility of all protected assets and data… regardless of whether they reside in a traditional data center, a private cloud, or a public cloud.

Compliance Confusion

Finally we need to acknowledge compliance. It is not yet clear how it will affect cloud adoption. We don't think regulation will be able to derail the cloud juggernaut, but it would be foolish to expect assessors to simply sign off on protected data being moved into shared environments without proper controls and oversight. That puts security monitoring squarely on the critical path for moving these key functions to the cloud.

So far the only certainty is that monitoring must provide end-to-end visibility of all protected assets and data… regardless of whether they reside in a traditional data center, a private cloud, or a public cloud. Compliance requires you to address all these environments. Your assessor couldn't care less whether you buy and provision servers yourself or spin them up using cloud autoscaling. If devices can access protected or sensitive data, you will need to substantiate controls.

Emerging SOC Use Cases

As stated above, numerous disruptive forces are increasingly complicating security monitoring. Those new models require much greater automation, with significantly less visibility and control over the physical layer of the technology stack. So you need to think about monitoring a bit differently.

This starts with getting a handle on the nuances of monitoring, which depend on where applications run. So we will discuss monitoring both IaaS (Infrastructure as a Service) and SaaS (Software as a Service). Not that we discriminate against PaaS (Platform as a Service), but for monitoring PaaS is quite similar to IaaS. We will also consider the impact of private clouds on your security monitoring. You cannot unplug your data center, so you need to provide an end-to-end view of your infrastructure, including both technology you directly control in your data center, and stuff you don't in the cloud.

Monitoring IaaS

The biggest and most obvious challenge in monitoring Infrastructure as a Service is the reduced visibility because you don't control the physical stack. You are largely restricted to logs provided by your cloud service provider. We see encouraging improvement in the depth and granularity available from cloud log feeds, but they still provide much less detail than devices in your data center.

You also cannot tap the network to capture packets for analysis. IaaS vendors offer abstracted networking, which lacks many features you have come to rely on. Depending on the maturity of your security program and incident response process, you might not be doing much packet capture in-house either, but it is no longer an option in the cloud.

One workaround is to run all network traffic through a cloud-based choke point for collection. In essence you perform a 'man-in-the-middle' attack on your own network traffic to regain a faint taste of the visibility inside your own data center, but that sacrifices much of the architectural flexibility that makes the cloud so attractive.

You also need to figure out where to aggregate and analyze collected logs, from both the cloud service and individual instances. These decisions depend on a number of factors — including where your technology stacks run, the kinds of analysis to perform, and what expertise you have available on staff.

Monitoring SaaS

If monitoring IaaS offers a 'foggy' view compared to what you see in your own data center, Software as a Service is 'dark'. You see what your SaaS provider shows you, and that's it. You have access to neither the infrastructure running your application, nor the data stores that house your data. What can you do?

If monitoring IaaS offers a 'foggy' view compared to what you see in your own data center, Software as a Service is 'dark'. You see what your SaaS provider shows you, and that's it.

You can take solace in the fact that many larger SaaS vendors are starting to get the message from angry and worried enterprise clients, and they increasingly provide activity feeds to pull into your security monitoring environment. They don't provide visibility into the technology stack, but you will be able to track what your employees are doing within the service — including administrative changes, record modifications, and login history.

You will need to figure out thresholds and actions to alert on, most likely by taking a baseline of activity and then looking for anomalies. There are no out-of-the-box rules to monitor SaaS in your environment. As with IaaS you need to figure out the best place to aggregate and analyze.

Monitoring a Private Cloud

Private clouds virtualize your existing infrastructure in your own data center, so you still have an opportunity to get full visibility, right? Yes, but there are differences. You will be able to tap the physical network within your data center for additional visibility. But for the abstracted layer above that — which contains virtualized networks, servers, and storage — you need proper access and instrumentation to see what happens within virtual devices.

As with IaaS you can route network traffic within your private cloud through an inspection point, but the cost in flexibility is again substantial. The good news is that existing security monitoring platforms are rapidly adding the ability to monitor within virtual environments by leveraging inspection points available within the private cloud. We will address options for extending existing monitoring environments below.

The table below summarizes the data sources, issues and workarounds for the major cloud deployment models:

	Use Case	Data Sources	Limitations	Workarounds
IaaS	Alerting: ++ Forensics: + Compliance: +++	Cloud provider logs, instance logs, app logs	No physical network access	Route traffic through inspection point
SaaS	Alerting: — Forensics: 0 Compliance: +	SaaS Provider Logs	No access to technology stack or app	SLAs
Private Cloud	Alerting: +++ Forensics: ++ Compliance: +++	Virtualization layer logs, instance logs, app logs, physical network layer	Need to instrument virtualization layer	Route traffic through inspection point
On-Prem (Traditional SIEM)	Alerting: +++ Forensics: +++ Compliance: +++	Event logs from security, network and applications	Significant effort to deploy and maintain. No visibility to cloud resources.	Cloud-based collector

(Key: + is good. — is not so good.)

SLAs Are Your Friend

As we teach in the CCSK (Certificate of Cloud Security Knowledge) course, you don't have much leverage to demand access to logs, events, or other telemetry from a cloud provider. So exercise whatever leverage you have during the procurement process: document the specific logs, access, and other visibility points you want in your agreements. You will find that some cloud providers (the smaller ones) are much more willing to be contractually flexible than the cloud gorillas. So you need to decide whether standard logging from the big guys is sufficient for your analysis.

Exercise whatever leverage you have during the procurement process: document the specific logs, access, and other visibility points you want in your agreements. Once you sign an agreement, what you negotiated is what you get.

The key is that once you sign an agreement, what you negotiated is what you get. You will be able to weigh in on product roadmaps and make feature requests, but we all know how that goes.

CloudSOC

If a large fraction of your technology assets have moved into the cloud, there is a final use case to consider: moving the collection, analysis, and presentation functions into the cloud as well. It may not make much sense to aggregate data from cloud-based resources, and then pull it back to your on-premise monitoring environment for analysis. More important, it is cheaper and faster to keep logs and event data in low-cost cloud storage for future audits and forensic analysis.

Part of monitoring the hybrid cloud is weighing the cost and latency of moving data to your in-house monitoring system against running monitoring and analytics in the cloud. This isn't really an either-or decision — you will probably need some of both.

But the fact is that you are likely to run computing both on-prem and in the cloud (a hybrid) for a while, which requires monitoring infrastructure both on-premise data centers and the cloud. As mentioned above, there are a variety of decision points for figuring out whether SOC systems should run in the cloud, on-premise, or both.

Solution Architectures

The good old days: Monitoring employees on company-owned PCs, accessing the company data center across corporate networks. You knew where everything was and who was using it. Even better, the company owned it all, so you could largely dictate where and how you performed security monitoring. The cloud and mobile change things, and we believe change things for the better. The agility and flexibility the cloud provides will spur a new wave of business innovation promising to change the nature of delivering technology services.

That being said, these new architectures will require new approaches to collecting event data. The sources and the information they contain are different. Equally important, although more subtle, is how to deploy monitoring services. Deployment architectures are critical to deploying and scaling any Security Operations Center (SOC) — they define how you manage security monitoring infrastructure and what event data you can capture. Additionally, how you deploy the SOC impacts performance and data management.

A variety of different architectures are available to address the use cases above. It is time to consider alternative ways to deploy collectors in the cloud, and the possibility of using a cloud security gateway as a monitoring point. Then we will take a look at basic cloud deployment models for a SOC architected to monitor the hybrid cloud, focusing on how to manage pools of event data from distributed environments — both inside and outside the organization.

Data Collection Strategies

Monitoring requires data, so how can you collect data from cloud resources? You have a few options:

- **API:** Automated, elastic, and self-service are all characteristics of cloud computing. Most cloud service providers offer a management dashboard for convenience and unsophisticated users, but advanced cloud features are typically exposed only to scripts and programs. Application Programming Interfaces (APIs) are the premier interfaces to cloud services; they are essential for configuring cloud environments, configuring and activating monitoring, and gathering data. These APIs can be called from

APIs are the cloud equivalent to platform agents, providing many of the same capabilities where a 'platform' is a virtualized abstraction and a traditional agent wouldn't work.

any program or service, running either on-premise or within a cloud environment. APIs are the cloud equivalent to platform agents, providing many of the same capabilities where a 'platform' is a virtualized abstraction and a traditional agent wouldn't work. API calls return data in a variety of ways, including the familiar `syslog` format, JSON files, and various proprietary formats. Aggregated data from APIs is a key source of information on hybrid clouds.

- **Cloud Gateways:** Hybrid cloud monitoring often depends on a gateway — typically an appliance deployed at the 'edge' of your internal network to collect events. Leveraging existing infrastructure for data management and SOC interfaces, this approach requires all cloud usage to first be authenticated to the cloud gateway as a choke point; after inspection traffic is passed to the appropriate cloud service. The resulting events are then passed to event collection services, comparable to on-premise infrastructure. This enables tight integration with existing security operations and monitoring platforms, and the initial authentication enables all resource requests to be tied to specific user credentials.

- **Cloud 2 Cloud:** A newer option is to have one cloud service — in this case a monitoring service — act as a proxy to another cloud service; tapping into user requests and parsing out relevant data, metadata, and application calls as the traffic flows past. As with a managed email security service, traffic passes through a cloud provider to parse incoming requests before they are forwarded to internal or cloud applications. This model can incorporate mobile devices and events — which otherwise never touch on-premise networks — by passing their traffic through an inspection point before they reach cloud service providers such as Salesforce and Microsoft Azure. This enables the SOC to provide real-time event analysis and alert on policy violations, with collected events forwarded to the SOC (either on-premise or in the cloud) for storage. In some cases these services can also add security by proxying traffic. One technique is to check personnel against on-premise identity stores to confirm current employment before granting access to cloud resources.

- **App Telemetry:** Mobile carriers, mobile OS providers, and handset manufacturers all provide very limited logging capabilities — just like cloud providers. Mobile platforms are intended to be secured from outsiders and not leak information between apps. But we are beginning to see mobile apps developed specifically for corporate use, as well as company-specific mobile app containers on devices which send basic telemetry back to the corporate customer to provide visibility into device activity. Some telemetry feeds include basic data about the device, such as jailbreak detection, while others append user 'fingerprints' to authorize requests for remote application access. These capabilities are compiled into individual mobile apps or embedded into app containers which protect corporate apps and data. This capability is very new, and will eventually help to detect fraud and misuse on mobile endpoints.

- **Agents:** You are highly unlikely to deploy agentry in SaaS or PaaS clouds; but there are cases where agents have an important role to play in hybrid clouds, private clouds, and IaaS clouds — generally when you control the infrastructure. Because network services are virtualized in most clouds, agents offer a way to collect events and configuration information when traditional visibility and taps at the network layer are unavailable. Agents also call out to cloud APIs to check application deployment.

- **Supplementary Services:** Cloud SOCs often rely on third-party intelligence feeds to correlate hostile acts or actors attacking other customers, helping you identify and block attempts to abuse your systems. These are almost always cloud-based services that provide intelligence, malware analysis, or policies based on a broader analysis of data from a wide range of sites and data to detect unwanted behavior patterns. This type of threat intelligence supplements hybrid SOCs and helps organizations detect potential attacks faster, but is not itself a SOC platform. You can refer to our other threat intelligence papers for details, including Leveraging Threat Intelligence in Security Monitoring and Leveraging Threat Intelligence in Incident Management.

Deployment Strategies

The following are all common ways to deploy event collectors, monitoring systems, and operations centers to support security monitoring:

- **On-premise:** We will forgo a detailed explanation of on-premise SOCs because most of you are familiar with this model and we have already covered them extensively. The infrastructure to monitor a hybrid cloud generally remains the same. The most significant change is inclusion of data from remote clouds, mobile events, and configuration data, along with monitoring policies to digest remote events. Be prepared for significant customization — cloud and mobile event data formats vary, and typically include slightly different information from one source to the next. Remember all your work a decade ago to get connectors to properly parse security event data? You will be doing that again until a standard format emerges. You will also need a new round of tuning detection rules — apparently acceptable activities for internal users and systems can be malicious, especially coming from remote locations or cloud services.

- **Hybrid:** A hybrid SOC is any deployment model where some analysis is performed in-house and some is performed remotely in the cloud. Monitoring cloud resources could be offloaded to a monitoring service vendor as described under “Cloud 2 Cloud” above, or perhaps a mix and match model where preliminary “Level One” analysis is performed by the external managed services team that monitors externally facing devices, with advanced forensics analysis handled by internal resources. Another option is for you to continue to run and operate your existing SIEM with all its event collectors, sending a subset of events to an external provider for the heavy lifting of event analysis and forensics if they offer expertise you don’t have in-house. Alternatively you could use an external provider to directly aggregate and analyze remote/cloud activity and send filtered alerts to your on-premise

SOC for analysis. A hybrid SOC offers agility for addressing new challenges while leveraging in-house investments and expertise, though there is a cost to maintain both internal and external monitoring capabilities.

- **Exclusively Cloud:** It is rare but definitely possible to push all data from both on-premise and cloud services up to a third party for full remote SOC services. This requires the remote SOC to provide all data management, analysis, policy development, and retention for security data. On-premise events are fed through a gateway to the cloud service; the gateway provides filtering, compression, and security to protect and optimize on-prem event data before its sent to the cloud.
- **Third Party Management:** Many large enterprises run security operations in-house, with a team of employees monitoring systems for attacks and analyzing suspicious alerts. But not every firm has a sophisticated and capable security team in-house to do the difficult and expensive work of writing policies and security analysis. So it is attractive (and increasingly common) to offload difficult analysis problems to others, keeping only a portion of this role in-house. You have flexibility in how to engage with a service provider. One approach is to have them take control of your on-premise monitoring systems. Alternatively a third party can supplement what you have by handling just external cloud monitoring.

Managing Vendor Lock-in

As you move towards the hybrid cloud and start to experiment with different IaaS and PaaS vendors, vendor lock-in needs to be a consideration. The fact is at least some portion of your monitoring strategy will leverage APIs and potentially other services (like logging, alerts, and message services) that could be proprietary to the specific cloud provider.

At this point, there isn't really anything you can do about that, except be aware and build your monitoring infrastructure (especially cloud-based resources) in a way to maximize flexibility. That's easier said than done, especially as the cloud providers continue to roll out additional services and capabilities, so you don't have to build them yourself.

Given a lot of the new services that Amazon is introducing within AWS (Amazon Web Services), we were joking that they are looking like the Hotel California. You can check out anytime you like, but you can never leave. Kidding aside, it's definitely something to be aware of, as you look to implement auto-scaling of your CloudSOC and leverage other capabilities of the cloud provider.

Technical Considerations

New platforms for hybrid cloud monitoring bring both new capabilities and new challenges. We have already discussed some differences between monitoring different cloud models, and some of the different deployment options. Now let's dive into some technical considerations for these new hybrid platforms, highlighting potential benefits and issues for data security, privacy, scalability, security analytics, and data governance.

As cool as a 'CloudSOC' sounds, there are technical nuances which must be factored into the decision and selection processes. There are also data privacy issues, because some types of information fall under compliance and jurisdictional regimes. Cloud computing and service providers can provide an opportunity to control infrastructure costs more effectively, but service models costs are calculated differently than on-premise systems, so you need a detailed understanding of the computing and storage characteristics of a SOC platform to work out where you are spending money.

Let's jump into some key areas where you need to focus.

Data Security

As soon as event data is moved out of one 'cloud' such as Salesforce into another, you need to consider its sensitivity, which drives the decision on how to handle security. Using SSL or similar technology to secure data in motion is the easy part — what to do with the data at rest, once it reaches the CloudSOC, is far more challenging.

You can get hints from folks who have already grappled with this question: security monitoring providers. They either build their own private clouds to accommodate and protect client data, or leverage yet another IaaS or PaaS cloud to provide infrastructure to store it. Many organizations find the cost and scalability advantages of storing cloud data in cloud services more attractive than moving all that collected data back to an on-premise system.

Whether you build your own CloudSOC or use a managed service, any time you have an external organization provide a key part of your security strategy, you need to pay special attention to the Service Level Agreements (SLAs) you establish with providers. These agreements specify the security controls implemented by a provider, and if something is not specified in that agreement they have no obligation to provide it. An SLA is a good starting point, but be wary of unspecified areas, where gaps are most likely to emerge.

A good place to start is a comparison of what the provider does against what you do internally today. Ask questions and get clear answers on every topic you don't understand — after you

execute an agreement you have no leverage. If you are running your own CloudSOC, make sure you carefully plan out your cloud security model to take advantage of your IaaS provider's offerings. You may decide some data is too sensitive to be stored in the cloud without obfuscation (encryption) or removal (typically redaction, tokenization, or masking).

Data Privacy and Jurisdiction

Over and above basic data security for logs and event data, some countries have strict laws about how Personally Identifiable Information (PII) data may be collected and stored, and some even require that PII not leave its country of origin — even encrypted. If you do business in these countries your team likely understands the relevant regulations, but for a hybrid SOC you also need to understand the locations of primary and backup cloud data centers, along with *their* regional laws. This can be incredibly confusing — particularly when laws conflict between countries.

Over and above basic data security for logs and event data, some countries have strict laws about how Personally Identifiable Information (PII) data may be collected and stored, and some even require that PII not leave its country of origin — even encrypted.

Once you understand your requirements and where your cloud (including CloudSOC) providers are located you can determine which security controls you need. Again data encryption addresses many legal requirements, and data masking and tokenization can remove sensitive data without breaking applications or security analytics. To figure out the right mix of controls you need to know where the data will be stored.

Automation and Scalability

If you have ever used Dropbox or Salesforce or Google Docs, you know how easy it is to store data in the cloud. When you move beyond SaaS to PaaS and IaaS you find it just as easy to spin up whole clusters of new applications and servers with a few clicks. Security monitoring, deploying collectors, and setting up proxies for traffic filtering… all benefit from the cloud's ease of use and agility. You can automate deployment of collectors, agents, and other services; or agents can be embedded in the start-up process for new instances or stacks. Verification and discovery of services running in your cloud can be performed with a single API call. Automation is a hallmark of the cloud, so you can script pretty much anything you need.

As you move toward production you will be constructing and refining initialization and configuration scripts to launch services, and defining templates which dictate when collectors and analytics instances are spun up and shut down via the magic of autoscaling.

But getting started with basic collection is a long way from getting a CloudSOC into production. As you move toward production you will be constructing and refining initialization and configuration scripts to launch services, and defining templates which dictate when collectors and analytics instances are spun up and shut down via the magic of autoscaling. You will write custom code

calling cloud APIs to collect events, and event filters if the API does not include suitable options. It is basically back to the future — hearkening back to the early days of SIEM when you spent as much time writing and tuning collectors as actually analyzing data.

You will also need to define and implement archiving. The cloud offers very granular control of which data gets moved from short-term to long-term storage and when. In the long run cloud models offer huge benefits for automation and on-demand scalability, but there are short-term set-up and tuning costs to get a CloudSOC working the way you need. A managed CloudSOC service will do much of this for you, at additional cost.

Other Considerations

- **Management Plane:** A cloud service's management plane is a double-edged sword. It gives IT admins the power to automate all services, using simple commands, from a single dashboard. But it also means you are completely helpless if an attacker gains access to the console. The power provided by a management console and management APIs demand greater diligence to ensure proper authentication and authorization than on-premise systems. That means far more attention paid to administrative rights, administrative entitlements, and monitoring from where and by whom the console is accessed — via both web console and API calls. Finally, we recommend a heavy dose of threat modeling to ensure your policies are tuned to the ways attackers could misuse cloud resources to access your cloud management environment.

- **Analytics:** To better detect malware and application misuse, companies look to leverage cloud-based big data computing for security analytics. This is a highly specialized field, with tools and techniques evolving rapidly. Cloud infrastructure providers make sophisticated analytical tools and infrastructure core offerings, helping to accelerate development of these capabilities for security. The issue is generally not a lack of infrastructure, but more often a personnel skills gap. Building and running security analytics require both competency with "big data" architectures and security analytics (analytics experts are typically called "data scientists") to mine through it. Regardless of how little it may cost to build a data warehouse today, only a handful of companies actually employ people capable of standing up a sophisticated security analytics environment. We see more companies using third party services — sometimes even in parallel with their own efforts — to perform additional analysis and triage security events across cloud and on-premise systems. These external companies have invested (typically VC money) in the resources required to deliver sophisticated security analytics.

- **Pricing Model:** To build your own CloudSOC you need to reconsider the economic model for cloud services, and then plan out how to move, store, and process data. Data travels through your data center for free. You ran the cable and installed the switches; those sunk costs enable you to use all available bandwidth without additional costs. PaaS and IaaS providers offer different pricing tiers for different types of network connectivity. Some offer free 'local' network traffic (within a logical network/availability zone), but charge for data

movement between data centers. If you leverage cloud messaging services for added reliability and event processing in your SOC, you will pay a tiny fraction of a penny per message. But even a low per-message price adds up across millions or billions of events captured and processed every year. Different data storage tiers are available, with performance and reliability rising alongside costs. The good news is that cloud providers offer good metrics and fairly clear pricing. The bad news is that you need to figure out how much of an abstract service (which you have never used) you need to model your cloud environment costs. Cloud economic models are fundamentally different, but your need to model costs remains.

The good news is that cloud providers offer good metrics and fairly clear pricing. The bad news is that you need to figure out how much of an abstract service (which you have never used) you need to model your cloud environment costs.

Migration Planning

We will finish up with a migration path to monitoring the hybrid cloud. Whether you choose to monitor just the cloud services you consume in a cloud-based monitoring environment, or go all the way and create your own SOC in the cloud, these steps will get you there.

Phase 1: Deploy Collectors

The first phase is to collect and aggregate the data. You need to decide how to deploy event collectors — including agents, 'edge' proxies, and reverse proxies — to gather information from cloud resources. Your goal is to gather events as quickly and easily as possible, so start with what you know. That means leveraging the capabilities of your current security solution(s) to get new events into the existing system. The complexity is not around understanding the new data sources — flow data and `syslog` output are well understood. The challenge comes in adapting collection methods designed for on-premises services to a cloud model. If an agent or collector works with your cloud provider's environment, either to consume cloud vendor logs or those created by your own cloud-based servers, you are in luck. If not you will likely find yourself rerouting traffic to and/or from the cloud into a network proxy to capture events.

We suggest collecting data directly from your cloud provider whenever possible, because much of that data is unavailable from instances or applications running inside the cloud.

Depending on the type of cloud service (such as SaaS or IaaS) you will have various means to access event data (such as logs and API connectivity). We suggest collecting data directly from your cloud provider whenever possible, because much of that data is unavailable from instances or applications running *inside* the cloud. Monitoring agents can be deployed in IaaS and private cloud environments, where you control the full stack.

But in other cloud models, particularly PaaS and SaaS, agents are generally not viable. There you need to rely on proxies, which can collect data from all types of cloud deployments, provided you can route traffic through their data-gathering choke points. It is decidedly suboptimal to insert choke points in your cloud network, but it may be necessary. Finally, you might instead be able to use remote API calls from an on-premise collector to pull events directly from your cloud provider. Not all cloud providers offer this access, and if they do you will likely need to code something yourself using their API documentation.

Once you understand what is available you can figure out whether your source provides sufficiently granular data. Each cloud provider/vendor API, and each event log, offer a slightly different set of

events in a slightly different format. You may need to build a collector based on sample data from your provider, because not all cloud vendors/providers offer logs in `syslog` or a similarly convenient format. Also look for feed filter options to screen out events you are not interested in — cloud services are excellent for flooding systems with (irrelevant) data.

Our monitoring philosophy has not changed. Collect as much data as possible. Get everything the cloud vendor provides as the basis for security monitoring. Then fill in deficiencies with agents, proxy filters, and cloud monitoring services as needed. This is a very new capability, so you likely will need to build API interface layers to your cloud service providers.

Our monitoring philosophy has not changed. Collect as much data as possible. Get everything the cloud vendor provides as the basis for security monitoring. Then fill in deficiencies with agents, proxy filters, and cloud monitoring services as needed.

Keep in mind that using proxies or forcing cloud traffic through appliances at the 'edge' of your cloud is likely to require re-architecting both on-premise and cloud networks, to funnel traffic in and out of your collection point. This also requires that disconnected devices (phones, tablets, and laptops not on the corporate network) be configured to send traffic through choke points, and cloud services be configured to reject direct access which circumvents these gateways. An inspection point which can be bypassed cannot effectively monitor security.

Now that you have figured out your strategy and deployed basic collectors, it is time to integrate these new data sources into your security monitoring environment.

Phase 2: Integrate and Monitor Cloud Resources

To integrate these cloud-based event sources into your monitoring solution, you need to decide which deployment model will best fit your needs. If you already have an on-premise SOC platform and supporting infrastructure it may make sense to simply feed the events into your existing SIEM, malware detection, or other monitoring systems. But there are a few considerations.

- **Capacity:** Ensure the existing system can handle your anticipated event volume. SaaS and PaaS environments can be noisy, so expect a significant uptick in event volume and account for the additional storage and processing overhead.
- **Push vs. Pull:** Traditional monitoring via Log Management and SIEM systems collect events from remote systems and agents *pushing* events. Then the collector grabs the events, perhaps performs some event preprocessing, and forwards the stream to the main aggregation point. But what if you cannot run a remote agent to push the data to you? This is the case in the cloud, so many cloud events must be *pulled* from the cloud service via active API requests via an HTTPS, SSL, or VPN connection. These requests are not automatic — you need a program or script to request the data. And the program (script) must supply credentials or identity tokens to authenticate itself to the cloud service. You need to make sure your system is capable of initiating the pull request and securely managing the API service credentials to retrieve the data.

- **Data Retention:** Cloud services require network access, so you need to plan for when your connection is down — especially given the current frequency of DoS attacks and network service outages. Understand the impact if you cannot collect remote events for a while. If the connection goes down how long can security data be retained or buffered? You don't want to lose that data, especially due to an auxiliary attack which is covering someone's tracks. The good news is that many PaaS and IaaS platforms provide easy mechanisms to archive event feeds to long-term storage to avoid event data loss, but this also requires setup.

- **Aggregation and Correlation:** Determine whether you need to aggregate and correlate cloud and on-premise activity within the same system. It may make more sense to store and monitor cloud resources separate from on-premise resources in your data centers, given that normal use (and misuse) event patterns differ between cloud and on-premise usage. Enforcement polices may be stricter for cloud resources because the data is "out there". You need to consider how best to correlate event data between the cloud and on-premise systems; cloud access logs typically include different information and may make it difficult to track users, requiring additional correlation against directory services and identity stores to produce actionable alerts.

If the environments being monitored are different enough between on-premise and the cloud you will not gain much leverage in terms of policies, reports, and dashboards by monitoring on a common platform. So it may make more sense to use a separate cloud service to monitor cloud resources. If scalability of your on-premise system is an issue consider pushing more monitoring and alerting into the cloud to take advantage of easy scaling; this may enable more robust analytics as well.

Phase 3: Policy Development and Testing

The security policies you have today, and the specific conditions that trigger alerts, will need updating for the cloud. Of course there is no simple recipe for this, so once again you need to dig in and start building out the policies. Start with the kinds of threats you need to catch, the data you need to detect those conditions, and alert thresholds that will help your folks respond faster to potential incidents. You can then identify gaps and incrementally tune policies to improve both accuracy and actionability.

For example you should ensure only the right folks can access your cloud services, but correlating IP addresses against user identities for cloud resources may not be possible. Further complicating matters, you likely don't want to limit access from mobile devices to cloud services the way you do with in-house services. And you need to build new policies that address specific cloud use cases — including access to the management plane, issuance of security certificates, and launching new applications. So we recommend taking a fresh look at cloud resources, and not assuming you will monitor cloud resources the same way as on-premise systems.

There is no short cut — this is work, plain and simple. Verify that you have the necessary event data to evaluate cloud-based activity and adjust policies to alert on cloud risks as part of your migration

and deployment processes. Understand that this is an iterative process; it will take time to enumerate potential attacks to look for in your hybrid environment, and then to tune policies for maximum effectiveness.

Phase 4: Automation and Orchestration

The bad news is that many of the workflows and incident response plans that (more or less) work for internal systems break when you move to the cloud. The way you detect a malware infection may be similar between IaaS and on-premise systems, but incident response is entirely different. So consider how your SOC processes and tools will need to change. Traditionally manual functions — including taking devices offline, upgrading hardware, and extracting images from devices — now happen via a cloud console or API calls. These cloud APIs provide a comprehensive way to orchestrate response and recovery without human intervention, based on a variety of triggers for policy violations.

Traditionally manual functions — including taking devices offline, upgrading hardware, and extracting images from devices — now happen via a cloud console or API calls. These cloud APIs provide a comprehensive way to orchestrate response and recovery without human intervention, based on a variety of triggers for policy violations.

The good news is that cloud computing enables you to respond to events faster and better. First, some types of attacks (including traffic anomalies, DoS, and Bitcoin mining) will likely be detected by your cloud service provider, who should notify you that something is amiss. For a real-life example check out our own cloud *faux pas*. Other issues are simply no longer problems in the cloud, so you won't need to respond to those situations. Some cloud vendors even offer 'add-on' security services such as configuration change detection, intrusion detection, and application threat analysis so you don't need to handle these functions yourself.

More importantly, cloud services provide a means to automate event response. In this CloudSOC model managing cloud-based resources no longer requires skilled investigators to manually validate and respond to all attacks — instead your response process leverages cloud APIs to automate necessary IT and security functions within your response plan. For example it is trivial to isolate a suspect application or server, spin up a freshly provisioned and patched replacement, move workloads over to the clean replacement, and then investigate the suspect device and forensic images at leisure. All this can happen automatically within seconds if your response processes have been rebuilt to take advantage of these capabilities.

And that is just scratching the surface of how you can establish a far more sophisticated prevention, detection, and response environment. Of course this requires work on your part — not least because each cloud provider supports different triggers and actions than their competitors — but the potential for much more sophisticated security than simple alerting and blocking on common

attacks, and the possibility of automating so much response, offer compelling motivation for migration to the cloud.

Phase 5: Migrate SOC Infrastructure to the Cloud

Sunk costs in existing infrastructure and economic realities will drive many of you to use your in-house SOC to monitor cloud services. There is nothing wrong with that — much of your infrastructure will likely run on-premise for at least the next couple years. For those looking to leave the in-house SOC behind, to leverage the agility and flexibility of the cloud, we offer some advice on migrating your SOC to an IaaS hosted environment.

First get your feet wet by standing up a smaller version of what you run today — basically a mini CloudSOC — which mirrors your in-house platform in an IaaS cloud. Use this mini CloudSOC to monitor cloud-based resources: aggregate and analyze event traffic and data collected from cloud API services, and dedicate a portion of your team to manage it. This approach is only a minor disruption to current on-premise SOC efforts, and gives your team time to understand the new tools and to focus on tuning collectors and policies for the cloud.

Once you have the mini CloudSOC in production and have learned how to tune it, you can scale it up by redirecting more and more collectors to it — perhaps including events and other data from on-premise data center assets. Regardless of whether you move all security monitoring to your CloudSOC, you will need similar processes and infrastructure to what you use with your on-premise monitoring system.

A wholesale shift of on-premise security monitoring to an IaaS CloudSOC is not for the faint of heart, so supplementing in-house systems with a mini CloudSOC dedicated to monitoring cloud services offers a good path for scaling up gradually. You will be running parallel systems for a while in any case; moving forward cautiously can help you make informed decisions about how quickly to proceed.

A wholesale shift of on-premise security monitoring to an IaaS CloudSOC is not for the faint of heart, so supplementing in-house systems with a mini CloudSOC dedicated to monitoring cloud services offers a good path for scaling up gradually.

Another option is to engage a third party for migration and management assistance. They can fill the gaps when your SOC team is stretched thin or lacks needed cloud skills. Third parties can help with migration or even take over CloudSOC operations entirely depending on what you need. Monitoring cloud activity is complicated by the cloud's tendency to break assumptions baked into monitoring tools, and the lack of in-house expertise to fully capitalize on its advantages. This transition is not easy so either short-term or long-term help can be valuable for getting where you need to be.

Summary

There are a variety of different use cases for monitoring the hybrid cloud. You can look at extending your installed on-premise SOC platform to gather data from SaaS and IaaS environments. You could aggregate events from cloud resources by collecting them in the cloud. You could also build a separate CloudSOC to monitor those resources. There are many choices for security monitoring as you support a rapidly evolving technology infrastructure.

We have discussed the pros and cons of these different alternatives and highlighted some of the technical considerations of the various choices. There are no right or wrong answers at this point — decisions are driven by how quickly your organization is moving to the cloud and what technical resources you have on staff. You will need to collect and analyze events from both on-premise resources and the cloud.

Collecting data from the cloud is inherently different, involving API calls and custom collectors to parse traffic, whether your aggregation point is in the cloud or within your existing SOC. So there will be a learning curve as you extend your monitoring environment to the cloud, which may be a good opportunity to engage with service providers who can supply data analysis capabilities and skills leveraged across many customers.

Over time we expect many organizations to embrace a model where their SOC runs in the cloud, as they hit a tipping point where most of their technology runs outside their data centers. The CloudSOC approach can provide scalability and analytics which are difficult to duplicate in traditional systems. But there are many ways to get there.

We recommend a controlled migration, embracing monitoring in the cloud for cloud-resident assets initially, while learning about the cloud and how to tune the monitoring environment. We understand that monitoring in two diverse environments creates many challenges, but the situation is manageable if you plan ahead. We wrote this paper to offer knowledge to help you start that planning.

If you have any questions on this topic, or want to discuss your situation specifically, feel free to send us a note at info@securosis.com.

About the Analysts

Adrian Lane, Analyst and CTO

Adrian Lane is a Senior Security Strategist with 25 years of industry experience. He brings over a decade of C-level executive expertise to the Securosis team. Mr. Lane specializes in application, database, and data security. With extensive experience as a member of the vendor community (including positions at Ingres and Oracle), in addition to time as an IT customer in the CIO role, Adrian brings a business-oriented perspective to security implementations. Prior to joining Securosis, Adrian was CTO at database security firm IPLocks, Vice President of Engineering at Touchpoint, and CTO of the secure payment and digital rights management firm Transactor/Brodia. Adrian also blogs for Dark Reading and is a regular contributor to Information Security Magazine. Mr. Lane is a Computer Science graduate of the University of California at Berkeley with post-graduate work in operating systems at Stanford University.

Mike Rothman, Analyst and President

Mike's bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Mike specializes in the sexy aspects of security — such as protecting networks and endpoints, security management, and compliance. Mike is one of the most sought-after speakers and commentators in the security business, and brings a deep background in information security. After 20 years in and around security, he's one of the guys who "knows where the bodies are buried" in the space.

Starting his career as a programmer and networking consultant, Mike joined META Group in 1993 and spearheaded META's initial foray into information security research. Mike left META in 1998 to found SHYM Technology, a pioneer in the PKI software market, and then held executive roles at CipherTrust and TruSecure. After getting fed up with vendor life, Mike started Security Incite in 2006 to provide a voice of reason in an over-hyped yet underwhelming security industry. After taking a short detour as Senior VP, Strategy at eIQnetworks to chase shiny objects in security and compliance management, Mike joined Securosis with a rejuvenated cynicism about the state of security and what it takes to survive as a security professional.

Mike published The Pragmatic CSO <http://www.pragmaticcso.com/> in 2007 to introduce technically oriented security professionals to the nuances of what is required to be a senior security professional. He also possesses a very expensive engineering degree in Operations Research and Industrial Engineering from Cornell University. His folks are overjoyed that he uses literally zero percent of his education on a daily basis. He can be reached at mrothman (at) securosis (dot) com.

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. Our services include:

- **The Securosis Nexus**: The Securosis Nexus is an online environment to help you get your job done better and faster. It provides pragmatic research on security topics that tells you exactly what you need to know, backed with industry-leading expert advice to answer your questions. The Nexus was designed to be fast and easy to use, and to get you the information you need as quickly as possible. Access it at <https://nexus.securosis.com/>.

- **Primary research publishing**: We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and conform to our Totally Transparent Research policy.

- **Research products and strategic advisory services for end users**: Securosis will be introducing a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessment.

- **Retainer services for vendors**: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. Even with paid clients, we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.

- **External speaking and editorial**: Securosis analysts frequently speak at industry events, give online presentations, and write and/or speak for a variety of publications and media.

- **Other expert services**: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These tend to be customized to meet a client's particular requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis. For more information about Securosis, visit our website: <https://securosis.com/>.