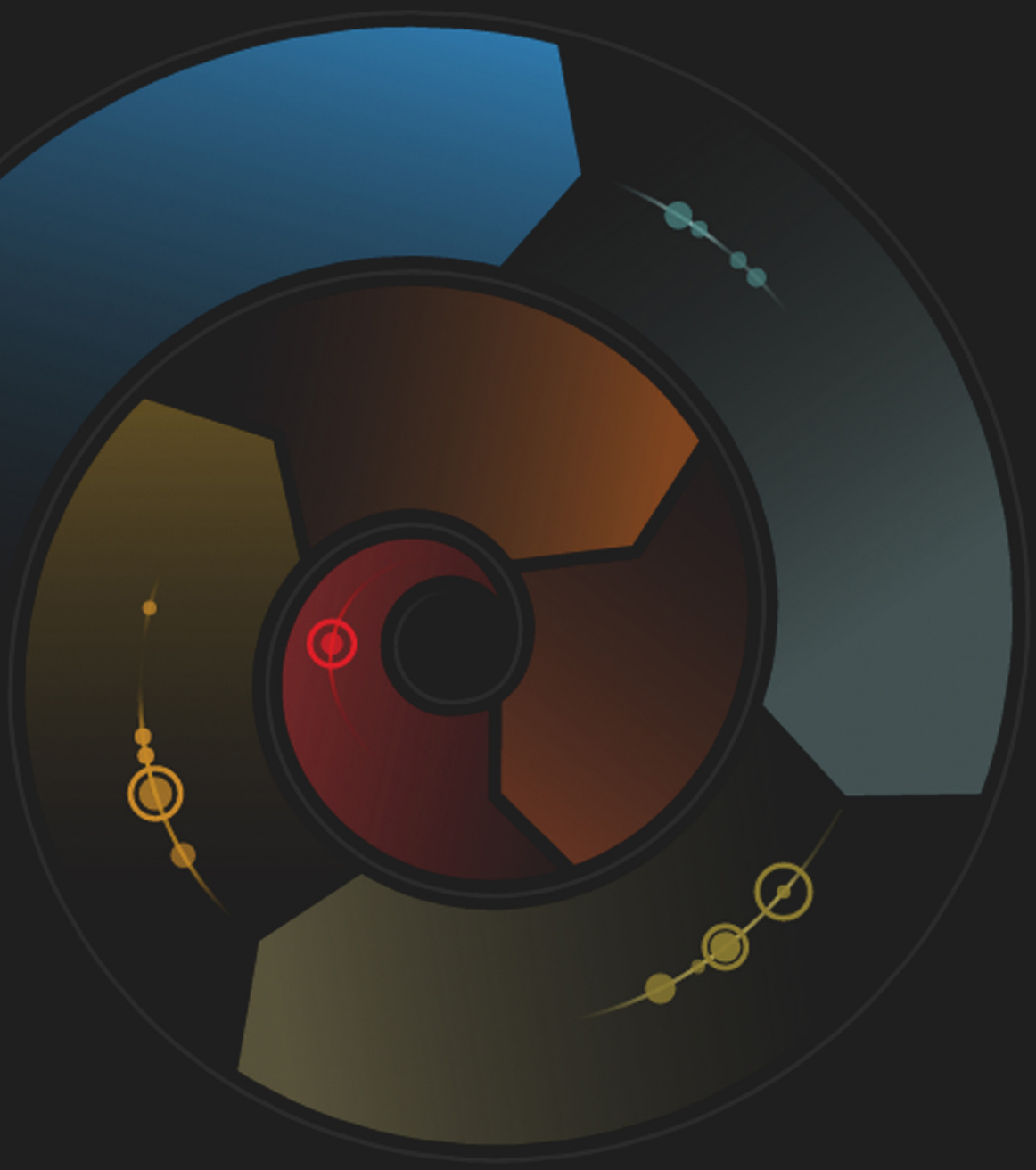
A CISO's Guide to Cloud Security

WHAT TO KNOW AND WHAT TO ASK BEFORE YOU BUY

A PROTECTWISE WHITEPAPER



It wasn't so long ago when the idea of moving your organization's workloads to the cloud was unthinkable. Today you'll find most organizations have a growing portion of their IT infrastructures in the cloud. In fact, Gartner estimates that by 2020 "cloud-first" and "cloud-only" will be standard corporate policies rather than exceptions[1], and a study by IDC says that by 2021 more than half of the typical enterprise IT infrastructures will be in the cloud[2].

This rapid migration presents a unique security challenge. New cloud workloads are spun up, expanded, moved, and torn down frequently, and traditional products for on-premises networks were never designed to secure these dynamic environments. Although some security vendors have attempted to "cloud wash[3]" their products they still can't provide the visibility into threat activity on cloud segments analysts need to be effective.

Finding security professionals is hard enough[4], but retaining them is an additional challenge. Tasking them with the mundaneness of making a web of disconnected legacy products, which offer varying levels of cloud support, work together will not set them or your organization up for success. A modern approach to security should allow security teams to focus on what they were hired to do: investigate and hunt for any attacks threatening cloud workloads.

And while the need to secure cloud workloads may be your primary motivation for evaluating alternative approaches, not all organizations are making the same progress in their migrations to the cloud. Therefore, any evaluation must also consider the security of hybrid environments during the transition.

This guide provides some important considerations to keep in mind when investigating a cloud security platform that can address today's realities and tomorrow's cloud-first or cloud-only end goals.

[1] http://www.gartner.com/newsroom/id/3354117

[2] http://chartchannel.icharts.net/chartchannel/worldwide-cloud-it-infrastructure-market-forecast-deployment-type-2015-2021-shares-0

[3] Cloud wash (v.) An intentional and misleading attempt to rebrand, refresh, or repurpose legacy security products for use in cloud environments, usually with less robust feature sets, diminishing their overall value.

[4] http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html

STEP 1: ASSESS YOUR SITUATION

Enterprises can't move to the cloud quickly enough. That's a big problem for security professionals stuck relying on a hodge-podge of disparate, disconnected security products that were never architected to provide security in cloud environments. Formulating a strategy to secure your network depends largely on where your organization stands in its migration to the cloud.

WHERE ARE YOU IN THE PROCESS OF MIGRATING WORKLOADS TO THE CLOUD?

If your organization is still working on moving workloads to the cloud, it's not alone. A recent Forrester Research report reveals only about 28% of enterprise infrastructure decision makers in North America and Europe have adopted public cloud services, and 44% are actively building private clouds[5].

Some organizations may have no plans to migrate entirely to the cloud, since it's also the case that not one size fits all. Depending on your organization's size, office locations, or even its industry, it may make sense to move some workloads to the cloud while maintaining on-premises hardware and servers.

Whether you're in transition or if you're planning to maintain both cloud and on-premises workloads, you'll need to address unique security concerns when managing hybrid environments.

- Will the product you're evaluating provide visibility for heterogeneous enterprise and cloud environments?
- Can it unify management and threat detection for these disparate networks?

HAVE YOU TRANSITIONED TO A CLOUD-FIRST OR CLOUD-ONLY STRATEGY?

Forward-thinking CISOs and a mind-blowing drop in costs have driven many organizations to adopt a cloud-first or cloud-only infrastructure strategy. In fact, by 2020 about 92% of workloads will be processed by cloud service providers. More than two thirds (68%) of these workloads there will be in public cloud services while the remaining 32% will be in private clouds[6].

If your organization's workloads have already made it to the cloud then congratulations, but don't start celebrating just yet. One of the toughest challenges to keeping workloads secure in the public cloud is visibility. That's because while for all intents and purposes, the instance you lease from AWS, Google, or Microsoft is yours, it isn't.

[5] https://go.forrester.com/wp-content/uploads/Predictions-2017-Customer-Obsessed-Enterprises-Launch-Clouds-Second-Decade.pdf

[6] https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf

Few bleeding-edge security products, and certainly fewer legacy security products, can provide visibility into the cloud. For most organizations, the best legacy security products will allow you to tap network activity from the enterprise perimeter to the cloud, but no further. Without a solution designed with this limitation in mind, what happens in your cloud stays in their cloud.

- Does the product you're evaluating enable visibility for public cloud network segments you don't own by providing it as a service in the cloud instance?
- Is it capable of scaling automatically as cloud instances are spun up, grow, or are taken down?

IS NOW THE RIGHT TIME TO MAKE A CHANGE, AND IF SO, ARE YOU READY?

Change is inevitable, and sometimes it's painful when those changes affect the technology you've spent hours researching and hard dollars acquiring. Network technology is no different, so cloud security platforms you implement must be designed in a way that meets your needs today and will continue to do so in the future.

- Will the cloud security product you're evaluating be flexible enough to work with new technologies you may implement later?
- Is it extensible to other security products you have today, or that you may implement later, so that it can continue providing value?

STEP 2: DEFINE YOUR REQUIREMENTS

During every routine infrastructure project, it makes sense to ensure your business objectives aren't fuzzy and that your stakeholders are all in sync. Evaluating a Cloud security platform is no different, so be sure you've considered the requirements for an effective platform.

- Is the cloud security platform you're considering **scalable and elastic**? Will it be able to grow as storage and compute as needs change over time?
- Will it be **extensible**? Does its vendor provide a set of open APIs that allows exporting of analysis from within the platform to other products in your security stack? And can it accept data and analysis from those products to provide additional context?
- Does it help **automate** routine or mundane security tasks, thereby freeing up analyst's time so they can hunt for threats proactively?
- Is it **intelligent** enough to provide analysts and threat hunters with contextual, **actionable information**, or does it only supply flat charts and graphs?
- Will it be capable of pinpointing threats **proactively**, and can it take the analysis it's already performed and then perform it again **retrospectively** using the latest threat intelligence to discover previously unknown threats?
- Is the product **easy to use**? Was it designed to help busy analysts get more done in less time? Can it enable them to pivot effortlessly between endless points of threat data?

STEP 3: IDENTIFY YOUR USE CASES

The security stack your organization has built over some years can't handle the needs of today's cloud-oriented enterprise. That's not to say that these products don't or can't continue to provide value to your business, but the legacy, appliance-based security products enterprises have relied on for years simply weren't designed to secure the cloud. And "cloud-washed" versions of their predecessors lack the robust features needed and the visibility required to secure workloads in the cloud.

A modern and comprehensive approach to cloud security shouldn't be simply to add another product to your stack. Rather, you should look for ones that provide coverage for more than just one use case, and should be capable of working with the products you already have so that your entire security infrastructure can work better together.

Let's look at some of those use cases, how legacy security products no longer help where workloads have moved to the cloud, and some important questions to ask when evaluating a cloud security platform.

INTRUSION DETECTION

Traditional Intrusion Detection Systems (IDS) are not effective in the modern network since the modern enterprise isn't longer limited to traditional on-premises networks. It now includes public cloud environments and, for some companies, industrial environments. Additionally, attacks have increased in sophistication. It's becoming more common that attacks unfold over longer periods of time which makes them harder to detect, and new attack techniques are constantly being developed that can't be identified by signatures and rules alone.

A recent survey conducted by the cloud Security Alliance reveals the average enterprise using cloud services generated over 2.7 billion (yes, billion, with a "B") events. A tiny fraction—only 2,542 of those on average—were out of the ordinary. Of those, just 23 were found to be actual threats. Unsurprisingly 32% of the respondents said they just ignored alerts altogether[7].

Further complicating incident investigation and response with legacy detection technology is a lack of enough information about an event to determine its severity or its impact on the business. Legacy IDS products capture only the packets associated with a rule being triggered and so they are unable to provide information about what came before and what came after, which is vital if you're trying to paint a complete picture.

[7] https://www.scmagazine.com/crying-wolf-combatting-cybersecurity-alert-fatigue/article/667677/

- Does the product you're considering use advanced techniques like machine learning, custom threat intel, cross-customer analysis, and automated retrospective analysis complement signatures and rules to reduce false positives?
- Can it distill thousands of alarms down and prioritize them for rapid investigations with one-click access to full-packet capture data?
- Will it provide investigators with a full history of a breach, including not just the PCAP that triggered an event?
- Is it capable of correlating suspicious activity with security events found by other products in your stack for context that explains why an event was generated?
- Does it provide pervasive visibility on any network segment, including those not owned by the organization, such as the public cloud?

SECURITY ANALYTICS

There's no shortage of security analytics products out there, but enterprises are quickly realizing they aren't meeting their needs. Exorbitant costs for hardware and maintenance make it impractical to retain forensics for periods longer than the typical breach window, making it impossible to identify what information left the enterprise. These products are notoriously difficult to deploy, configure, and support which has also slowed their adoption.

Legacy security analytics products also weren't designed to move with workloads to the cloud. They can't maintain long term state long enough to present analysts with a picture of the entire attack. That leaves them incapable of adapting to new attack techniques or causes them to generate excessive false alarms which make analysts jobs more difficult. For short staffed security teams, who are already suffering from alert fatigue, additional warning bells that require significant investigative efforts to resolve would simply slip into the noise and result in the attack being missed.

- Can the cloud security platform you're evaluating make information and analysis available on-demand for more effective forensic investigation and incident[8] response?
- Can it visualize millions of datapoints in a way that makes it easier for analysts to tease out not-yet-identified attacks buried in massive amounts of data?
- Does it provide sophisticated analytics that deliver reliable data analysis for any network, whether it's a traditional enterprise network, cloud network or industrial control operational technology?
- Does it take a data science approach detection by training machine learning models with billions of attributes?
- Are integration points available to infuse analysis with data from other products in the security stack for better context about events and observations?

[8] Security incident: An event that violates an organization's security or privacy policies involving sensitive information such as social security numbers or confidential medical information.

INCIDENT RESPONSE

A recent SANS survey reported that 87% of respondents reported at least one security event in the last year, but a whopping 20% of those reported responding to at least 100 security events[9]. That number is particularly concerning if you factor in the scarcity of well-trained security talent to investigate and respond to those incidents. Keeping your organization's network secure depends on talent and technology that can help improve visibility across your network to help reduce attack dwell time.

- Can the cloud security platform you're evaluating provide pervasive visibility from the network to the endpoint for investigations that are free from blind spots?
- Does it provide an unlimited full-fidelity forensic window correlated with data from complementary security products?
- Does it include a robust feature set, and can it work with the products in your existing security stack to help shorten the detection-investigation-resolution workflow?

THREAT HUNTING

Discovering malicious activity in your network goes well beyond the real-time detection of indicators of compromise. The reality is that cyber attacks can frequently occur under the radar, and you don't always know they've happened until the damage is done. That makes threat hunting, or the process of proactively searching out evidence of malicious activity, a critical function for any organization with sensitive data or resources—which is just about every organization. Hunting down new or unknown threats on your network today is especially challenging. Your team needs to be equipped with the right data and techniques to sift out suspicious activity from seemingly normal behavior.

- Can the cloud security platform you're evaluating capture full-fidelity PCAP and store it in the cloud indefinitely to give threat hunters access to data for periods of time that exceed breach windows?
- Can it build a unified, highly contextual, and easily accessible haystack that provides threat hunters with the depth of information they need to test their hypotheses?
- Is it capable of high-speed, on-demand analysis so threat hunters can build and test complex searches of thousands of attributes quickly, even across massive sets of data?
- Does it visualize in a way that provides threat hunters instant access to infinite points of data without having to pivot between multiple user interfaces?

[9] https://www.sans.org/reading-room/whitepapers/incident/show-on-2017-incident-response-survey-37815

STEP 4: DETERMINE METRICS FOR SUCCESS

Executives love a dashboard, and at some point in the life of your cloud security platform, someone will ask for quantifiable evidence that it's making a positive impact. Every business is different, but a few actionable metrics you may want to consider include:

REDUCTION OF FALSE ALARMS

The number of false alarms that can distract busy analysts from their core mission of protecting your business is staggering. In fact, over a third of banks receive over 200,000 alerts per day[10]. That's way more than any human being can handle. the cloud security products you evaluate should:

- Use advanced analysis techniques and machine learning models to reduce false alarms so analysts can focus on the security events that matter most.
- Prioritize alerts based on the severity of their impact on your business.

IMPROVED THREAT DETECTION

Threat detection has long been a stalwart product in every enterprise security stack. However, technologies that teams relied on as little as a few years ago haven't adapted to today's sophisticated threats which can evolve over long periods of time. To help improve the efficacy of these products, many organizations, especially those with large threat teams, may develop highly-tailored, proprietary intelligence, which should also be a consideration during your cloud security buyer's journey. the cloud security products you evaluate should:

- Use custom threat intel and cross-customer analysis of threats to complement commercial signatures and rules.
- Be able to use threat intel sources that capture the uniqueness of your organization's network based on its industry and other factors.
- Correlate suspicious activity with security events for context that helps explain why an event was generated.

REDUCED TIME TO RESOLUTION

It can take just seconds to get compromised[11], but weeks or months for security analysts to realize something's gone wrong, and even longer to complete a full investigation. the cloud security products you evaluate should:

- Enable efficient end-to-end incident response, which means making sure multiple solutions can work together.
- Integrate with other products in your security stack to help automate repeatable processes so security teams can be more efficient so they can spend less time responding to meaningless alarms and more time identifying and stopping attacks.

[10] https://www.americanbanker.com/news/alert-there-are-too-many-cybersecurity-alerts

[11] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

DECREASED DEPLOYMENT TIME

If it takes days, weeks, or months to deploy a cloud security platform, it's taking far too long. Products that are built in the cloud and designed to work with the cloud should be up and running in hours, if not minutes. the cloud security products you evaluate should:

- Be architected specifically for the cloud, making deployment easier and faster not just for itself, but also to help speed deployment of other cloud products securely.
- Be flexible and scalable enough to handle any new cloud-based products you add to your IT infrastructure.

INCREASED NETWORK COVERAGE

Perimeter security products provide no visibility into threat activity within an organization, and when workloads move to the cloud, enterprises are left completely blind because appliance-based solutions require architectural changes and often can't be used in a public cloud. the cloud security products you evaluate should:

- Centralize threat management for your network core, perimeter, owned and unowned cloud assets, and, for some industries, industrial control systems.
- Have the ability to collect and analyze information from any ingress or egress point on your network, no matter where the network segment lives.

REDUCTION IN ATTACK DWELL TIME

Breaches are sometimes inevitable, and when a vulnerability is exposed on your network, it's the attacker's job to stay there for as long as possible. the cloud security products you evaluate should:

- Continuously evaluate historical network traffic and packet data against the latest threat intelligence, enabling security teams to discover threats that were missed previously.
- Use analysis of threats discovered in the past to help inform predictive discovery of security threats in the future.

STEP 5: EVALUATE YOUR OPTIONS

Use the table on the following page to evaluate two solutions. Provide 1 point for each question that can be answered with a "Yes". Total the points for each solution and use that in your decision making.

REQUIREMENT	SOLUTION 1		SOLUTION 2	
DOES THE PRODUCT YOU'RE EVALUATING PROVIDE	**YES**	**NO**	**YES**	**NO**
1. PERVASIVE VISIBILITY?				
Collects and analyzes information from any ingress or egress point on your network.	○	○	○	○
Centralizes threat management for your entire enterprise network?	○	○	○	○
Supports heterogeneous networks including enterprise, cloud, and industrial controls.	○	○	○	○
2. AUTOMATED THREAT DETECTION?				
Uses advanced analysis techniques and machine learning models to help reduce fatigue from false alarms.	○	○	○	○
Uses custom threat intel and cross-customer analysis to complement signatures and rules.	○	○	○	○
Correlates suspicious activity with security events for greater context.	○	○	○	○
Prioritizes alerts based on severity of impact on your business.	○	○	○	○
Evaluates historical network traffic and packet data continuously against the latest threat intelligence.	○	○	○	○
Uses analysis of threats to help inform predictive discovery of future threats.	○	○	○	○
3. UNLIMITED FORENSIC EXPLORATION?				
Captures high-fidelity packets for extended periods of time.	○	○	○	○
Integrates with other security products to provide highly-contextual information about events.	○	○	○	○
4. FRICTIONLESS DEPLOYMENT AND SCALABILITY?				
Speeds deployment of cloud products by providing cloud-native security.	○	○	○	○
Scales and adapts to handle new cloud-based products.	○	○	○	○

CONCLUSION

If you've read this far, the time is probably right for your organization to consider a cloud security platform. Although cyber security for cloud workloads is a technological gray area for many enterprises, it doesn't have to be, if you keep in mind today's enterprise security realities:

- Traditional appliance-based security products won't work in cloud environments because they can't provide coverage beyond the network perimeter.
- Cloud-washed versions of these products offer poor visibility into cloud instances, and they rarely have the robust feature sets needed to be effective.
- Security point products offer questionable value to an already crowded security stack.

As you move ahead in your evaluation of solutions that can secure workloads in the cloud, remember to map out your use cases, requirements, and must-have features. Then formulate your metrics for success so you can be sure you're meeting the expectations of your executives.

About ProtectWise

ProtectWise™ is disrupting the security industry with The ProtectWise Grid™, its enterprise security platform that captures high fidelity network traffic, creates a lasting memory for the network, and delivers real time and retrospective alerting and analysis in a rich, innovative visualizer. By harnessing the power of the cloud, The ProtectWise Grid provides an integrated solution with complete detection and visibility of enterprise threats and accelerated incident response. The ProtectWise Grid delivers unique advantages over current network security solutions, including an unlimited retention window with full-fidelity forensic capacity, the industry's only automated smart retrospection, advanced security visualization, and the ease and cost-savings of an on-demand deployment model. For more information, visit www.protectwise.com.

20170831

PROTECTWISE™

1601 WEWATTA ST • SUITE 700 • DENVER, CO 80202 • 1.303.625.6802
WWW.PROTECTWISE.COM • INFO@PROTECTWISE.COM