ACHIEVING CLOUD SECURITY CONFIDENCE IN THE AGE OF ADVANCED THREATS

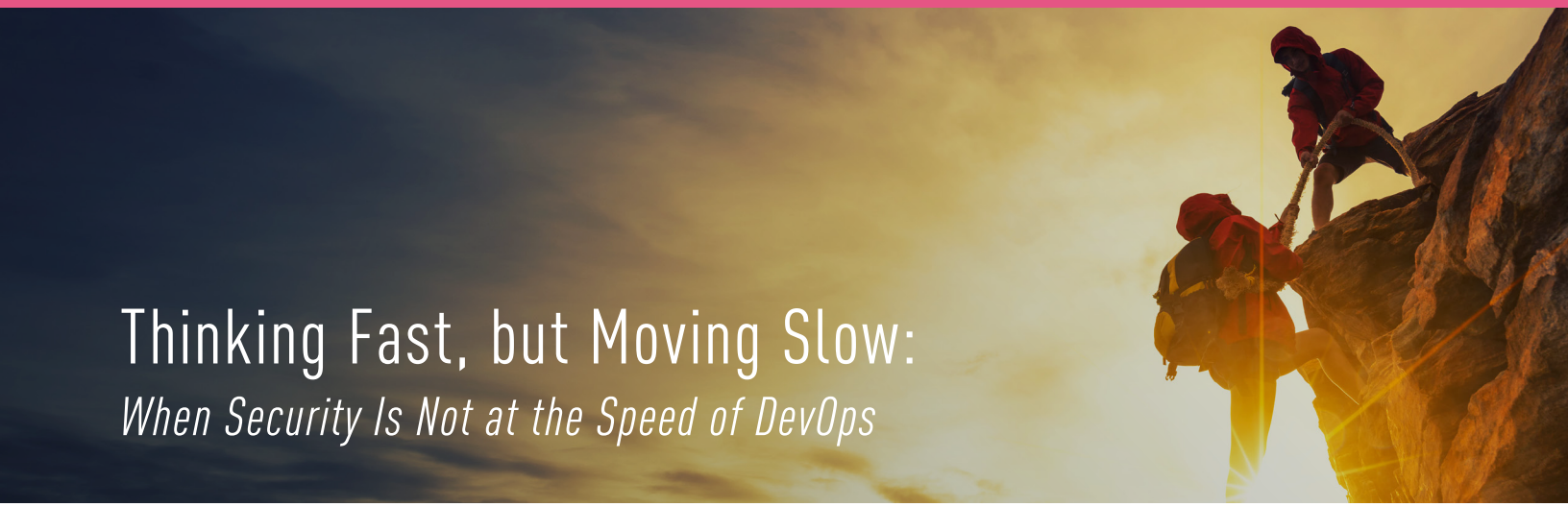
Executive Summary

Traditional desktop software and servers have been replaced by cloud computing tools. In recent years, with the advent of digital transformation, cloud computing has garnered massive momentum, and has reshaped enterprise IT as we know it. The ease and availability of the cloud provides businesses with dynamic options for developing and deploying services and applications at a fast pace. These advances drive business performance, but they've also resulted in security that just can't keep up.

Detecting threats after they have already made their way into a network means that it may be too late to avoid damage. In the age of highly targeted, advanced cyberattacks, threat prevention is a must. Optimizing threat prevention mechanisms so that they work non-stop, and can arrest attacks before they happen is critical for your continued business growth and long-term confidence in your cloud security architecture.

Enterprises routinely fall short in implementing cloud security that they can see, manage, and trust. Meeting cloud security goals may require rethinking and adapting to agile processes, reducing complexity, maximizing visibility, and automating compliance. Leveraging new, comprehensive tools can help address these challenges.

The following white paper offers robust insights into how you can achieve optimal cloud threat prevention and establish the best possible cloud security posture for your business.



Thinking Fast, but Moving Slow:

When Security Is Not at the Speed of DevOps

Conventional security measures are static; they cannot deploy the necessary automation or offer the continuous insights needed to instantly pin-point, monitor, and secure rapid changes within the cloud. The cloud is too dynamic to successfully integrate with conventional security. Because of this, each time there's a change in a cloud service or in application deployment requirements, there's a possibility of a new security risk. These risks include lack of data privacy, threats to applications themselves, and threats to API storage gateways. Here are some of the true dangers that come with these pitfalls:

Data Privacy: When sudden changes to cloud configurations take place in environments with conventional security structures, malicious insiders may suddenly have the opportunity for exfiltration of sensitive, personal identifiable information (PII) from cloud servers or storage. In 2019, a third-party app developed on a social media platform leaked 540 million records[1]. The developers had deployed to the cloud without reassessing their security measures, potentially causing problems for consumers. Cloud security must be as agile as the cloud itself.

Application Vulnerability: According to Forrester 90% of applications have codebases made up of open source material[2]. Whether proprietary or open source, unpatched software vulnerabilities are one of the biggest cyber threats organizations face, and unpatched open source only adds to that risk. Without agile security controls, cloud native development and deployment of unpatched application into the cloud introduces major risk for organizations..

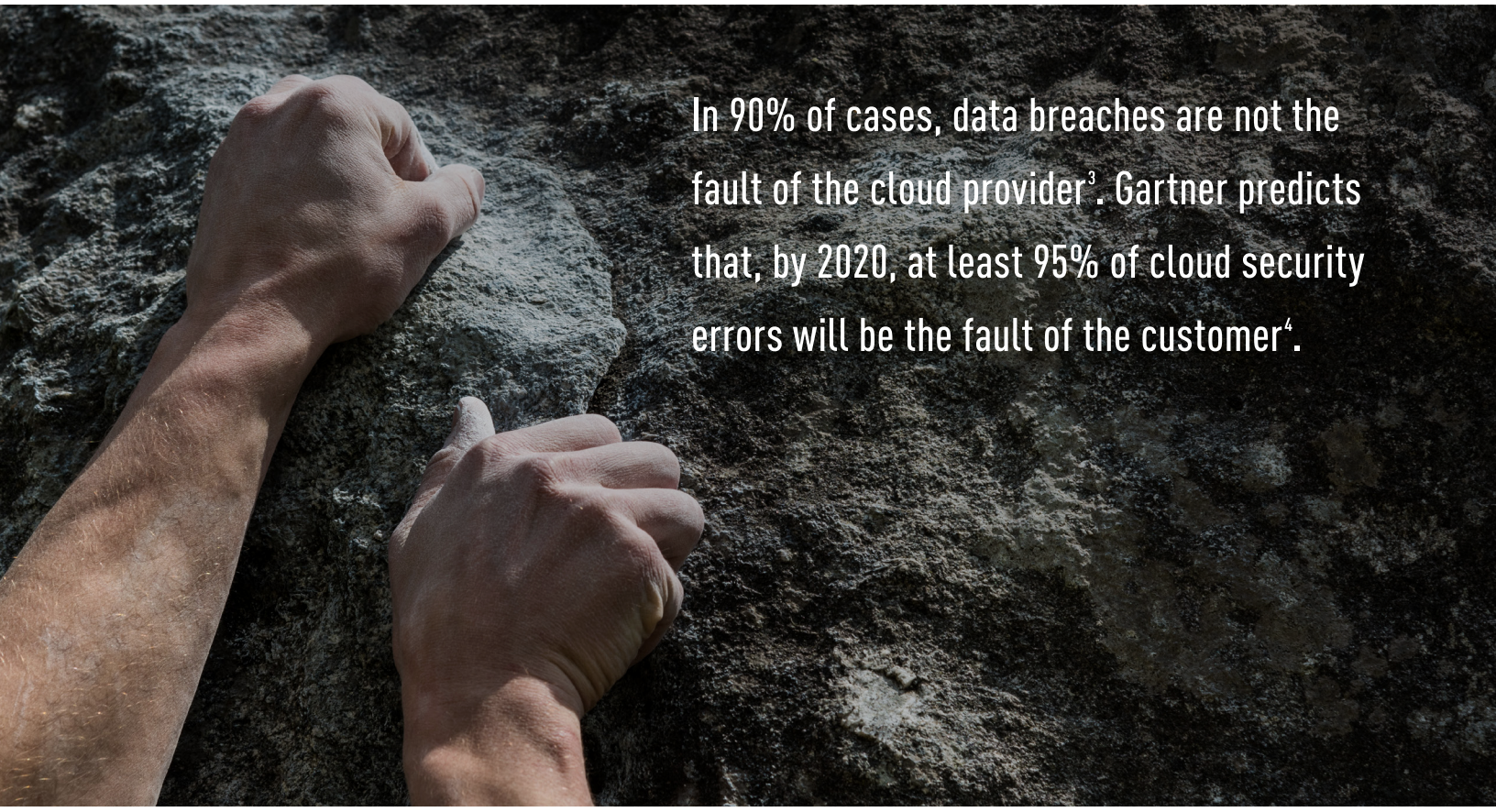
API: Similarly, abrupt changes to cloud configurations can also lead to API vulnerabilities. Should an attacker choose to steal a token for service access that belongs to a customer, the hacker can potentially manipulate a customer's data. Again, cloud security must be agile in order to be trustworthy.

[1] "Data on 540 Million...Exposed," BBC, April 4th, 2019

[2] "The Forrester Wave: Software Composition Analysis, Q1, 2017," February 23, 2017

The availability of cloud services and a workplace emphasis on agility means that DevOps teams often move at a breakneck speed, leaving security behind. Application developers and the supporting DevOps teams are constantly on tight deadlines to get the next so-called 'killer app' deployed. Due to the frequent, fast and furious push to develop, test, deploy, and iterate, security is often an afterthought. The DevOps team may create the right environment for application deployment, but DevSecOps must ensure that cloud security is firmly in place, and appropriately prevents large-scale threats. The more that organizations can 'Shift Left,' and identify vulnerabilities early, the greater the long-term payoff in terms of business outcomes.

As illustrated above, cloud security failures commonly occur due to human negligence or human error. When the DevOps team wants to move fast, but mature security configurations require a slower approach, employees may try to cut corners, causing integration issues and security flaws. In 90% of cases, data breaches are not the fault of the cloud provider[3]. Gartner predicts that, by 2020, at least 95% of cloud security errors will be the fault of the customer[4]. The desire for immediate corporate growth, and lack of forethought can stall or upend business objectives, resulting in costly breaches and fines. To develop and deploy frequently and securely requires investment in an equally agile and dynamic security solution.



[3] "90% of Data breaches are Caused by Human Error," Techradar.com, 2019

[4] "Is the Cloud Secure?," by Kasey Panetta, Gartner, March 27, 2018

Promise and Threat

The Multi-cloud Security Conundrum

Adopting a multi-cloud infrastructure offers businesses unprecedented advantages, ranging from the capacity to segregate private and public facing data, to the ability to select specific services from each vendor, to enhanced reliability. Although all of these advantages positively contribute to your prevention model, installation complexity can be the root cause of incorrect server configurations, and can directly contribute to data breaches.

When it comes to setting up and securing Amazon Web Services (AWS) servers for example, one expert aptly states that it's "not exactly like [following] Ikea instructions." Flaws in firewalls or improper encryption are known sources of extreme damage. Not only can a human misconfiguration slip in the multi-cloud create chaos, so too can mismanagement of the multi-cloud's many different components.

Within cloud computing, having many services, platforms, technologies and tools to deploy applications in the cloud can burden your security teams. This 'operational sprawl' adds to security complexity, and slows down processes. Within the multi-cloud environment, the management burden is compounded by incompatibility issues that arise as users move between clouds. The security services and controls in a Microsoft Azure cloud may not match the level of controls needed within an AWS cloud, or your on premise, or private clouds. Multi-cloud architectures with inconsistent controls can actually slow down your business rather than ramp it up.

Close the gaps in your multi-cloud security by standardizing security across all platforms using a comprehensive third party security solution. With one click deployment and rapid scalability, an automated solution can bring you the control you need to confidently own your businesses' day-to-day security posture.

[6] "Human Error Often the Culprit in Cloud Data Breaches," by James Rundle, The Wall Street Journal, August 27 2019

Maximizing Visibility

Deep Insights with Data Analytics

You cannot secure what you cannot see. The fast scale of cloud, log data, and elastic and dynamic nature of cloud makes it extraordinarily difficult for your security teams to see and understand what's going on. Seeing what's happening in your cloud reduces rates of incidents, and shortens incident response time.[6]

In the age of cloud security, SIEM solutions alone are largely ineffective. Cloud security solutions that integrates with your SIEM solutions to feed them enriched critical data can help you correlate event and log data. Because singular pieces of event and log data can be manipulated by cyber criminals, it's imperative to leverage active flow logs that offer insights across network infrastructure, and across extended lengths of time. Ensure that you capture detailed traffic information in order to identify patterns, and tightly track malicious activity.

The importance of clear visibility into data analytics cannot be overstated. Enhanced visibility translates to better monitoring and compliance, and better overall business outcomes. As the cloud has evolved through the introduction of new services and technologies, so has event logging. Today's cloud environments can track terabytes of log data per consumer. Trying to establish context and an understanding of these logs, especially during incident response, can be a challenge. Graphical relationship presentation of data seems to be the next shift in log presentations. As an example, since the inception of Amazon Web Services (AWS), AWS has provided the CloudTrail service as a means of logging events in the cloud. Recently, AWS has made an attempt towards graphical representation of these event through the introduction of services like Macie or Guard Duty, which provide enhanced visibility around logs and events in the cloud. It is important to recognize the need for investing in newer intuitive tools that provide enhanced cloud visibility.

The fast scale of cloud, log data, and elastic and dynamic nature of cloud makes it extraordinarily difficult for your security teams to see and understand what's going on.

[6] "You Can't Protect What you Can't See," by Phil Quade, CSO Online, February 19, 2019

The Compliance Cornerstone

The Final Foundational Element in Securing Your Infrastructure

Software engineers develop and/or deploy apps to the cloud as rapidly as possible, often every day or every few days. As much as 10% of the sensitive data in a typical enterprise is going to unsanctioned cloud-based applications[7]. This extends disquieting potential for DevSecOps teams to discover holes, open ports and misconfigurations that violate compliance protocols.

Compliance challenges can also arise due to lack of user authentication protocols. Assigning users access rights, and creating corresponding enforcement policies helps you identify anomalous behavior, and enforce compliance. When employed properly, and monitored correctly, access management can serve as a business enabler.

In 2019, a well-known banking institution that rapidly deployed to the cloud without confirming the viability of their security controls, encountered a serious insider threat. The criminal who extracted the data exposed millions of records. Such exploits by unauthorized persons can lead to significant, public repercussions

Encryption is another essential component of robust data security, and a best practice when it comes to maintaining the integrity of your systems. To augment compliance, data stored in the cloud should be encrypted by default. Be sure that you can receive alerts regarding any compliance violations that could increase your organization's level of risk. Ensure that there are no deviations from your corporate policies, and that legal compliance directives are continually met.

Continuous compliance pays off in that you'll avoid financial penalties. In the US, the Federal Trade Commission (FTC) can charge organizations with violating Section 5 of the FTC Act, which fines organizations for careless business practices, and deceptive behaviors. Fifty-two different cybersecurity-related bills across individual states also aim to protect consumers and to assign penalties to organizations for negligent security practices[8]. The state of California recently passed a new data privacy law due to take effect on January 1st, 2020, and broad federal mandates and penalties are in development phases within the US.

[7] "Managing multi cloud," by Myles S. Suer, CIO.com, March 11, 2019

[8] "Cybersecurity Legislation 2018", National Conference of State Legislators, February 2nd, 2019

[9] GDPR vs Australian Data Privacy Regulations: 5 Key Differences", Information Age, Nick Ismail, March 5th, 2018

[10] "Cybersecurity Legislation 2018", National Conference of State Legislators, February 2nd, 2019

The European Union is well on its way in this regard. The data privacy laws in Europe, as expressed through GDPR, are written into a compendium of 11 chapters and 99 articles[9]. In the UK, legislation now requires that companies guilty of inadequate data protection pay a penalty of up to €20 million euros, or 4% of global turnover, depending on the greater number[10]. The bottom line is that meeting compliance requirements helps you proactively enhance your threat prevention model, and can increase your confidence in the cloud.

Code Space Dissolves

The consequences of weak cloud security can be dramatic. In 2014, when a hacker gained access to Code Space's Amazon EC2 control panel, and exploited the network, which was hosted entirely on the cloud, the company faced a damaging DDoS attack. The company refused to pay the corollary ransom, and the hacker then destroyed all of Code Space's critical data, ultimately forcing the company to shut down.

Despite the fact that Code Space is ostensibly the victim in this circumstance, "many experts are in agreement that they share some of the blame," says CSO Online[11].

Within the shared responsibility model, CSOs and others in similar roles, must continually ask themselves, 'Am I doing enough to be confident in my security?'

In Conclusion

Maintaining confidence in your cloud security depends on the ability to keep pace with the agile nature of the cloud, the capacity to adequately protect a multi-cloud environment, visibility into rich data analytics capabilities, and upholding compliance and governance standards. By placing these elements at the core of your cloud security strategy, you'll build operational transparency and consistency that drives trust. Be secure. Stay secure. Grow securely.

If you're seeking a best-in-class cloud threat prevention solution, Check Point Software offers powerful, flexible, scalable, and comprehensive cloud security solutions designed to move your business forward. For more information about how to secure your cloud with confidence, visit the Check Point CloudGuard solutions website or reach out to your local Check Point representative.

[11] "Code Spaces Forced to Close its Doors After Security Incident," by Steve Ragan, CSO Online June 18 2014

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com