WEBINAR SUMMARY

May 6, 2021

Stealing the Silver Lining from Your Cloud

Anant Shrivastava, Technical Director, NotSoSecure Global Services
Don Shin, Security Marketing Strategist, ExtraHop

KEY TAKEAWAYS

- Migrating to the cloud involves a major paradigm shift in security.
- Cloud attacks begin with asset enumeration and credential hunting.
- Storage is the lynchpin of cloud existence and is susceptible to attack.
- AWS authentication services have been used to gain access to systems.
- Detection and response require more than just analyzing logs.
- ExtraHop Reveal(x) 360 improves security efficacy and compliance coverage.

in partnership with

ExtraHop

OVERVIEW

By 2020, many organizations were already migrating to the cloud because they saw problems with their outdated on-premise environments and saw significant benefits from the cloud. Then, overnight, the pandemic created a mostly remote workforce, which pushed businesses that hadn't yet taken the leap to quickly move into the cloud, and encouraged those that were moving slowly to move even faster.

While security concerns still exist in a cloud environment, these concerns may be different and not as well understood as those in an entirely on-premise, company-owned environment.

Solutions like ExtraHop Reveal(x) 360 help companies ensure their cloud environments are secure and improve response capabilities when attacks occur.

CONTEXT

Anant Shrivastava discussed key security concerns in the cloud, as well as some of the cloud-based attacks that have occurred. Don Shin described the importance of moving beyond logs for security, and how ExtraHop Reveal(x) 360 can help companies better secure their environments.

KEY TAKEAWAYS

Migrating to the cloud involves a major paradigm shift in security.

Companies are either born in the cloud—typically startups, software-as-a-service (SaaS) providers, and cloud service aggregators—or they are migrating to the cloud from existing on-premise environments. This migration to the cloud is a paradigm shift from conventional environments, including cloud security.

Top Cloud Security Concerns

- Misconfigurations, the biggest concern
- Access control failures, such as insecure application programming interfaces (APIs) and interfaces
- Unauthorized access due to credential leakage
- Unintended data exposure to the public
- Data loss and data sovereignty—becoming a concern, especially with the EU's general data protection regulation (GDPR) and similar regulations

Misconfigurations are a major concern, especially as companies migrating to the cloud often misunderstand cloud provider and client responsibilities. As the matrix below (Figure 1) shows, in a SaaS or cloud environment, the tenant, or customer, is still responsible for client-side configurations, data both in transit and in the cloud, and identity and access management.

> A tenant owns the responsibility for data storage and identity and access management. And that's where the major chunk of problems come up.
>
> *Anant Shrivastava*

Most cloud vendors provide a basic set of tools to clients, which companies can further supplement with third-party offerings, which are especially useful in multi-cloud and hybrid environments.

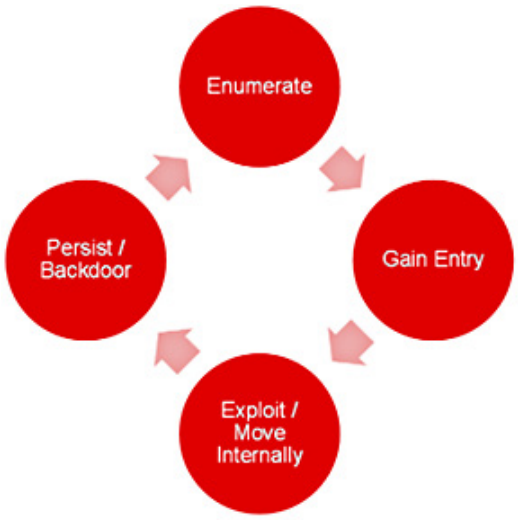
Figure 1: Tenants (customers) still have responsibilities in a SaaS or cloud implementation

Responsibilities	On-prem	IaaS	CaaS	PaaS	FaaS	SaaS
All Things Client Side	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Data (Transit and Cloud)	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Identity & Access Management	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Functional Logic	Tenant	Tenant	Tenant	Tenant	Tenant	Provider
Applications	Tenant	Tenant	Tenant	Tenant	Provider	Provider
Runtime	Tenant	Tenant	Tenant	Provider	Provider	Provider
Middleware	Tenant	Tenant	Provider	Provider	Provider	Provider
OS	Tenant	Tenant	Provider	Provider	Provider	Provider
Virtualization	Tenant	Provider	Provider	Provider	Provider	Provider
Load Balancing	Tenant	Provider	Provider	Provider	Provider	Provider
Networking	Tenant	Provider	Provider	Provider	Provider	Provider
Servers	Tenant	Provider	Provider	Provider	Provider	Provider
Physical Security	Tenant	Provider	Provider	Provider	Provider	Provider

Cloud attacks begin with asset enumeration and credential hunting.

Most attackers take a circular approach to attacking the cloud, beginning with asset enumeration and credential hunting. Once the attacker gains a foothold in a system, they return to the enumeration phase again, often as an internal user with higher privileges than were initially used to gain entry.

Figure 2: Cloud attacks are circular, beginning with enumeration



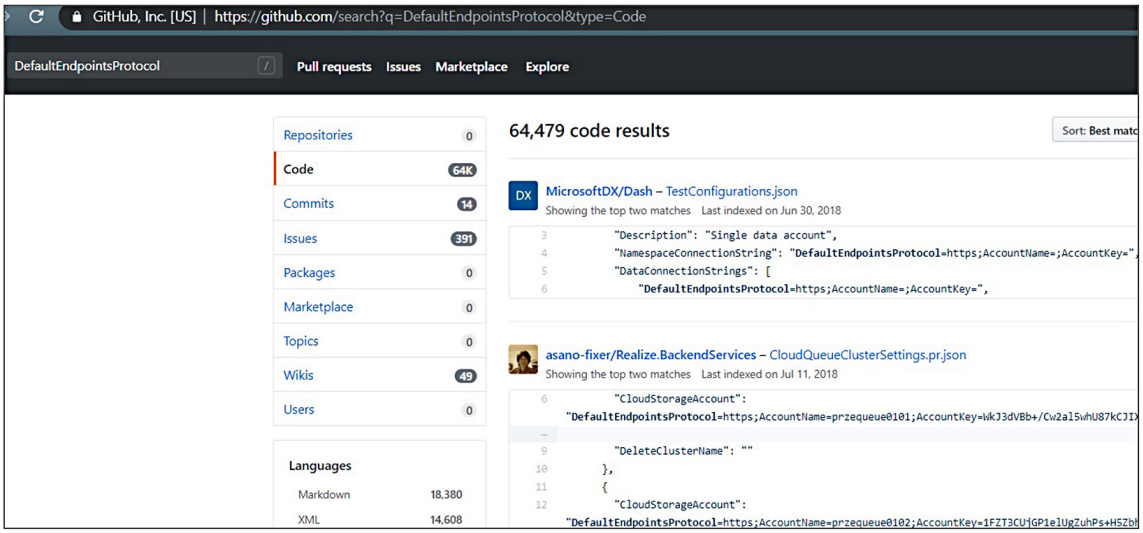
Enumeration typically begins with asset enumeration, looking first at subdomains and then open-source intelligence (OSINT) sources like search engines and certificate transparency logs. Credential hunting is also part of the enumeration phase. With credential hunting, attackers look at user names and OSINT, like code repositories. They also conduct Google dorking, which uses Google applications to find security holes in the configuration and code used by websites.

Storage is the lynchpin of cloud existence and is susceptible to attack.

Regardless of the cloud services in use, all organizations need to store data either in a database or in a storage entity. Application code for platform-as-a-service (PaaS) and function-as-a-service (FaaS) are also stored in the storage entity, which offers a large attack surface.

As with cloud attacks, enumeration is the first step in attacking storage entities. Tools like cloud-enum enable attackers to enumerate cloud service providers, including AWS, Azure, and Google Cloud Platform (GCP), using keywords like company names or default endpoint protocols to find exposed information that can be used for an attack.

Figure 3: Example of a leaked storage account keys in an Azure blob



AWS authentication services have been used to gain access to systems.

Authentication services vulnerabilities and incorrect configurations can be used to gain access to cloud systems. Misconfiguration and vulnerabilities have been found in AWS Identity and Access Management (IAM) and AWS Cognito.

AWS IAM has cloud shadow admin accounts with permissions that attackers can abuse to escalate privileges and take control of the entire environment. Misconfiguration typically plays a role in this security gap, as these accounts are typically overlooked, but vendor error can play a role as well; Amazon had to roll out a new policy—AmazonElasticTranscoder_FullAccess—to close a security gap created by the Amazon Elastic Transcoder Full Access policy.

Amazon's authentication service, AWS Cognito, also has known issues with its unauthenticated and authenticated credentials, which can allow an attacker access to the environment.

Detection and response require more than just analyzing logs.

Cloud providers often recommend that clients capture and analyze events from logs and metrics to detect and investigate security events. Unfortunately, logs don't provide the real-time, transaction-level detail necessary to properly identify and respond to attacks.

Table 1: Logs were not made for detection and response

Log characteristics	Detection requirements
Post-hoc	Real time
Shallow	Transaction-level detail
Difficult to wrangle	No visibility gaps
Easily disabled	Tamper proof

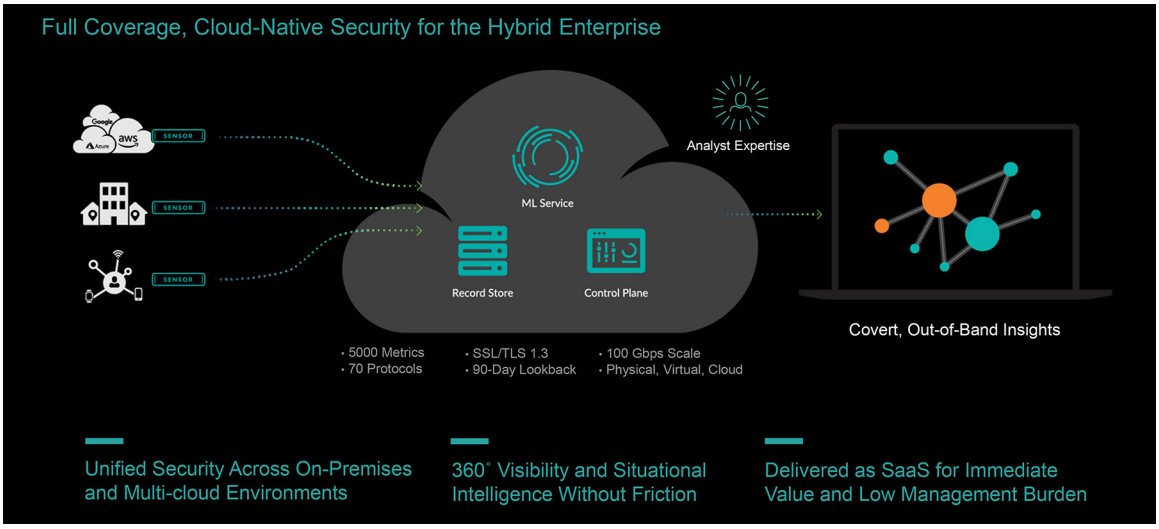
> Logs are not built to be a detection and response platform. Logs, by their nature, are really a post-event analysis type of information.
>
> *Don Shin*

Recognizing the deficiencies of using only logs for security, AWS now offers traffic mirroring for its virtual private cloud. This allows customers to detect and respond faster to attacks that are often missed by log and agent-centric tools.

ExtraHop Reveal(x) 360 improves security efficacy and compliance coverage.

ExtraHop recognizes that logs are not enough to stop advanced threats before these threats do damage to an organization and its infrastructure. The Reveal(x) 360 platform provides full coverage, cloud-native security for the hybrid enterprise, improving security efficacy and compliance coverage.

Figure 4: ExtraHop Reveal(x) 360 provides full coverage, cloud-native security



Reveal(x) is a next-generation intrusion detection system (IDS), offering network detection and response (NDR). Users can see at a glance which assets may be under attack and can further drill into those assets to gain better insight into the threat and how to respond to it.

Figure 5: The Reveal(x) 360 dashboard provides attack information across assets at a glance

ADDITIONAL INFORMATION

- NotSoSecure is presenting virtual courses as part of BlackHat 2021.
- ExtraHop is offering a free trial of Reveal(x) 360.

BIOGRAPHIES

Anant Shrivastava

Technical Director, NotSoSecure Global Services

Anant Shrivastava is an information security professional with 12+ yrs of corporate experience with expertise in Network, Mobile, Application and Linux Security. He is the Technical Director for NotSoSecure Global Services. During his career has been a speaker and a trainer at various international conferences (Black Hat -USA, ASIA, EU, Nullcon, c0c0n and many more). Anant also leads Open Source projects Android Tamer (www.androidtamer.com) and CodeVigilant (www.codevigilant.com). He also maintains the archive portal: http://hackingarchivesofindia.com/. In his free time he likes to participate in open communities targeted towards spreading information security knowledge such as null (null.community). His work can be found at anantshri.info.

Don Shin

Security Marketing Strategist, ExtraHop

DonShin is a security Marketing Strategist who is passionate about simplifying the complex to solve real problems. He has extensive experience with application, database, and network security technologies, having served in various roles at Imperva, A10 Networks, AlienVault, Ixia, BreakingPoint, and others.