



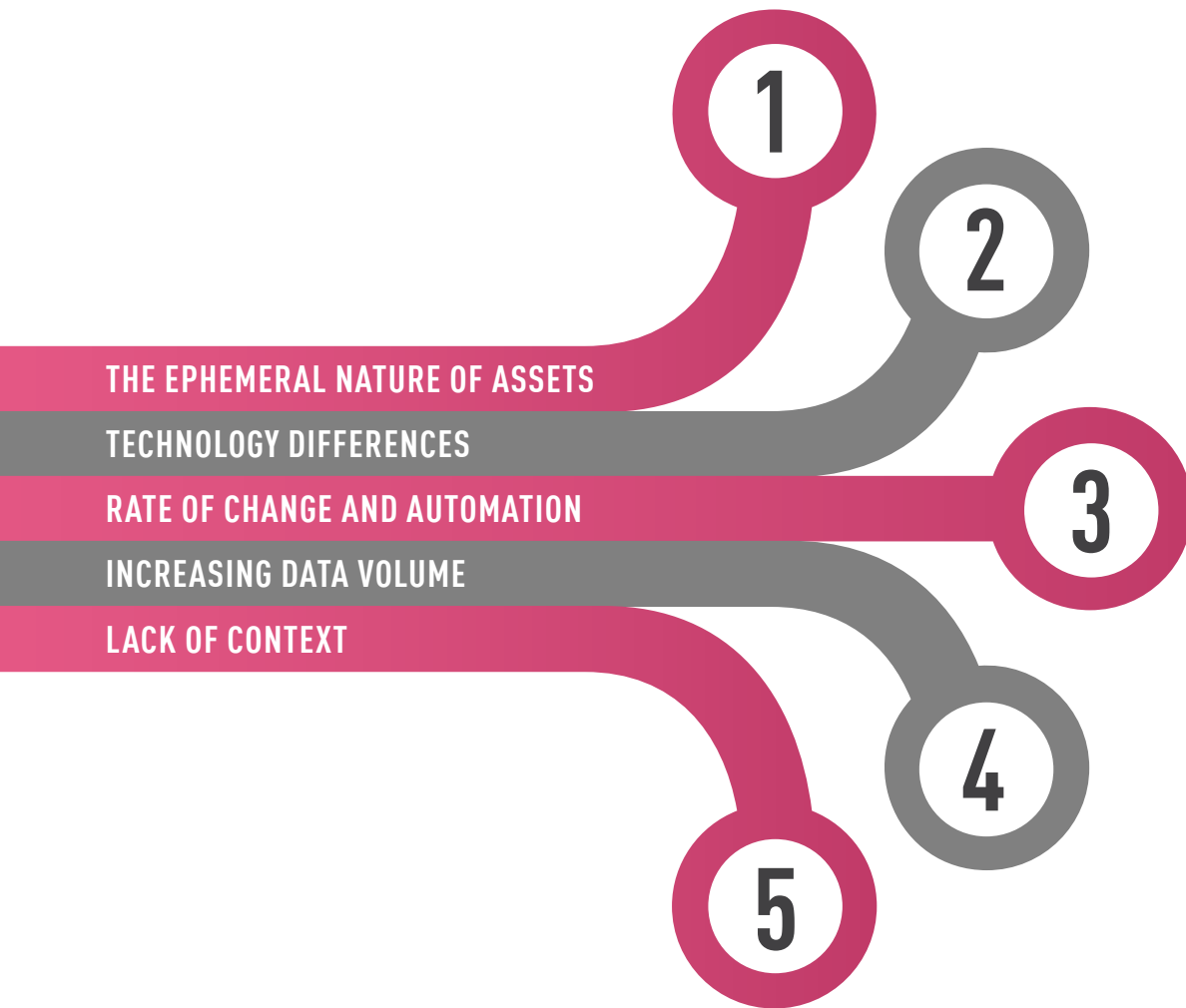
TOP 5 CHALLENGES AND RECOMMENDATIONS FOR **CLOUD MONITORING**

The transition to cloud-based applications appears unstoppable. However running applications on cloud platforms such as Amazon Web Services or Microsoft Azure creates a number of security challenges not in seen on-premises deployments.

This whitepaper will review some of the challenges that create issues with capturing and leveraging log data, followed by several recommendations for coping with them. Achieving viable security for cloud-based applications is impossible if you don't know what you're up against.

THE CHALLENGES OF LOGGING IN CLOUD BASED ARCHITECTURES

The most fundamental activity for securing monitoring and response is the collection and analysis of log data. Every compliance regulation requires this activity in some form, and for good reason. Therefore any organization moving to the cloud needs to understand how the environment will change with respect to logging. While a truly exhaustive description of all the aspects of cloud architectures that affect security event logging, processing, and response is beyond the scope of this whitepaper, there are a more manageable number of challenges that are both highly impactful and ubiquitous. These are described below. Note that the relative priority of these issues will vary with the environment and over time, but all are likely to come up at some point.



1 THE EPHEMERAL NATURE OF ASSETS

On-premises infrastructure and applications are relatively static: Internal IP addresses and ports, DNS entries, VLAN assignments, and persistent operating systems all tend to be configured and then rarely changed. In fact, most IT shops avoid changes whenever possible, fearing that a seemingly minor change (e.g. re-addressing a subnet) might cause an outage, for example by breaking a script everyone had forgotten about. This makes it easy to use these static definitions for security, for example in firewall rule tables or log correlation to critical assets.

However cloud deployments are all about flexibility and agility: objects come and go by design, and in some cases are deliberately failed periodically to test resiliency. Virtually nothing is static. So it's impossible to base security constructs on static object definitions.

2 TECHNOLOGY DIFFERENCES

Certain constructs in on-premises IT infrastructure play a crucial role for security insertion and log extraction. Examples include

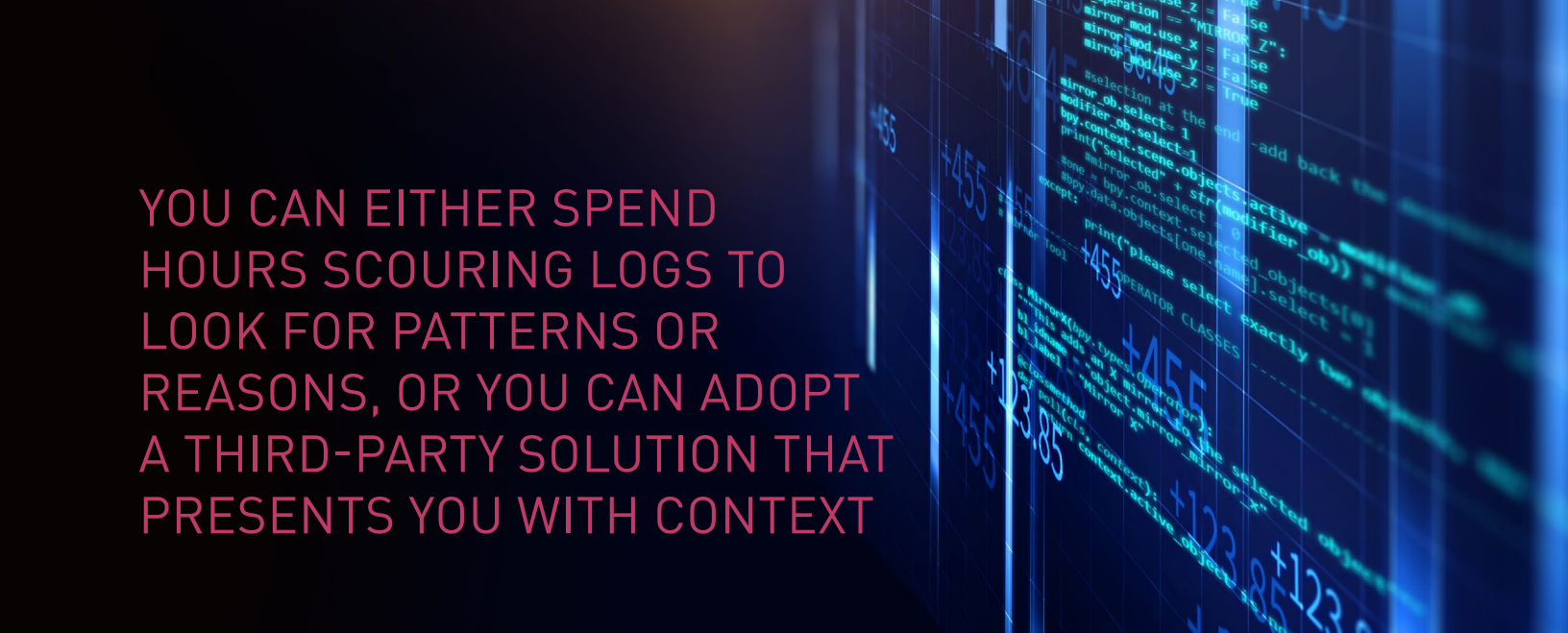
- Network insertion via transparent bridging;
- SPAN port monitoring;
- Agents deployed within a limited set of approved operating systems or at the virtualization layer;

In the cloud, many of these constructs either don't exist, or are expensive to deploy, making it difficult to implement event generation without major architectural changes.

3 RATE OF CHANGE AND AUTOMATION

We've already noted that cloud assets are ephemeral. But the highly changeable nature of the cloud runs deeper than that. In particular, the applications themselves change rapidly. Unlike on-premises apps which might be updated a couple times a year in a waterfall process, cloud apps can change daily. This makes it hard to model them, which makes it hard to differentiate normal application behavior from activity driven by adversaries. In addition, the process of change is highly automated, meaning that it isn't viable to insert human-driven control points in the development process.

CLOUD DEPLOYMENTS ARE ALL ABOUT FLEXIBILITY AND AGILITY, ..IT'S IMPOSSIBLE TO BASE SECURITY CONSTRUCTS ON STATIC OBJECT DEFINITIONS



YOU CAN EITHER SPEND HOURS SCOURING LOGS TO LOOK FOR PATTERNS OR REASONS, OR YOU CAN ADOPT A THIRD-PARTY SOLUTION THAT PRESENTS YOU WITH CONTEXT

4 INCREASING DATA VOLUME

The volume of data in motion in cloud architectures is usually much larger than in traditional data centers. This creates a scaling problem: A security methodology that works on-premises may not work in the cloud because it can't scale. This is particularly true if humans are involved, because security staffing hasn't kept up with the increase in responsibilities associated with securing a hybrid, multi-cloud environment.

5 LACK OF CONTEXT

Spikes in traffic can happen for a lot of reasons. Even after fine-tuning your cloud infrastructure system, public cloud solutions can be frustratingly vague. You can either spend hours scouring logs to look for patterns or reasons, or you can adopt a third-party solution that presents you with context.

One example of this vagueness is the CloudWatch alert system in Amazon Web Services. CloudWatch alerts will send you an alert email that some condition was met, but the email often does not contain enough contextual information to make the alert truly actionable. You know that a threat was found, but what was it, and how should you respond. The answer requires additional digging to find out what caused the condition, and if it is actually of some concern.

One clear result of these issues has been a decrease in the efficacy of cloud native logging and SIEM solutions. These solutions play a critical role in security and compliance, but if the data they ingest can't be correlated with people, assets, and data, they are ineffective for risk management. This has always been a challenge, but the situation is much worse than it used to be, and in many hybrid cloud deployments these solutions have lost their viability for situational awareness and efficient incident response. This is a huge problem, as logs are the most important post-incident tool available.

RECOMMENDATIONS FOR VIABLE CLOUD MONITORING

Given all these challenges, what concrete steps can be taken to improve security logging in the cloud? Here are a few recommendations worthy of consideration.

Combine configuration data with real-time instrumentation

Because of the ephemeral nature of cloud assets, it's crucial to combine real-time configuration telemetry with log data. All cloud platforms support APIs for data mining the tenants' configuration, and this context is essential for enriching infrastructure log data (e.g. network flows) with application level information. The key is doing so in a way that is accurate over time, which isn't easy given the rate of change and possible concerns about exposing the (sensitive) configuration data.

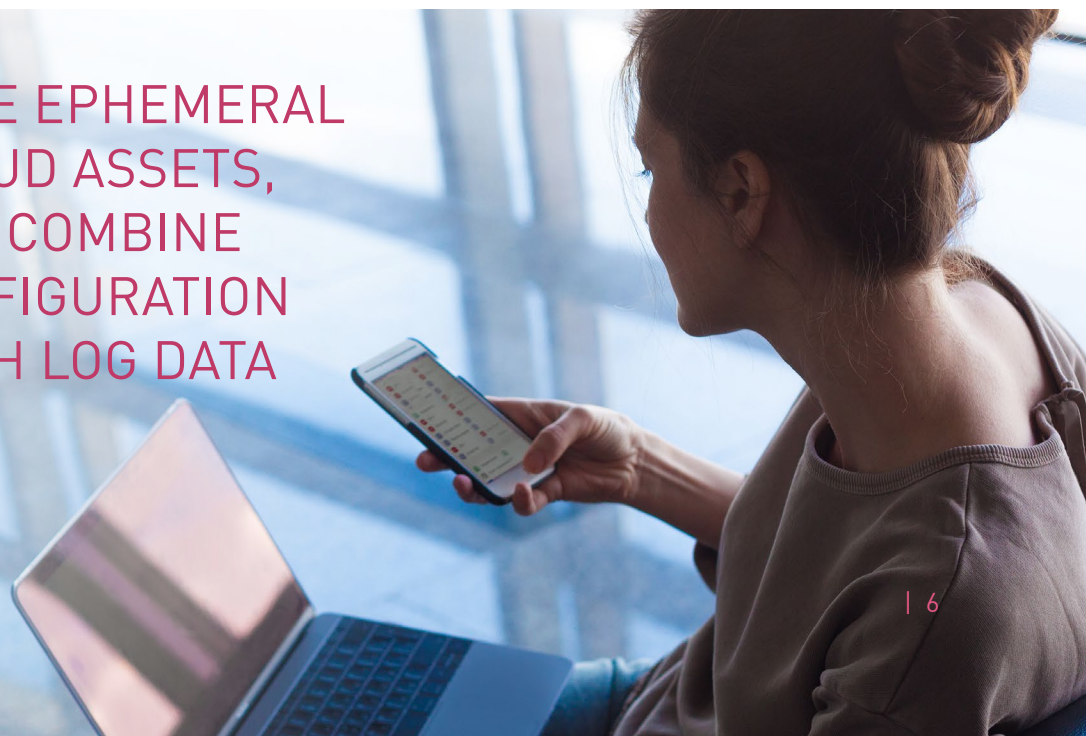
Use business context to prioritize security operations

Virtually all security teams struggle with prioritization: given a flood of alerts and anomalies, which ones should be addressed first? Simply mapping flows to applications isn't sufficient—what's crucial is knowing which applications are the most important. And since application roll-out in the cloud is more dynamic, this problem is generally harder. Therefore, IT Security should look to partner with application developers to embed at least minimal application metadata into the DevOps processes. This can then be used to improve the context included in log data to prioritize threat detection and incident response processes.

Use AI to model and scale

Given the vast amount of data created in the cloud, automation is mandatory to scale. With respect to threat detection and response, AI will play an increasingly important role. While far from a panacea, AI allows rapid baselining and anomaly detection based on log data with minimal staff requirements. This makes it an effective filter to keep the human workload manageable. But because algorithms are rapidly evolving, it's important to architect a strategy that supports experimentation.

BECAUSE OF THE EPHEMERAL
NATURE OF CLOUD ASSETS,
IT'S CRUCIAL TO COMBINE
REAL-TIME CONFIGURATION
TELEMETRY WITH LOG DATA



Decision Point: Multi-Cloud Consolidation vs Native Tools

All cloud platforms (e.g. AWS, Azure, GCP) are starting to offer security services, as cloud providers know that security concerns are a major inhibitor to cloud adoption. Because these services are offered by the platform vendor, they can have a high degree of integration with cloud infrastructure, and in some cases even with the applications themselves.

The challenge with native tools however is that they are proprietary to each cloud vendor, while most organizations are pursuing a hybrid, multi-cloud strategy. Therefore using native tools creates major issues with respect to policy consistency, and may inhibit workload agility, since it will be difficult to move an application's security policy transparently between platforms. This suggests that third-party offerings that support consistency and log normalization across the hybrid multi-cloud will bring significant benefits.

Log.ic for Cloud Security

Check Point is constantly seeking ways to better support organizations seeking to optimize their security and compliance needs. We are continuously adding new cloud security solutions to our portfolio to help solve the challenges discussed in this whitepaper. For example, our Log.ic offering is purpose-built to enrich cloud platform logs for security visibility, threat detection, incident response, and compliance. Log.ic was designed to address a number of the challenges outlined in this whitepaper in a scalable way across a multi-cloud environment.

Learn more about how Check Point Log.ic is Transforming Logs In to Logic, by delivering cloud intrusion detection, network traffic visualization and user activity analytics, to help your security operations team reduce incident response time from days, to hours and minutes:

checkpoint.com/products/public-cloud-security-analytics/