March 2021

SETTING THE FOUR CORNERSTONES OF CLOUD SECURITY

Accountability, Strategy, Visibility & Enablement

Sponsored by:

ARCTIC WOLF

CYBER SECURITY HUB

EXECUTIVE SUMMARY

Cloud migration led to cloud evolution which has led to a cloud-first mindset. With a pandemic push, global corporate enterprise has gravitated to the exponential perimeter. The four cornerstones of cloud security now must be realized:

ACCOUNTABILITY:
With a hat-tip to the RACI matrix, identifying responsibility

STRATEGY:
Envisioning a cloud security roadmap moving forward

VISIBILITY:
Brining an entirely secure enterprise back into focus

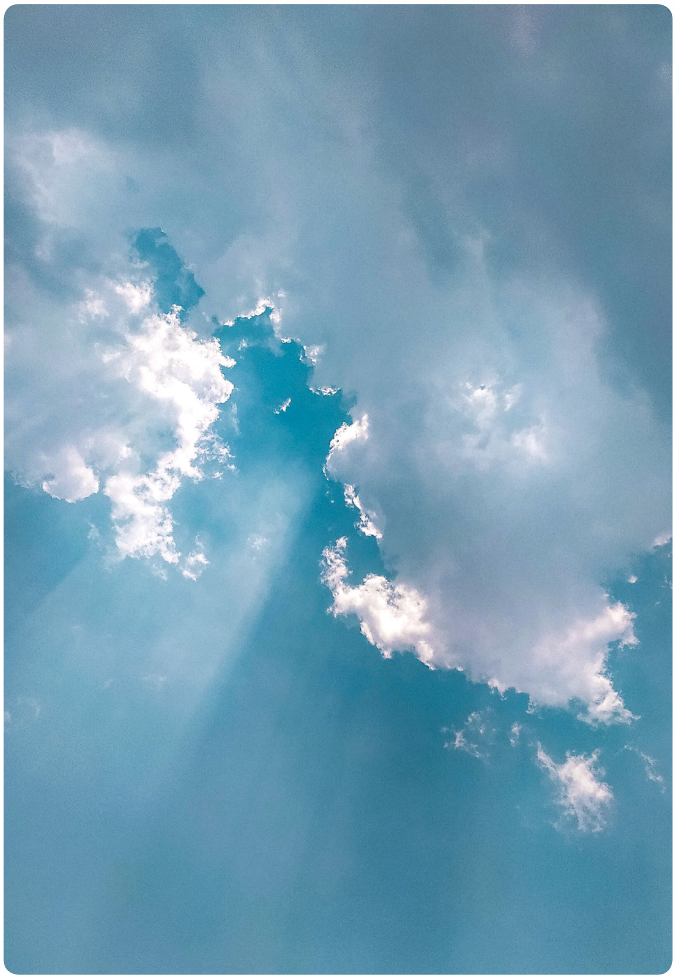
ENABLEMENT:
Outpacing innovation on the edge to ensure continuous business enablement

Beginning with the end in mind, organizations of course have the goal of continued secure business enablement. To ensure a secure infrastructure, visibility must be apparent. To ensure visibility- a cloud infrastructure strategy must be in place. And to ensure a strategy is in place, accountability for the initiative must be clear.

Security accountability, of course, is the responsibility of the CISO. Infrastructure Complexity, Unique Vulnerabilities, User Access, Data Security, Consistent Application Controls, Inconsistent Talent and Regulatory Compliance are just some of the gargantuan pressing issues which must be addressed in cloud security and covered in this report.

And addressing those pressing issues are the initial steps needed in setting the four cornerstones of cloud security.

TABLE OF CONTENTS



ACCOUNTABILITY

The RACI Matrix does a good job of providing clarity on accountability. RACI stands for Responsible, Accountable, Consulted and Informed. Several people can be Responsible, Consulted and Informed, but only one person is Accountable. While the CISO (Chief Information Security Officer) must be Responsible, Consulted and Informed, there is a question as to whether that is the optimal job function to be Accountable for the entire cloud infrastructure at any given organization. The CIO, CRO and COO have all been suggested as appropriate executives to take the role of Accountability for the entire cloud infrastructure.

The CISO is accustomed to restricting access to ensure security. Cloud security solutions are traditionally discussed via Infrastructure-As-A-Service (IaaS), Software-As-A-Service (SaaS) and Platform-As-A-Service (PaaS). The concept of anything "as a service" is a key to why the CISO has had to move from running the Department of No to running the Department of Know. The value of cloud-based services resides in high availability. Thus allowing for business enablement demands the acceptance of new risk.

"Understanding the shared responsibility model with each SaaS and IaaS vendor is essential for organizations to effectively mitigate risks, as while cloud vendors assume some responsibilities, they do not assume all risks on behalf of their customers."

KAYNE MCGLADREY

Cyber Security Hub Executive Advisory Board

"It depends on your risk appetite" is a missive often offered in response to cloud security questions. But while most Boards, CEOs and business stakeholders feel that they have a risk appetite which equates to operating at the pace of change, an incident which makes 'the front page' is unacceptable.

"Having a single point of accountability in highly distributed organizations is challenging unless a governance program establishes the concepts of system, data, and service/functional ownership. Cloud service is simply using someone else's data center. The CISO is accountable for cloud security – with the (business) functional owner of the data/service used in that data center being accountable for having the right service at the right cost and delivered at the right time."

BOB TURNER

CISO, University of Wisconsin-Madison

Operating at the pace of change means operating in the cloud. Thus enabling the business to operate in the cloud with a security consciousness is the responsibility for which the CISO is accountable. To execute that responsibility, the CISO must ensure that they are consulted and informed in real time of the machinations of operating in the cloud.

STRATEGY

The CISO must conceive of a cloud security strategy to ensure that the business consults and informs the cyber security operation. There are three different aspects of cloud security which need to be accounted for in that strategy:

- Security of the Cloud
- Security while accessing the Cloud
- Security of the applications and data in the cloud

**It could be argued that a fourth area could be cloud lifecycle management*

SECURITY OF THE CLOUD

Unfortunately, the security of the Cloud depends on the cloud provider. Most global organizations have some combination of Azure, AWS, Google Cloud, Alibaba Cloud, IBM Cloud, Oracle Cloud and/or Tencent Cloud. When one of those organizations is compromised, any organization utilizing the exposed provider must be able to detect the incident and remediate accordingly.

That leaves security while accessing the cloud and security of the applications and data in the cloud.

SECURITY WHILE ACCESSING THE CLOUD

Secure access occurs with identity as the perimeter. PAM, IAM, Zero Trust, SASE; most organizations have implemented at least one piece of the secure access quadrigeminal. Evolving to a security architecture which utilizes Identity as it's centrifugal force has become mandatory.

Consistent Cyber Security Hub surveys showcased that investments in this area topped budget expenditures for the past few years. And at the end of last year, we noted that 20% had at least taken one step on the zero trust journey- putting ZTNA on the plateau of productivity on the famed Gartner Hype Cycle.

While it might be an aberration, feedback over the past few months is that secure access is no longer a top investment area. There are inevitable trailing costs for any solution, but the shift in investment could mean that global corporate enterprise is perhaps level-setting on security while accessing the cloud. But with that security coming through newly sourced solutions, it must be verified.

SECURITY OF APPLICATIONS AND DATA IN THE CLOUD

The glaring action items of cloud security are clearly in the security of applications and data in the cloud.

Infrastructure Complexity

Some assets remain on-prem while some assets have been positioned in the cloud. To date, a lift and shift mindset dovetailing into a pandemic-inspired collaborative tool explosion have ensured that any given global corporate enterprise suffers from cloud infrastructure complexity.

Unique Vulnerabilities

Simply migrating to the cloud opens up unique vulnerabilities. But it is cloud infrastructure complexity which obfuscates visibility and metastasizes threat opportunities.

Data Security

Identity as the perimeter does help data security if you know who is accessing what, where, when, for how long and for what purpose...with the ability to have that identity go through multiple layers of authentication.

Consistent Application Controls

Security controls are usually where the rubber meets the road. But where we're going, we don't need roads. What was once solved by tacit knowledge and key technology needs to now be solved by business acumen and interpersonal skills.

Inconsistent Talent

Current cyber security talent is not necessarily future cyber security talent. Network architects are not necessarily cloud network architects. Threat Intel analysts are not necessarily SOAR technicians. Unlocking a pipeline of needed talent is perhaps the most important aspect of the CISO role moving forward.

Regulatory Compliance

Any cloud decisions made must come after reading the tea leaves of proposed local legislation the world over. The concept of saving organizational dollars by not spending in an area that will clearly soon have regulatory oversight has been proven to be foolish.

VISIBILITY

Top cyber security executives have seen this all before. The implementation of new and increasingly decentralized systems and tools to help manage the security of the enterprise has been happening since the beginning of the information security discipline itself.

But when defending a castle with a moat and other ever increasingly complex apparatus, visibility was more straightforward. As DevOps increasingly occurs in a cloud environment and business users continue to utilize more and more cloud-enabled SaaS tools, the enterprise itself now mostly exists and operates on the edge.

Main Street was once the nerve center of a community. Businesses were distinct yet connected. Everything needed was in one place, connected by one street. If part of that street was compromised, all businesses were affected. Enterprise has evolved over the past half-decade to once again reside on just 'one street' - the cloud. True interconnectedness between supply chain partners has brought true security interdependence. This construct has birthed dependency confusion.

With the evolution of how the business works and how businesses are connected, there has been an evolution in cyber security threats. With the evolution of cyber security threats, some of the install base tacit knowledge is moot.

"A high-level approach is called for which engages procurement to vet potential supply chain partners in order to ensure that a level of cyber hygiene does not present a risk to the purchaser. More to the point, because of the intertwined ecosystem, we have a responsibility to be good citizens and assist supply chain partners when an incident occurs. Not in a punitive context but in a supportive capacity for the greater good. Ultimately, a system like the financial services KYC program is needed."

IAN THORNTON

Cyber Security Hub Executive Advisory Board

There is a significant global shortage of cyber security talent for the open positions today. But job functions are also evolving. Network architecture experts are needed less. Cloud network architecture experts are needed more. Blue team job functions are needed less. Purple and Red team job functions are needed more.

Thus the process of gaining visibility resides in the connective tissue of systems but also the evolution of the people overseeing those systems along with the ability to simultaneously be interconnected with supply chain partners yet not suffer from dependency confusion.

ENABLEMENT

While the need for information security had its onset when humans began to communicate with language, modern cyber security is a relatively recent phenomenon. Lessons have been learned by the good, tactics have evolved for their adversaries and zeitgeist best practice advances accordingly.

"Technology is a reactive protection. People and processes are the weakest links, and behavioral analysis creates visibility to risky users and proactive risk management."

LISA TUTTLE

CISO, SPX Corporation

The security executive learns from past adversarial strategies to forecast future attacks on a known threat landscape. When the landscape changes, the security executive adapts. Until very recently, a good defense has been the best offense. All things considered, a forward security posture has been assumed in rather rapid fashion- many more conversations these days are had around threat hunting than around firewalls.

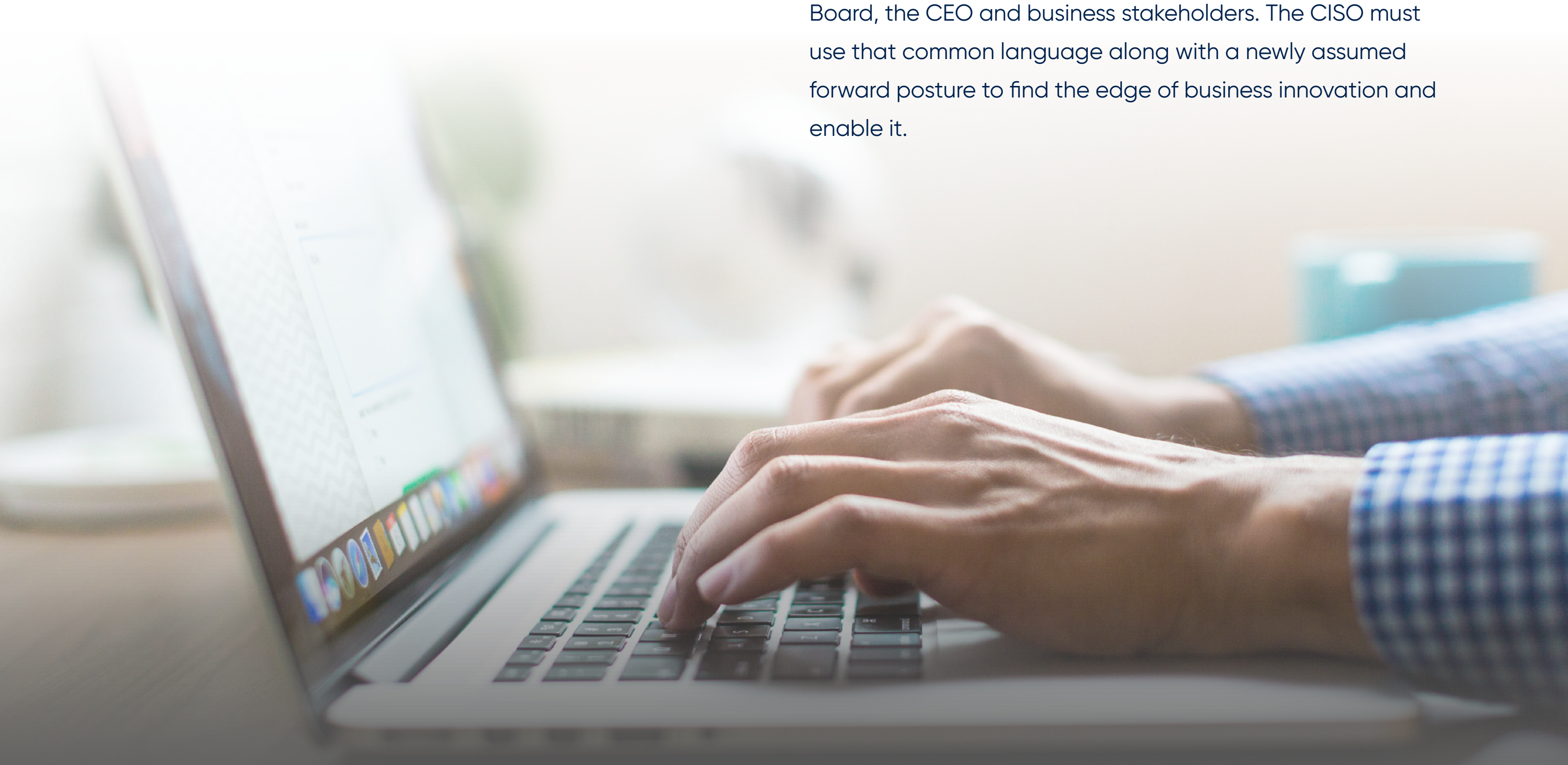
"We talk about 'data breaches' because of regulatory and statutory definitions that focus on the disclosure of data. An organization's security strategy should work with the end in mind, and focus heavily on denying threat actors access to those data with the highest regulatory, statutory, or contractual risks."

KAYNE MCGLADREY

Cyber Security Hub Executive Advisory Board

As security has gone from heel to toe, business operations have gone from the ground to the cloud. So while the philosophy of cyber security has revolutionized, the process of business has transformed. The business simply needs to consistently find and use new and different tools to ensure the organization outpaces change and provides value to shareholders and customers into the distant future. That cannot happen if the company cannot learn from previous security incidents.

And so, cloud security embodies the essence of the CISO role. The landscape changes and the CISO adapts. But this adaptation is an evolution. The CISO is now a business executive who must speak with common language to the Board, the CEO and business stakeholders. The CISO must use that common language along with a newly assumed forward posture to find the edge of business innovation and enable it.



EXECUTIVE INTERVIEW

Louis Evans, Product Marketing Manager, Arctic Wolf Networks

WHAT IS THE CLOUD SECURITY LANDSCAPE?

The fundamental dynamic of the cloud security landscape is the balance of cloud security responsibilities between cloud providers and users. It's more complex than, "cloud providers are responsible for this and end users are responsible for that". It's about understanding shared responsibility: what kinds of security-relevant data cloud providers make available, how organizations can operationalize it, and so on. Cloud security vendors sit atop that dynamic and partner with users to help close that gap. Here at Arctic Wolf we apply our security operations approach to the gaps most businesses struggle with: detection, security posture management, unified security visibility, and so on.

CAN YOU PROVIDE A CLOUD SECURITY USE CASE?

Sure, let's talk about a really basic security best practice: multi-factor authentication (MFA). Everyone knows you need to implement it across your platforms—and especially in SaaS systems, where accounts and logins are the primary target for attackers. And SaaS vendors recognize this, and they offer MFA.

But security isn't necessarily the top priority for these SaaS vendors. So implementing multi-factor authentication is more complicated than it looks. It's not just a question of activating MFA for user login. It also requires going through all of your other settings—API calls, other access pathways—and deactivating single-factor authorizations. This is all pretty basic but it still gets very tricky—and a SaaS customer may not even know about this vulnerability until it's exploited by an attacker. That's true in this simple case and in lots of more sophisticated, complex cases. That's why partnering with a cloud security vendor can be so valuable.

HOW CAN THE BUSINESS ENGAGE IN SAAS AND CLOUD SECURITY BEST PRACTICES?

It's a real challenge. Typically, the gap is people and process rather than technology. Most of the technological requirements for most key security best practices are in place through the cloud provider. They have the configuration options needed, or they make they security-relevant data available. But organizations lack the cloud security experts with the knowledge of all of the best practices they should be implementing, and they lack the processes to go after their vulnerabilities and review their alerts in a systematic way. Often there's a certain technological gap too, a lack of data aggregation or a pipeline for new security configuration data, but they key gaps are definitely in people and process. Cloud security talent is so rare, and in such high demand.

> *"A cloud customer may not even know about their cloud vulnerabilities until an attacker exploits them. That's why it's so valuable to partner with cloud security experts."*
>
> **Louis Evans**
>
> Product Marketing Manager, Cloud Solutions, Arctic Wolf

HOW ARE YOU HELPING BRIDGE THE GAP?

The key ingredient is definitely our concierge security teams, who partner with our customers, bringing their expertise to the table as an extension of those customer IT teams. And our concierge teams sit on top of an involved security pipeline and process, where we're constantly collecting and updating vulnerability info, security benchmarks, indicators of compromise, and so on, and comparing them with customer cloud data. All of that together is how we're able to support our customers in such a new, dynamically evolving environment.

ABOUT ARCTIC WOLF

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we help organizations end cyber risk by providing security operations as a concierge service. Arctic Wolf solutions include Arctic Wolf® Managed Detection and Response (MDR), Managed Risk, and Managed Cloud Monitoring—each delivered by the industry's original Concierge Security® Team. Highly-trained Concierge Security experts work as an extension of internal teams to provide 24x7 monitoring, detection, and response, as well as ongoing risk management and cloud coverage to proactively protect organizations while continually strengthening their security posture.

FOR MORE INFORMATION, VISIT WWW.ARCTICWOLF.COM

ABOUT CYBER SECURITY HUB

The Cyber Security Hub is an online news source for global cyber security professionals and business leaders who leverage technology and services to secure the entire perimeter in their enterprise.

We're dedicated to providing the latest industry news, thought leadership and analysis in the cyber security space. Cyber Security Hub's expert commentary, tools and resources are developed through obtaining data and interviewing end users and analysts throughout the industry to deliver practical and strategic advice.

Our editorial team surveys and monitors the latest trends in cyber security and creates news articles, market reports, case studies and in-depth analysis for a captive audience consisting of C-Level executives, VPs and directors of cyber security and information technology.

CYBER SECURITY HUB TEAM

Dorene Rettas
Managing Director
Dorene.Rettas@CSHub.com

Seth Adler
Editor-in-Chief
Seth.Adler@iqpc.co.uk

Tilak Antony
Director of IQPC
Digital Partnerships
Tilak.Antony@iqpc.com

Imran Shafi
Sales Director
Imran.shafi@iqpc.com

Rose Morishita
Director of Marketing
Rosecley.Morishita@iqpc.com

Desiree Santiago
Marketing Manager
Desiree.Santiago@cshub.com

SOCIAL MEDIA INFORMATION

Facebook:
CSHubIQPC

Twitter:
CSHubUSA

LinkedIn:
CSHub – Enterprise Security Professionals

JOIN US AT OUR UPCOMING ONLINE EVENTS:

CYBER SECURITY DIGITAL SUMMIT FOR: THREAT INTELLIGENCE 2021 AMERICAS

March 16 - 17
Sessions Available On Demand

CYBER SECURITY DIGITAL SUMMIT FOR: THREAT INTELLIGENCE 2021 APAC

March 30 - 31
Sessions Available On Demand

CYBER SECURITY DIGITAL SUMMIT FOR: HEALTHCARE 2021

April 13 - 14
Sessions Available On Demand

CYBER SECURITY DIGITAL SUMMIT FOR: GLOBAL 2021

May 4 - 5
Sessions Available On Demand

CYBER SECURITY DIGITAL SUMMIT: APAC 2021

July 13 - 14
Sessions Available On Demand

CYBER SECURITY DIGITAL SUMMIT FOR FINANCIAL SERVICES 2020

September 14 - 15
Sessions Available On Demand

CYBER SECURITY DIGITAL SUMMIT FOR: EMEA 2021

October 19 - 20
Sessions Available On Demand

CYBER SECURITY DIGITAL SUMMIT FOR: NORTH AMERICA 2021

November 9 - 11
Sessions Available On Demand

CYBER SECURITY HUB

Visit CSHub.com for more information from cyber security leaders for the cyber security community