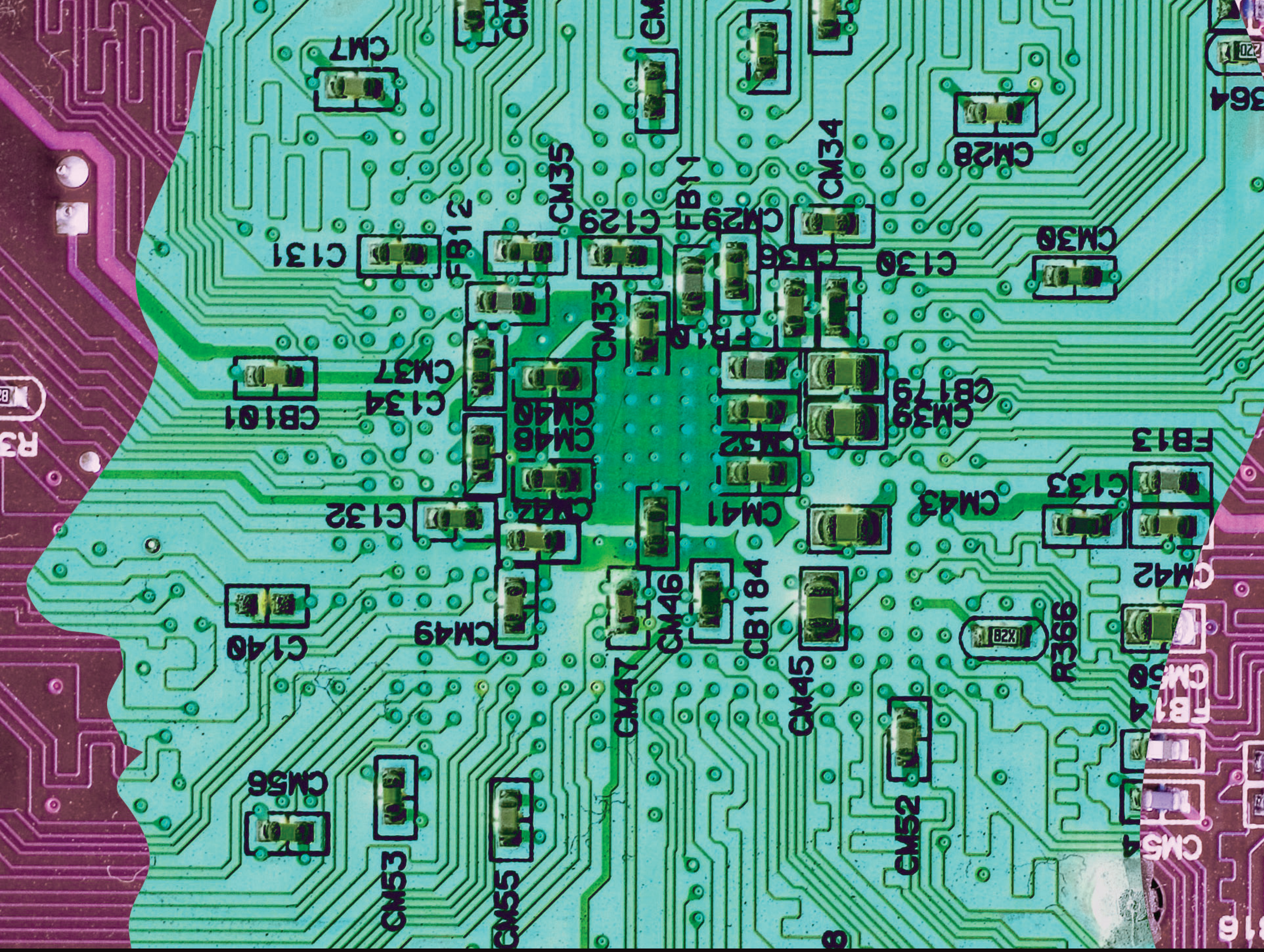


CENTER FOR LONG-TERM CYBERSECURITY

MITRE ATT&CK® as a Framework for Cloud Threat Investigation

JASDEEP BASRA AND TANU KAUSHIK

UC BERKELEY
CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

MITRE ATT&CK® as a Framework for Cloud Threat Investigation

JASDEEP BASRA AND TANU KAUSHIK

SEPTEMBER 2020

CLTC
Center for Long-Term
Cybersecurity
UC Berkeley

Contents

Executive Summary

With the rapid adoption of cloud computing, new security challenges have emerged for all enterprises. We surveyed and interviewed leading security professionals to investigate how they assess and confront these challenges, including rapidly changing technology and business models, ambiguity between cloud providers and purchasers of cloud services about shared responsibilities for security, and the need to manage threats in the cloud that are intertwined with on-premise and hybrid environments.

A strong majority of our research subjects believe that a unified investigation framework that includes both cloud and on-premise environments would improve their processes and outcomes by providing a single integrated solution for threat investigation. Such frameworks exist, but their overall utility is limited by several perceived shortcomings, most notably a lack of interoperability with security tools that impedes automation.

The MITRE ATT&CK® framework is the most widely adopted at present; many enterprises are moving toward more widespread adoption as this framework improves its integration and automation capabilities. Further improvement in these areas would facilitate firms more confidently leveraging the efficiencies gained from cloud computing.

Key findings from the report include:

- **Adversary techniques are executed against nearly all enterprises in the cloud:** 81% of organizations experience adversary techniques found in the ATT&CK Matrix for Enterprise covering cloud-based techniques (Cloud Matrix); 58% of all enterprises experience the "Initial Access" phase of an attack on a monthly basis.
- **Enterprises use the ATT&CK framework to determine gaps in currently deployed security products and for other important tasks:** Fifty-seven percent of global respondents believe the ATT&CK framework is helpful for determining gaps in currently deployed security tools. Fifty-five percent recommend the framework for security policy implementation, and 54% find the framework useful for threat modeling.
- **The ATT&CK for Cloud matrix is widely adopted:** Sixty-three percent of large- and medium-sized enterprises we surveyed use both the Cloud Matrix and Enterprise Matrix (Windows/Mac/Linux) in their security operations centers.
- **Large- and medium-sized enterprises are not fully confident that their security products detect all techniques in the ATT&CK matrices:** Only about 49% of

respondents feel highly confident in the ability of their security products to detect the adversary tactics and techniques in each of the ATT&CK matrices.

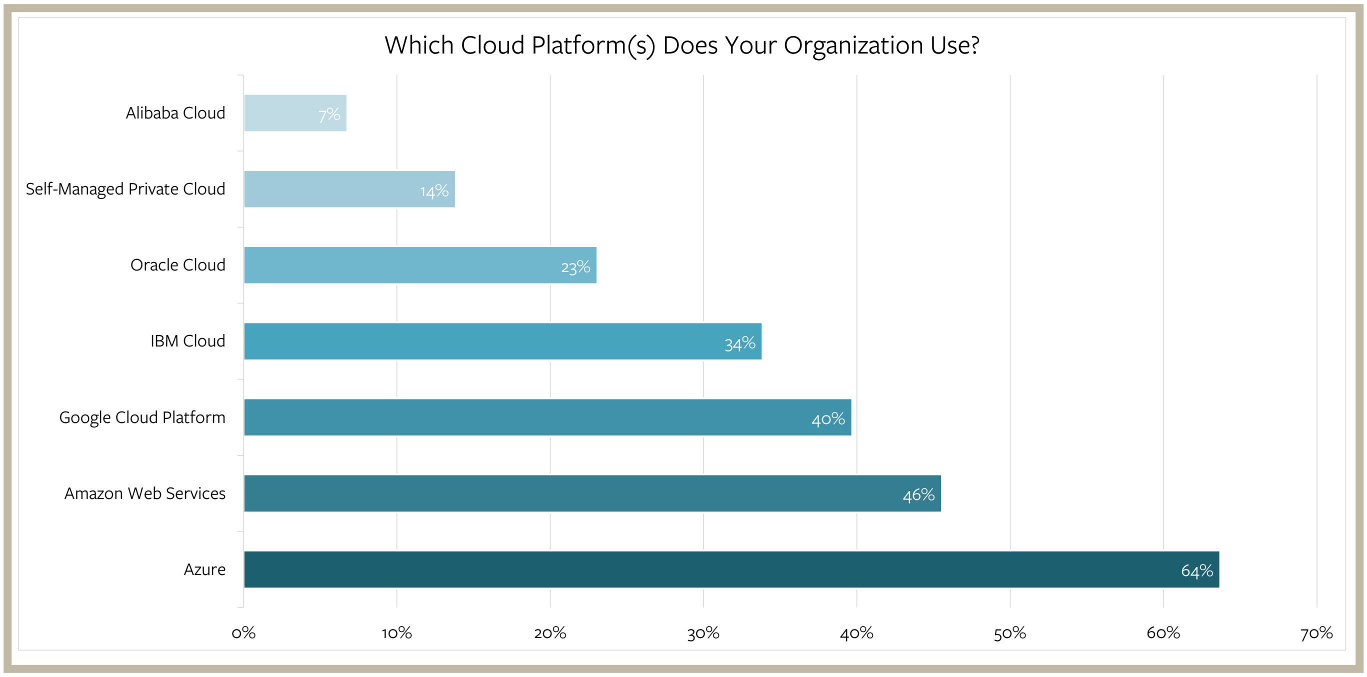
- **The biggest challenge with ATT&CK framework implementation is its lack of interoperability with security products:** 45% of global survey respondents identify the lack of interoperability with their security products as the biggest challenge with the ATT&CK framework, and 43% cite the challenge of mapping event data to tactics and techniques.
- **A large percentage of enterprises do not correlate events from the cloud, networks, and endpoints to investigate threats:** Only 39% of enterprises incorporate events from all three environments (cloud, network, and endpoints) when investigating threats.
- **The ATT&CK framework can increase confidence in cloud security and adoption:** Eighty-seven percent of survey respondents agree that adopting the ATT&CK for Cloud matrix will improve cloud security in their organizations. Seventy-nine percent say it would also make them more comfortable with cloud adoption, and 69% agree that they would be more comfortable with outsourcing their security operations center to a third-party provider that uses the ATT&CK framework.

Background and Motivation

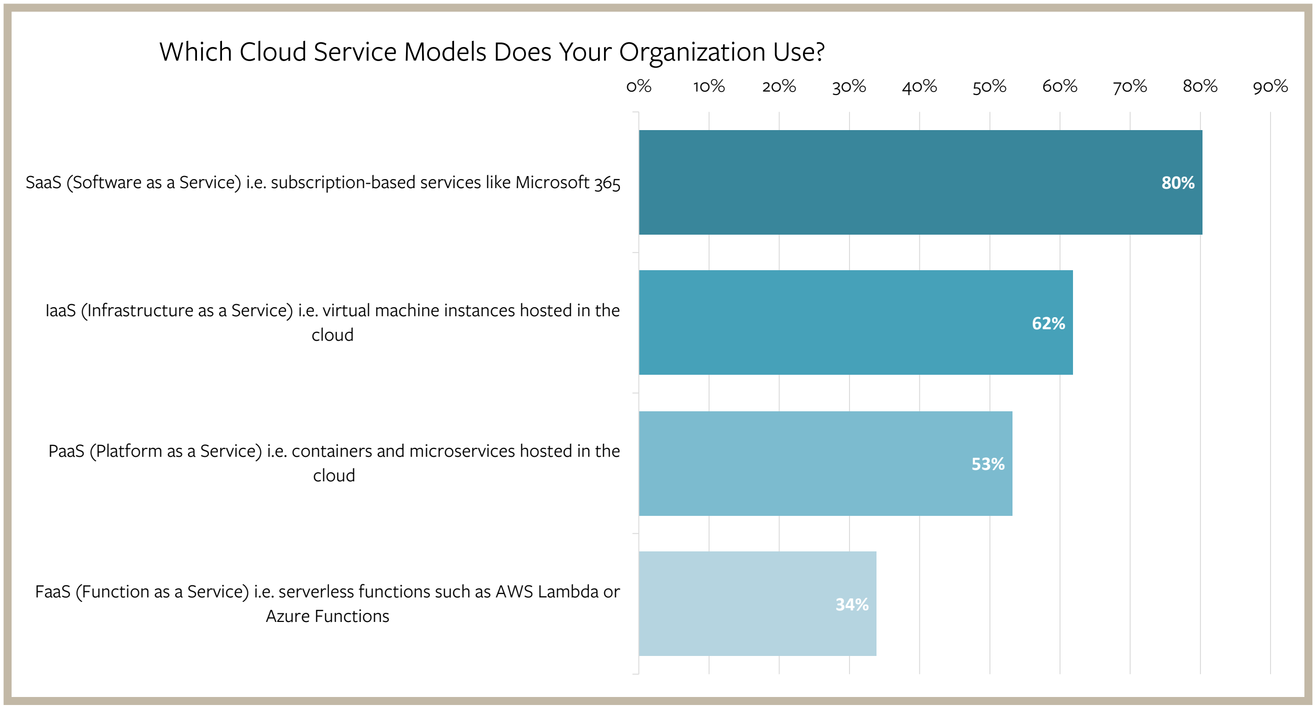
Cloud computing enables any organization to pay to use hardware and software resources housed in a cloud service provider's data center. The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1]

Cloud computing is primarily offered through four service models: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), and Function-as-a-Service (FaaS). Cloud deployment architectures can be public, private, or hybrid i.e. combining a self-managed private cloud with a public cloud.

Our survey indicates that, across the industry verticals we surveyed, hybrid cloud is the most popular deployment architecture across all major cloud providers, including AWS, Microsoft Azure, GCP, Oracle Cloud, Alibaba Cloud and IBM cloud. Amazon is the leading cloud provider with around 32% of global market share as of Q1 2020. However, Microsoft Azure is growing in popularity with market share increasing from 11% in Q2 2017 to 18% in Q1 2020.[2] Among our survey respondents, Azure was more popular than expected (64% use Azure, while 46% use AWS) and Azure was also most popular in all three market segments (United States; Europe,



Middle East and Africa; and Asia Pacific) by a great margin. We hypothesize that this is due to the survey sampling large enterprises and government agencies, which are more likely to already be invested in the Microsoft technology stack.



Currently, cloud infrastructure services represent the fastest-growing sector of the cloud computing market, although SaaS is — and is expected to remain — the largest segment overall.[34] This finding from Statista was confirmed by our survey, which found widespread adoption of SaaS (80% of total respondents).

While cloud computing provides the flexibility to choose from various service models and deployment architectures, it also presents serious security issues. These service models require varying responsibilities to be shared between the cloud provider and the customer. The IaaS model assigns responsibility for the security of the lower layers (i.e storage, networking, server, and virtualization layers) to the cloud provider. The customer is responsible for the security of the operating system and everything that runs on top of it. In the PaaS model, the cloud provider is responsible for everything but the data and application, including networking, storage, servers, virtualization, operating system, middleware, and runtime. The FaaS model, also referred to as a "serverless architecture," assigns customer responsibility for individual programming blocks that provide specific microservices, while the cloud provider is responsible for everything else. In the

Service Model	Lower Layers (Storage, Networking, Server, Virtualization)	Operating System	Middleware/ Applications	Functions	Configuration	Data
IaaS	Cloud Provider	Customer	Customer	Customer	Customer	Customer
PaaS	Cloud Provider	Cloud Provider	Customer	Customer	Customer	Customer
FaaS	Cloud Provider	Cloud Provider	Cloud Provider	Customer	Customer	Customer
SaaS	Cloud Provider	Cloud Provider	Cloud Provider	Cloud Provider	Customer	Customer

Illustration of the Shared Responsibility Model for Cloud Security

SaaS model, the cloud provider is responsible for everything related to the security of the service they operate. The greater the cloud provider's control of the service model, the more security responsibilities the cloud provider has. However, in every service model, the customer is still responsible for configuring the service, managing user access, and, critically, protecting its own data.

Given the advent of these new models of computing, we identified a need to evaluate the security challenges faced by enterprises that have adopted them. Our research is focused on analyzing the challenges that enterprises currently face in cloud security, such as breach detection, data exfiltration, and unauthorized access. For a comprehensive assessment, we conducted a survey of security leaders — including CISOs, CIOs, CTOs, and security operations center (SOC) analysts — across 325 large- and medium-sized enterprises in the UK, US, and Australia. Fifty-seven percent of our global survey respondents are large enterprises, and 62% have an in-house security operations center. We categorized enterprises with 5000+ employees as large- and 1000+ as medium-sized. We targeted diverse sectors for our survey, including IT, technology and telecoms, retail, transport, financial services, manufacturing and production, and other sectors. We investigated the challenges faced by security operations teams and evaluated the use and impact of standardized frameworks for threat investigation. We hypothesized that MITRE ATT&CK® would be the most widely adopted framework, and the survey results validated this assumption.

According to MITRE, the private, not-for-profit company that developed the ATT&CK framework, "MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community."[5]

Within this framework, we examined the application of two matrices and their respective sub-matrices: the more general "Enterprise Matrix" and the "Cloud Matrix," which is described as "the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques." ATT&CK contains 12 categories of adversary tactics and techniques, 10 of which are shared across all matrices. The 12 tactics are:

- Initial Access (e.g. from spear-phishing)
- Execution (e.g. through PowerShell)
- Persistence (e.g. using logon scripts)
- Privilege Escalation (e.g. with process injection)
- Defense Evasion (e.g. modifying registry)
- Credential Access (e.g. extracted credentials from web browsers)
- Discovery (e.g. network share discovery)
- Lateral Movement (e.g. connect over remote desktop protocol)
- Collection (e.g. data from local system)
- Command and Control (e.g. communication through non-standard port)
- Exfiltration (e.g. exfiltration over command and control channel)
- Impact (e.g. data encrypted by ransomware)

Our research investigated the efficacy and adoption of both the enterprise and cloud matrices, with a specific focus on the cloud matrix and the impact of the ATT&CK framework on overall cloud security.

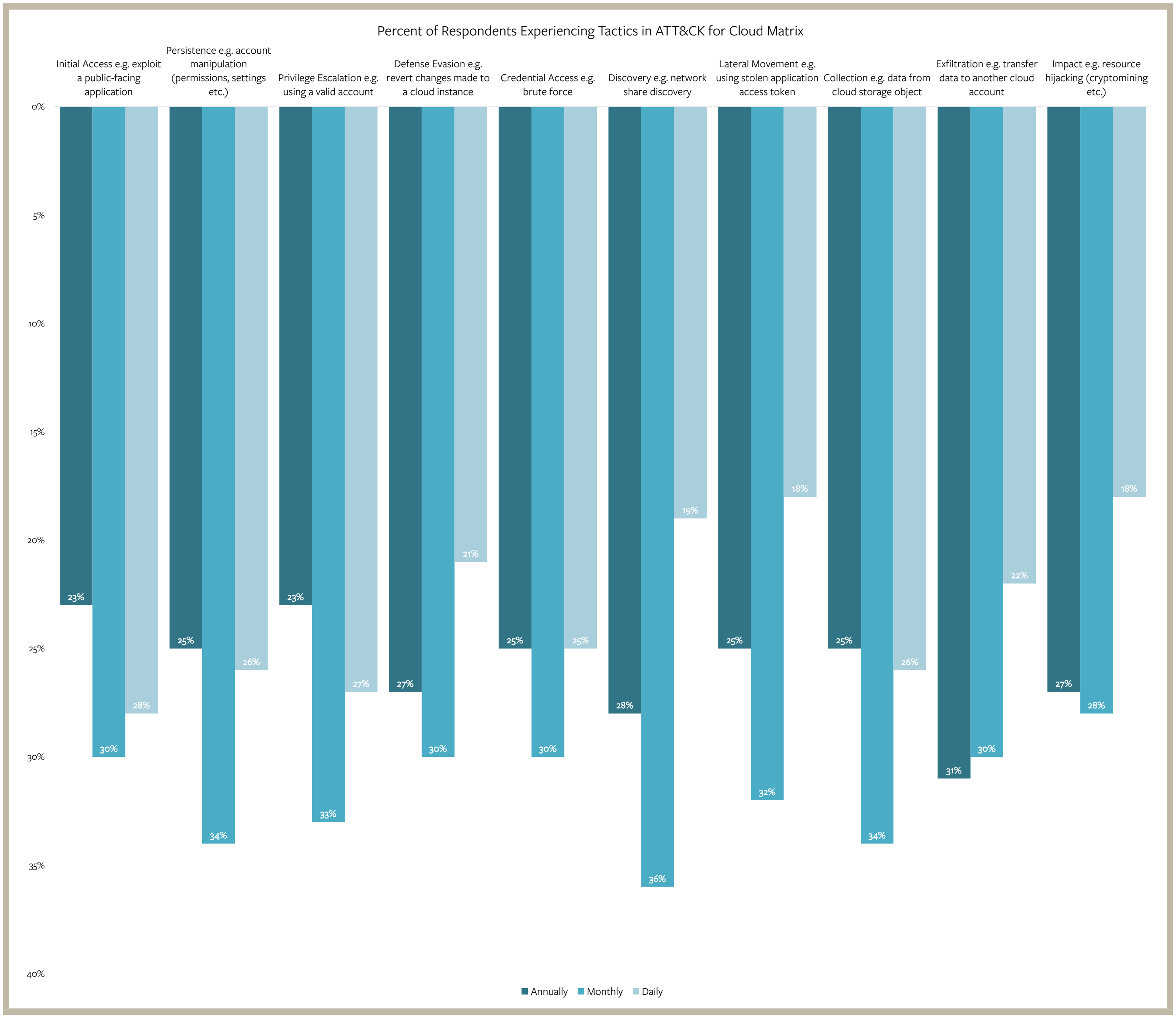
In parallel to the survey, we conducted in-depth interviews with ten leading security experts from large- and medium-sized enterprises working in different cybersecurity functions. Interviewees included individuals with a variety of backgrounds, including senior red team engineer, security product manager, cybersecurity manager at a cloud provider, and chief information security officer. All the interviewees highlighted that security operations centers should adopt a framework such as ATT&CK to investigate threats as it helps gain a comprehensive understanding of adversary tactics and techniques.

Cloud Security Challenges

All our interviewees highlighted that, despite the clear delineation in management and control, there is still ambiguity about the **shared responsibility for securing the cloud** in the event of a security incident. This is in part due to the lack of visibility into the layers managed by cloud providers; for instance, in the IaaS model, these lower layers include storage, networking, server, and virtualization. This lack of visibility makes it difficult to determine whether a customer's data breach resulted from a security incident on the cloud provider's hosting platform. For example, in 2019, a Fortune 500 company leveraging cloud services suffered a breach partially due to its cloud provider's internal security posture.[6] Thus, it can be very challenging to determine whether a breach resulted from the customer (cloud purchaser) or the cloud provider. The risk is compounded by cloud providers' desire to limit liability for security incidents when possible. According to one interviewee, cloud providers have large legal and technical teams that examine each incident to minimize their liability as much as possible.

Cloud service providers are increasingly introducing "as-a-service" offerings that give them greater responsibility for security. The Illustration of the Shared Responsibility Model for Cloud Security above demonstrates how models introduce new delineation for each layer i.e from lower layers to application specific configurations. Each model shifts the customer versus the cloud provider responsibilities and we have observed an increase in **new computing models which could further complicate the delineation of security responsibilities**. For instance, Function-as-a-Service (FaaS) is a relatively new offering that has seen rapid adoption, with Amazon, Google, and Microsoft offering serverless functions as of 2016/2017. The introduction of new service models like FaaS requires re-examination of security responsibility.

In addition to the ambiguity over the ownership of security controls, enterprises face challenges in defending cloud environments. Thirty-four percent of our survey respondents currently face challenges with **detecting an attack in progress**, 32% face challenges in **protecting and managing multiple cloud services**, 31% struggle with **insecurity due to data shared with third parties**, and another 31% struggle with **securing against unauthorized access**. We also asked respondents about their experience with the tactics listed in the ATT&CK for Cloud Matrix, and how often they see these tactics in their own environments. Eighty-one percent of respondents reported they had experienced all of these tactics on an annual to daily rate.



Our survey respondents observed all 10 tactics in the ATT&CK for Cloud Matrix — from initial access to data exfiltration — on a consistent basis, i.e once a month or daily. Organizations **struggle with multiple threat types concurrently**, each posing a high risk. Security operations teams function to triage and remediate this wide range of threats. Sixty percent of the organizations we surveyed have had a security operations center (SOC) in place for over four years, which we consider to be a "mature SOC." And we found an increase in the number of dedicated cloud threat investigators that companies have hired to deal with these concurrent challenges. We observed in our survey that 32% of respondents currently have 10-20 cloud threat investigators in their security operations centers, while 15% of respondents currently have 20+ cloud threat investigators.

With the numerous challenges and growing complexities in managing cloud security, SOC teams still need more analysts dedicated to cloud threat investigation. They also must ensure that cloud threat investigations are integrated with the rest of SOC investigations, since many threats are not isolated to the cloud or to on-premise infrastructure. According to a senior red team engineer we interviewed, a common technique used to gain access to an enterprise's cloud environment is to gain access to the cloud devops admin's workstations that are used to administer the cloud environment. Due to the **hybrid deployment models and heterogeneous environments, threats originating from cloud services can penetrate through the on-premise infrastructure and vice versa**.

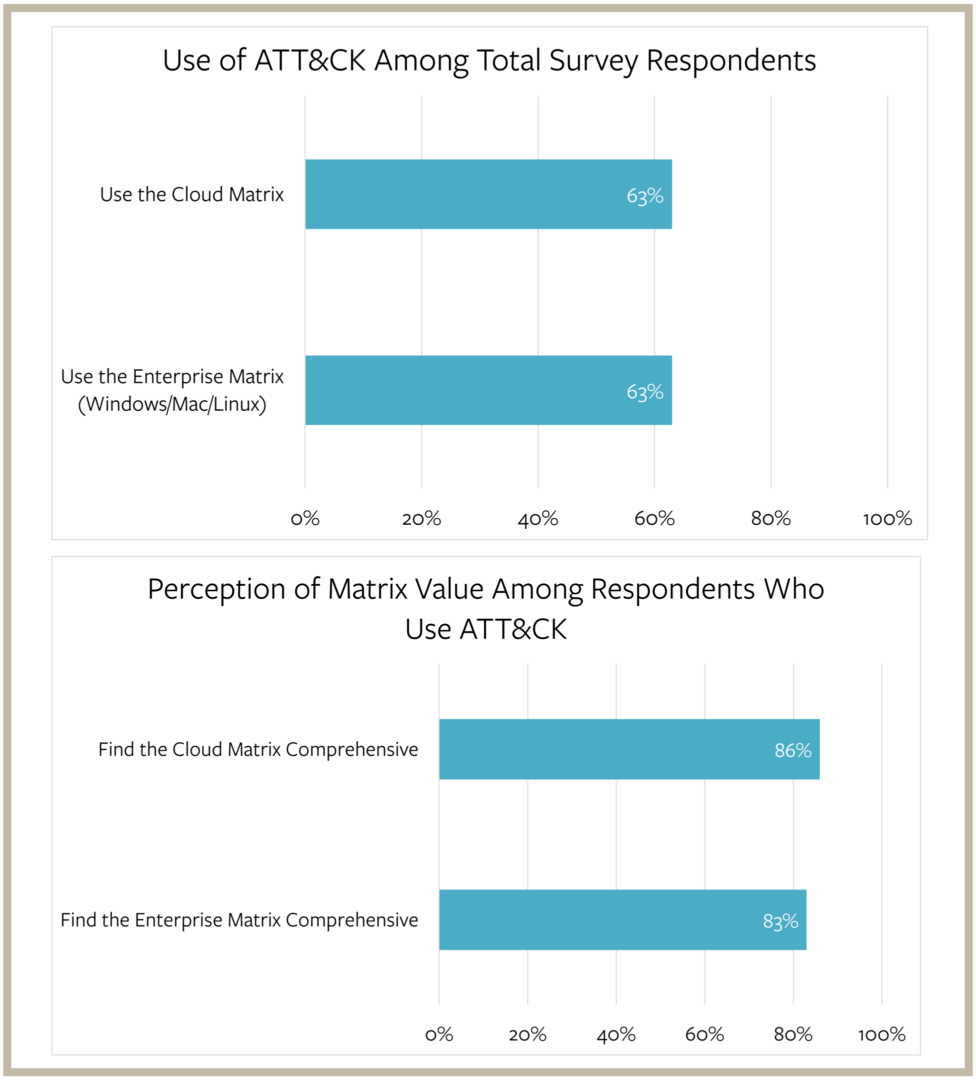
All these challenges highlight the need for a framework for threat investigation that can encompass both cloud-native threats and the threats to traditional on-premise infrastructure.

MITRE ATT&CK® as a Possible Solution

All interviewees highlighted that security operations centers should adopt a framework such as ATT&CK to investigate threats as it helps gain a comprehensive understanding of adversary tactics and techniques. Of the large- and medium-sized enterprises we surveyed, 63% use both the ATT&CK for Cloud and Enterprise (Windows/Mac/Linux) matrices in their current security operations centers.

Eighty-seven percent of survey respondents agree that adopting the ATT&CK for Cloud matrix will improve cloud security in their organizations. Seventy-nine percent say that it would also make them more comfortable with cloud adoption. Further, 69% agree that they would be more comfortable outsourcing their security operations center to a third-party provider that uses the ATT&CK framework. Therefore, service providers that use the ATT&CK framework in their security teams and products may be perceived as better meeting their responsibility to secure the use of cloud services. **ATT&CK is widely used by defenders across industries and in government to find gaps in visibility, security tools, and processes.**

We investigated the state of cloud security and security operations further by evaluating the adoption rate and value of the ATT&CK framework. Eighty-one percent of enterprises in our survey currently use the ATT&CK framework in general, with 63% using the Enterprise Matrix (Windows/ Mac/Linux) and 63% using the Cloud Matrix. **Among survey respondents who use the Enterprise Matrix, 83% find that it comprehensively represents the adversary tactics and techniques they face. Among survey respondents who use the Cloud Matrix, 86% find that it comprehensively represents the adversary tactics and techniques they face.**

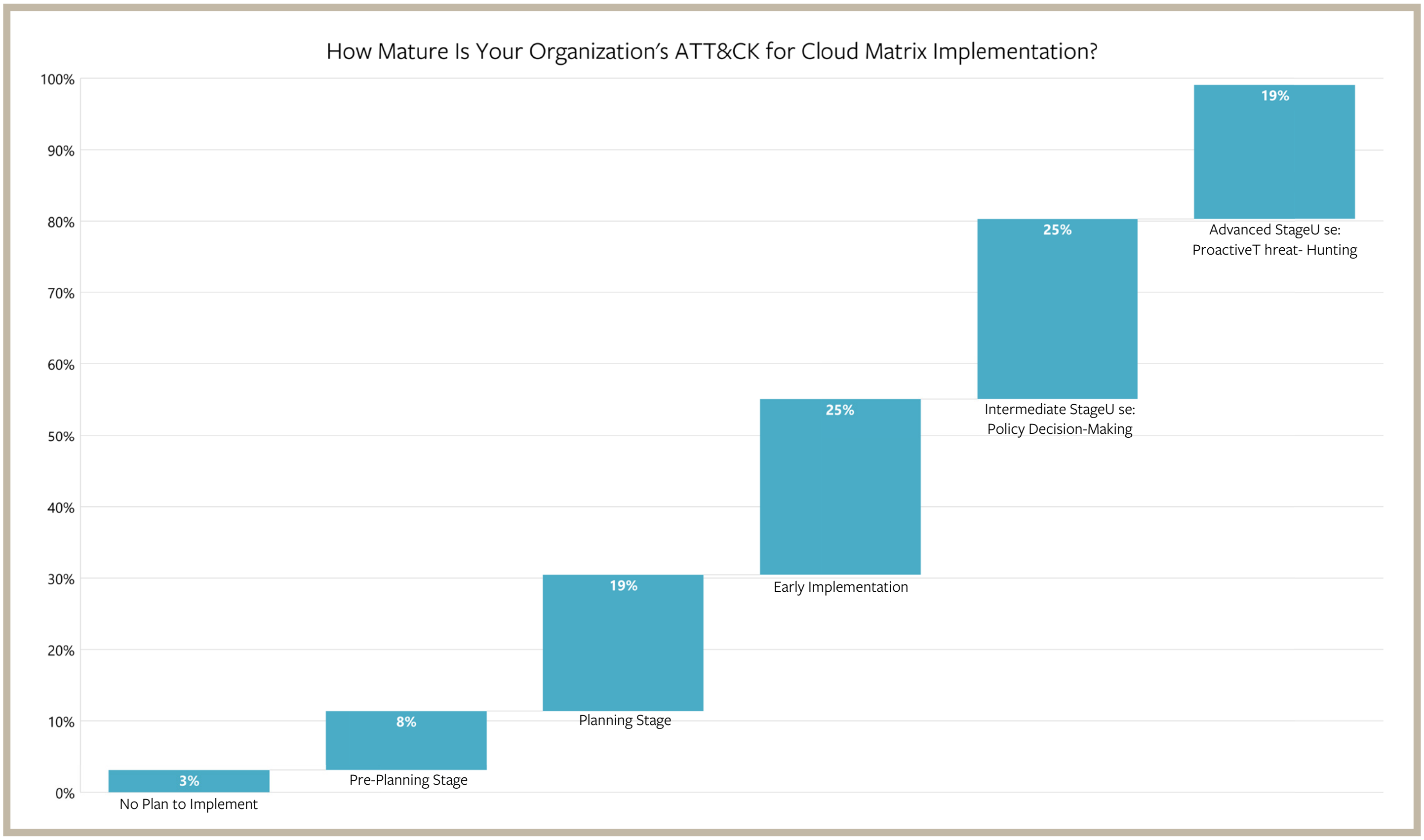


Use of ATT&CK Among Total Survey Respondents

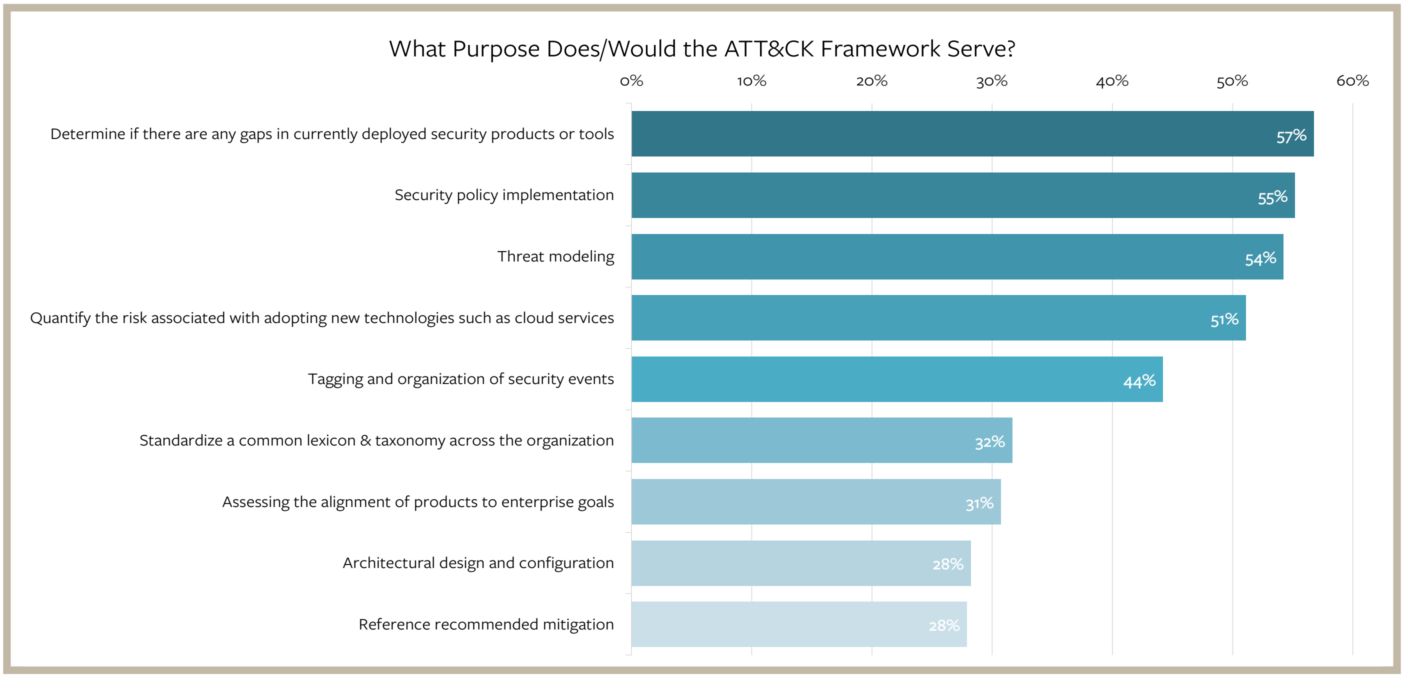
Perception of Matrix Value Among Respondents Who Use ATT&CK

To understand enterprise level of adoption of the Cloud Matrix in our survey, we categorize implementation into six different stages:

- No plans to implement
- Pre-planning stage
- Planning stage
- Early implementation stage (use for reference and knowledge management)
- Intermediate stage (informed decision-making and automated responses)
- Advanced stage (proactive threat-hunting)



We found that **44% of our survey respondents have successfully implemented the ATT&CK for Cloud matrix at an intermediate to advanced stage**, and another 44% are in the planning and early implementation stages. The adoption of the framework is driven by the purpose it can serve for each organization. In our study, the top purposes for adoption of the ATT&CK framework include determining gaps in currently deployed security products or tools (cited by 57% of respondents), implementing security policy (cited by 55% of respondents), and threat modeling (cited by 54% of respondents).



Furthermore, mature stages of framework implementation correlate with good security practices. For example, **60% of respondents that correlate security events from cloud, endpoint, and network environments together had an intermediate or advanced implementation of the ATT&CK for Cloud matrix**; 57% for the ATT&CK for Enterprise matrix. Comprehensive analysis of events from all sources leads to increased visibility, as it provides a better holistic understanding of the gaps in security incident detection and prevention.

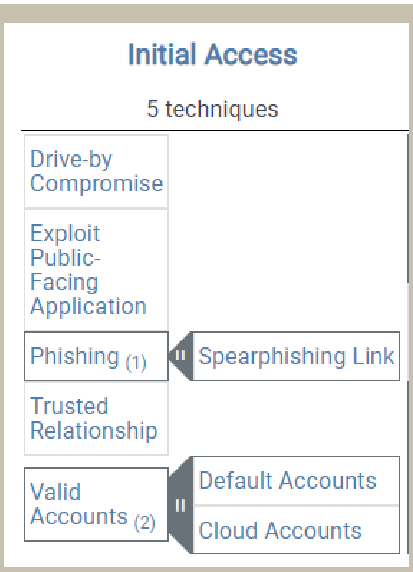
However, the challenge of performing ongoing analysis from all sources and correlation is a **major cause of SOC burnout**. These security events generate a large amount of data, and our interviewees highlighted the urgent need to implement automation. Hence, we investigated the adoption of automation, and found that 48% of respondents who have implemented the ATT&CK for Cloud matrix (in the Early Implementation, Intermediate, or Advanced Stage of adoption) tag events with their cloud security products and allow for the automation of policy changes. However, 43% of respondents tag events, but do not automate security policy changes. This means that 91% of those who have implemented ATT&CK for Cloud use their security products to tag events with techniques from the Cloud Matrix, but less than half have implemented automation for any policy changes.

We find that, **even after successful tagging, the necessary action of security policy implementation remains a manual job**. In our opinion, security operations teams can benefit from end-to-end automated workflows to identify threats based on successful tagging and apply necessary policies that prevent further incidents or enable just-in-time response. This led us to investigate challenges that may be hindering organizations from successful implementation and automation.

Implementation Gaps

We asked survey respondents to identify the challenges they observe while using the ATT&CK framework. Forty-five percent of organizations identified the lack of interoperability with security products while using ATT&CK, 43% cited the difficulty of mapping of event data to tactics and techniques, and 36% say they receive too many false positives. Some of these challenges could be solved by using security products to tag events based on the ATT&CK framework. According to the security leaders we interviewed, there is a need for more products that tag events based on the framework. However, they also caution that mere tagging of events is not the sole requirement. **Tagging of events with ATT&CK Tactics and Techniques helps identify which events should be prioritized by the SOC** — for instance, the “Exfiltration” tactic could be prioritized over “Initial Access.”

Individual organizations should conduct continuous testing to identify the efficiency of all the security products they use in order to identify all the techniques and sub-techniques associated with ATT&CK tactics, such as an Initial Access technique which contains three sub-techniques.



Initial Access

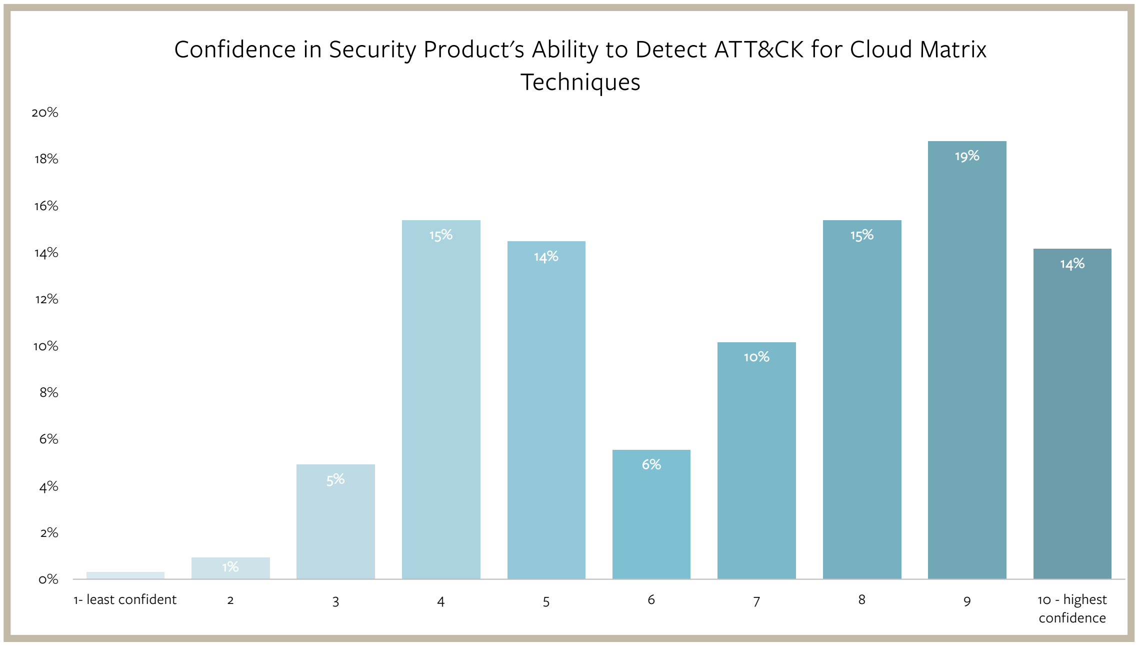
5 techniques

Drive-by Compromise	
Exploit Public-Facing Application	
Phishing (1)	Spearphishing Link
Trusted Relationship	
Valid Accounts (2)	Default Accounts Cloud Accounts

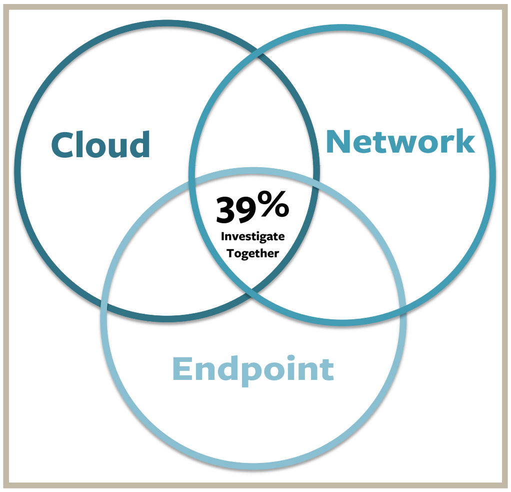
Example of Techniques and Sub-Techniques from the “Initial Access” Tactic of the ATT&CK Cloud Matrix

One other implementation issue we discovered from our survey results is that many organizations do not use the ATT&CK framework because it does not prioritize any adversary techniques, and no weights are assigned. We hypothesize that this is an intentional design decision, made to enable each business or security product to conduct its own independent risk assessment and identify which threats are more likely and have the greatest impact. Prioritization of tactics and techniques will be necessary for each enterprise based on the threat intelligence that they have for their sector and specific threat models.

To further understand firms' implementation gaps, we inquired about the confidence these organizations have in the ability of their security products to detect adversary tactics and techniques in each of the ATT&CK matrices. About 49% of respondents feel highly confident (response between 8-10, on a scale of 1-10, with 10 being highest confidence).


Confidence in Security Product's Ability to Detect ATT&CK for Cloud Matrix Techniques

We then reviewed how these organizations currently investigate threats. The distributed nature of cloud computing and the global accessibility it provides to users over the internet heightens the complexity of identifying and investigating threats across the networks, endpoints, and cloud components used by the enterprise. We asked survey respondents to identify which event sources (network, endpoint, and cloud) they use to correlate data during threat investigation. Based on qualitative assessments from our interviews, we identified that the best practice is to correlate data from all three sources. However, our survey found that only two in five (39%) respondents incorporate events from all three environments when investigating threats. A majority (57%) of those who have adopted the ATT&CK framework investigate both endpoint and cloud security events and threats together.



Organizations that do not correlate events from all sources lose the ability to identify threat patterns.

Finally, our research also indicated a desire that ATT&CK can be used as a risk management framework or to integrate with one, especially to clarify the risks shared between cloud providers and customers. Several of our interviewees highlighted the U.S. Government's Federal Risk and Authorization Management Program (FedRAMP) as a good model.[7] By delineating responsibilities between the federal government and cloud providers for all deployments, FedRAMP enabled the accelerated use of cloud computing by the U.S. Government, including through major contracts such as the Department of Defense's Joint Enterprise Defense Infrastructure (JEDI). Cloud providers have dedicated offerings for the U.S. Government, such as AWS GovCloud and Azure Government. However, further investigation is needed of the benefits or efficacy of the framework, and how the ATT&CK framework could fit into a cloud deployment's Authority to Operate (ATO). We notice that many security products and services that incorporate ATT&CK have been given ATO status, and further research could investigate this connection to determine whether ATT&CK can better assist in delineating shared responsibilities and supplement any risk management framework utilized.

Conclusion and Recommendations

Cloud security remains a continuously evolving landscape; however, most threats can be detected and prevented. Our research finds that enterprises as data owners should adopt a comprehensive approach to cloud threat investigation, irrespective of how the shared responsibility model segregates duties. Although some enterprises do adopt other frameworks to achieve the same effect, the ATT&CK framework is most widely adopted with over 80% of surveyed enterprises having adopted it. We found that adoption correlates with an improved security posture and enables organizations to more confidently leverage cloud computing resources. To clarify further, we recommend that cloud threat investigation should be assessed holistically with the following building blocks:

- **Adopt the ATT&CK framework for threat investigation:** Our survey highlights the importance of adopting a comprehensive framework that can be used to identify the tactics and techniques used by adversaries. Most organizations use the ATT&CK framework to standardize a common lexicon and taxonomy across the organization. In addition, the framework is most used to identify gaps in currently deployed security products or tools, guide security policy implementation, model threats, and assess the risk associated with adopting new technologies, such as cloud services.
- **Investigate threats from all data sources:** An important takeaway from our interviews is the importance of maintaining visibility into events to detect threat patterns. Investigating threats comprehensively and correlating events from network, endpoints, and cloud are critical steps for successful threat detection and prevention. Only two in five (39%) survey respondents are currently incorporating all three environments together when investigating threats.
- **Automation:** Our research also found that security operations teams face an overwhelming number of investigations. All the security leaders we interviewed emphasized the need for automation, and they agree that automatic tagging of events using a security framework would be beneficial. We identify the ATT&CK framework as most comprehensive for this purpose.

Future Research and Study

Our survey was a preliminary investigation to identify the challenges faced by security operations teams as they defend against threats in the cloud. We investigated the impact of the ATT&CK framework, but we did not investigate whether other frameworks could fulfill the same role. Further research could help identify other leading frameworks and how they compare. Survey respondents also indicated they experience a similar frequency (once a month) for the same categories of tactics in both cloud-native environments (AWS, Azure, GCP) and their enterprise environments (Windows, macOS, Linux). This could be due to the nature of hybrid cloud deployments. Further research could be performed to identify whether private or public cloud deployments show any diverging trends.

Endnotes

[1] https://csrc.nist.gov/publications/detail/sp/800-145/final

[2] https://www.statista.com/statistics/477277/cloud-infrastructure-services-market-share

[3] https://www.statista.com/statistics/258718/market-growth-forecast-of-public-it-cloud-services-worldwide/

[4] https://www.statista.com/statistics/477763/public-cloud-segment-revenue-forecast/

[5] https://attack.mitre.org/

[6] https://threatpost.com/capital-one-breach-senators-aws-investigation/149567/

[7] https://www.fedramp.gov/about/

Acknowledgments

The authors would like to thank the Center for Long-Term Cybersecurity at the University of California, Berkeley, especially Steven Weber and Ann Cleaveland for their guidance and help on this project. We also would like to thank Daniel Flaherty and Jennifer Burns for their insights and support. We are grateful to all the security experts who participated in our interviews, as well as those who responded to our survey.

This project was made possible by a gift from McAfee in support of independent academic research.

About the Authors

Jasdeep Basra is a Graduate Student Researcher at the Center for Long-Term Cybersecurity. He is a cyber security veteran with over 7 years of experience with the Department of Defense, focusing on developing cyber security architecture and conducting offensive cyber missions.

Tanu Kaushik is a Graduate Student Researcher at the Center for Long-Term Cybersecurity. She has over 12 years of expertise in Security, Cloud, IT Operations, and End User Services with specializations in Identity & access management and cloud security.

CLTC

Center for Long-Term
Cybersecurity

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley