RELIAQUEST

The Visibility Factor in Cloud Security:

What Every Organization Must Understand Before Migrating to the Cloud

This cloud security "primer" addresses only one key lesson about migrating to the cloud, because it's the most crucial one to know and understand:

Without visibility, cloud security is impossible.

Unfortunately, many organizations are learning this lesson the hard way. That's especially true for those that have moved fast to adopt and expand their use of the cloud during the coronavirus pandemic to accelerate digital transformation, support remote workers, and deploy new business models. In their haste, these organizations failed to prioritize security appropriately, and have created many blind spots and security gaps that now expose their data, users, and systems to risks, and which attackers are actively seeking to exploit.

In a study Ponemon Institute conducted for ReliaQuest[1], more than half (54%) of enterprises surveyed said the adoption of cloud environments has created blind spots that make them vulnerable to a data breach. And according to the 2021 Cloud Security Report[2] from the International Information System Security Certification Consortium (ISC)[2], 96% of organizations are moderately to extremely concerned about the state of their cloud security. Many security teams now face the daunting challenge of trying to find and fix cloud security issues before they become — or invite — more serious problems.

Standing in the way of their success is a lack of visibility. The Ponemon study found that 60% of organizations lack integrated visibility into their cloud and on-premises solutions — and it's proving to be a significant obstacle to security teams implementing effective threat detection and investigation practices that could strengthen cloud security. An issue that dovetails into this challenge for many organizations, according to Ponemon's research, is the difficulty they face trying to integrate data sources so they can gain visibility across their multicloud and hybrid cloud deployments.

[1] Making Security Possible and Achieving a Risk-oriented Security Posture, Ponemon Institute research report sponsored by ReliaQuest, available at: https://www.reliaquest.com/ponemon-institute-research-report/

[2] 2021 Cloud Security Report, (ISC)[2], 2021, available at: https://www.isc2.org/Landing/cloud-security-report

Securing cloud environments is indeed more difficult when organizations work with multiple providers and maintain hybrid cloud environments. Most enterprises today rely on a mix of cloud platforms and services like Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, and Software-as-a-Service (SaaS) applications to support their everyday operations. These multicloud environments are very complex — and managing them is an onerous task for IT and security teams.

60%

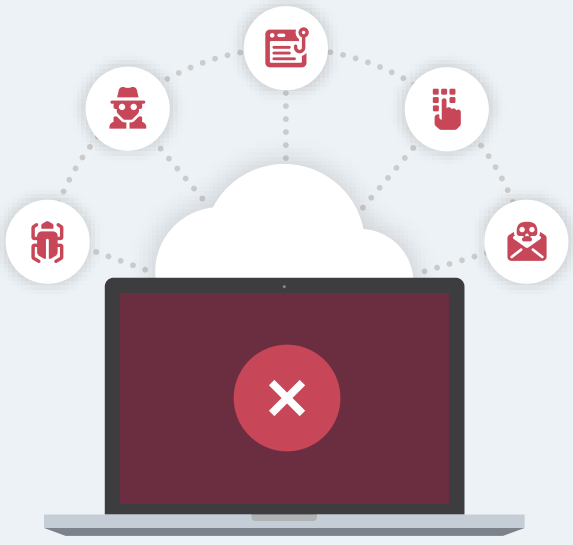
of organizations lack integrated visibility into their cloud and on-premises solutions.

Source: Making Security Possible, 2021, Ponemon Institute

AS CLOUD ADOPTION EXPANDS, SO DOES THE ATTACK SURFACE

Despite these challenges, many organizations are moving full-steam ahead with plans to widen their embrace of cloud — because they must. Some organizations seek to build on their success using cloud resources and services during the COVID-19 pandemic not only to survive, but also to seize new opportunities and grow. Meanwhile, other organizations are racing to catch up with their more digitally mature peers after realizing their digital transformation inertia prior to the crisis has prevented them from being agile and resilient. And now, that lack of digital maturity threatens their ability to compete effectively in the post-pandemic recovery.

Research for the 2021 Cloud Security Report[2] from the (ISC)[2] found that more than half (55%) of organizations are likely or very likely to deploy a new cloud security solution in the coming year.



And Gartner predicts that by 2026, public cloud spending will exceed 45% of all enterprise IT spending — up from less than 17% in 2021.

While the pressure is on to implement more cloud resources and services, organizations aren't likely to see a positive return on their investment if they suffer a major security incident. And the risk of that happening is very high if cloud security is weak. According to research conducted by IDC, 98% of companies have experienced a cloud data breach in the past 18 months.

So, what are the cloud security risks that could lead to a costly data breach or other security incident for an organization? Following are seven key threat types related to cloud environments:

MISCONFIGURATIONS

Misconfigurations expand the attack surface and leave cloud resources vulnerable to attack

PUBLICLY ACCESSIBLE APIS

These APIs can be lucrative targets for attackers, and can result in account takeovers, carding attacks, fake logins, and more.

11%

of organizations report that their IT security team has high confidence in the security of their multicloud and hybrid cloud environments.

Source: Making Security Possible, 2021, Ponemon Institute

DATA EXFILTRATION

This is a top concern for organizations that handle personally identifiable information (PII), personal health information (PHI), and payment card information (PCI) data

INFILTRATION

Attackers will hijack accounts and infiltrate networks or systems to attempt to penetrate an organization's cloud services.

DISRUPTION

Malicious actors will disrupt critical services or applications using either distributed denial of service (DDoS), ransomware, or other attack techniques.

EXPLOITATION

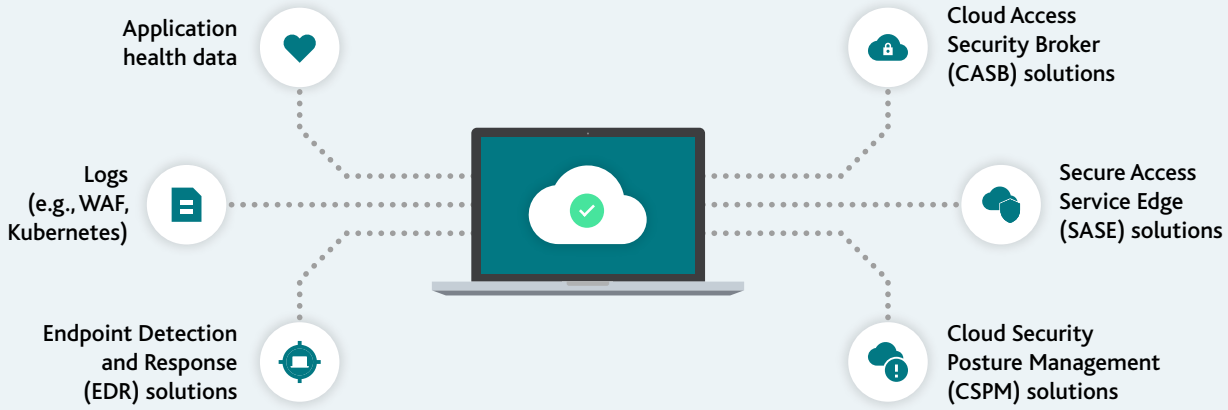
These attack methods include metadata service abuse, resource hijacking, backdoors, and more.

ABNORMAL AUTHENTICATION SCENARIOS

These scenarios, often seen with SaaS applications, include the compromise of OAuth applications or user accounts, which can lead to data compromise.

Why a Holistic View of Cloud Security Is a Must

Organizations can't manage those various threat types effectively, or migrate to the cloud with confidence, without a holistic view of all their cloud resources and services. Cloud security also requires organizations to consider how best to secure and monitor every cloud environment, application or service the business uses. Typically, that involves employing an array of tools from various vendors and data from different resources, such as:



To respond efficiently and effectively to relevant alerts and other intelligence from these tools and resources, security teams must be able to consolidate disparate pools of data into one place for monitoring, detection and response. They also require the ability to inject telemetry from cloud-specific tools and unify it with data from traditional sources to develop that one, cohesive, holistic picture of threats across all tools and attack surfaces.

Also, because threats are changing and becoming more complex all the time — as are the cloud environments themselves — security teams are under constant pressure to configure and reconfigure critical controls and secure architecture practices so they can address risks and quickly detect attcks. And they need to monitor these environments with speed and efficiency, 24/7/365.

Obviously, organizations need help to make all of that happen — but it won't come from their cloud providers. Many organizations have been taken off guard by the shared responsibility "surprise" — when they discover that their cloud vendors don't provide the visibility and monitoring of cloud environments they had expected (i.e., assumed). They didn't fully understand, until after moving critical infrastructure to the public cloud, that cloud security is a shared responsibility between providers and their customers. And that model can vary by provider and service type.

ReliaQuest GreyMatter helps organizations transcend these challenges by providing the visibility into the cloud they need to build a best-in-class cloud security program, no matter whether they're using AWS, Microsoft Azure, GCP, or all of the above.

Eliminating Cloud Security Blind Spots with ReliaQuest GreyMatter

GreyMatter is a cloud-native Open XDR platform that unifies telemetry from various sources across your cloud environment, eliminating any blind spots and providing singular visibility that unifies data from across on-premises and public cloud resources.

GreyMatter also brings together data from security information and management (SIEM), EDR, CASB, threat intelligence solutions, and other on-premises technologies to enrich investigations and drive fast response for proactive protection. Importantly, you benefit from the "network effect" by having access to learnings from across the ReliaQuest GreyMatter customer base that you can apply to your instance.

With GreyMatter, you can migrate to the cloud more confidently and securely with enhanced ability to pinpoint and address potential threats that can undermine the security of the cloud resources and services your organization relies on, including:

AMAZON WEB SERVICES (AWS)

GreyMatter processes telemetry from any AWS resource or activity, including CloudTrail, GuardDuty, CloudWatch, S3, EC2, Athena, Shield, Route 53, VPC flow data, AWS Elastic Load, AWS Security Hub, Inspector, CloudFront, Elastic Kubernetes, Amazon Workspaces, and Amazon API Gateway. The platform helps security teams quickly identify and respond to threats such as:

- **Misconfigurations:** AWS user added outside organization, AWS flow logs removed, AWS user added to a privileged group
- **Publicly accessible APIs:** S3 bucket made publicly accessible, API unauthorized action attempts, sensitive cloud bucket permissions modified
- **Data exfiltration:** EC2 instance assigned public IP, compute VPN tunnel created
- **Infiltration:** AWS API identity and access management (IAM) key created for other account, AWS user enumeration, AWS API activity for inactive user, API service account impersonation
- **Disruption:** cryptominer behavior on container, AWS config logging disruption
- **Exploitation:** modification of cloud instance access keys or IAM policy, AWS root account use

GOOGLE CLOUD PLATFORM (GCP)

GreyMatter processes telemetry from any GCP resource or activity, including but not limited to GCP Storage, Google Workspace, Cloud IAM, Workspace, API Gateway, Resource Manager, Compute Engine instance (VM), VPC service controls, Security Command Center, Ops agent, CASB (third-party), and WAF. It helps security teams to stay on top of:

- **Misconfigurations:** anomalous grant of IAM permissions, sensitive role granted to group with external member
- **Publicly accessible APIs:** GCP Service Account used for key and/or instance reconnaissance, workspace admin role assignments, domains added to workspace trusted domain

MICROSOFT AZURE

GreyMatter can process telemetry from any Azure resource or activity, including Microsoft 365 Defender suite, Azure Defender suite, Azure Sentinel, Azure Defender for Servers, Azure Monitor (including platform logs from Azure services), Azure AD, Azure Key Vault, and Microsoft Cloud App Security. The platform enables security teams to get ahead of and respond quickly to threats such as:

- **Misconfigurations:** service disabled, new log exclusions created, email forwarding rule to external domain created
- **Publicly accessible APIs:** Azure Blob made publicly accessible, SharePoint file shared outside of the organization, cloud ACL configured to allow all
- **Data exfiltration:** consent granted to suspicious application, data exfiltration to unsanctioned applications
- **Infiltration:** cloud brute-force password spraying, anonymous user SharePoint access
- **Disruption:** DNS record modified or added, startup script added to instance, abnormal multiple VMs created
- **Exploitation:** INGRESS firewall rule created from non-rfc1918 address, API call from threat host, anomalous API user agent

SAAS APPLICATIONS

GreyMatter processes telemetry from any SaaS resource or activity, including identity and access control, privileged and non-privileged access, audit and security logs, API access and activity, mobile access, location-based access, and changes to admin controls. The platform helps security teams uncover and mitigate threats such as:

- **Abnormal authentication scenarios:** activity from an infrequently seen country, impossible travel scenarios, activity from a terminated or disabled user
- **Misconfigurations:** data containing sensitive information (e.g., PII) observed, addition of credential to an OAuth app, email forwarding rule added (office app), shared file/folder publication (office app)
- **Data exfiltration:** suspicious impersonated activity, mass download of data, data accessed from personal account (office app)
- **Infiltration:** malicious OAuth app consent, suspicious OAuth app observed downloading files

Knowledge Is Power—So Is Visibility

No matter where your organization is with cloud adoption or digital transformation, it's essential that you take steps to securely migrate to and protect every cloud environment, private or public. More cybercriminals are targeting these environments, which is no surprise given that 50% of all corporate data is now stored in the cloud.[6] And these actors are eager to take advantage of any security blind spot or gap they may discover. So, your security teams need to find those vulnerabilities before they do.

With the ReliaQuest GreyMatter platform, your organization can:

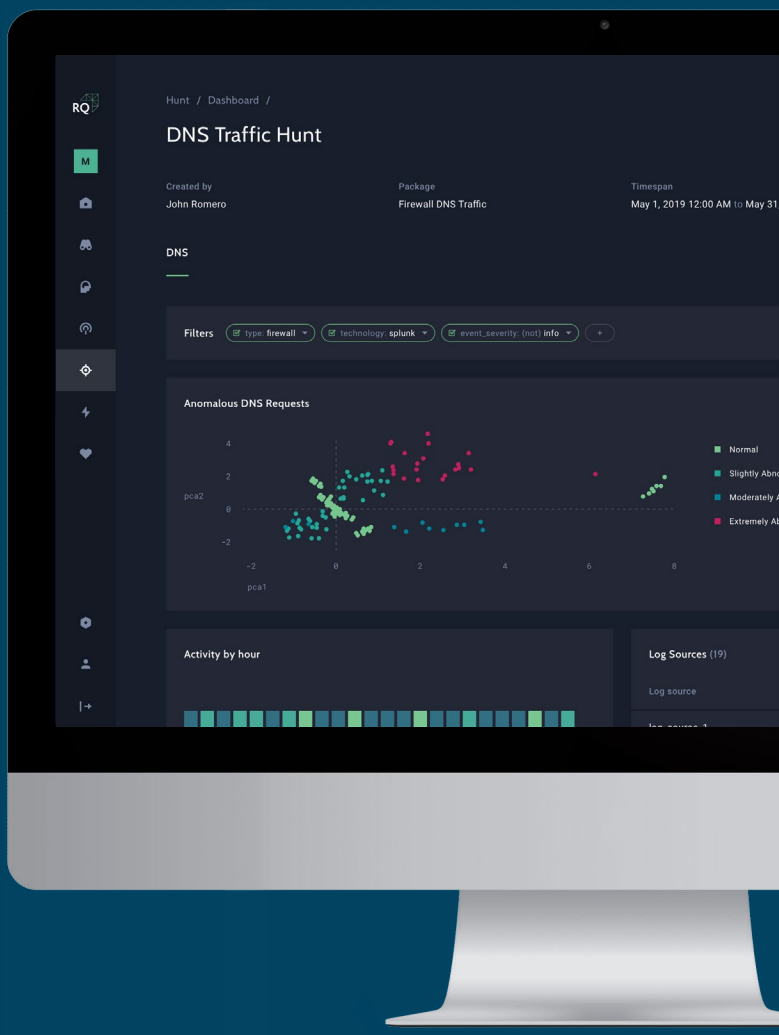
- Gain singular visibility across all of your cloud environments for better security
- Use continuously updated detection content and indicators of compromise (IOCs) to drive and support more proactive security measures
- Improve your overall security posture with actionable metrics and maps to industry-standard frameworks
- Benefit from the "network effect," with access to learnings from across the GreyMatter customer base that you can apply to your instance
- Streamline and unify security operations across your cloud and on-premises IT infrastructure
- Ensure confidence in threat detections with managed integrations and data integrity

This primer on cloud security may have offered only one lesson:
Without visibility, cloud security is impossible. But we're confident it's all the core knowledge you need to start making targeted investments and improvements that will reduce your exposure to cloud risks and threats.

[6] "Share of corporate data stored in the cloud in organizations worldwide from 2015 to 2021," Statista, July 30, 2021: https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/

About ReliaQuest

ReliaQuest, a global leader in Open XDR-as-a-Service, is known for being the force multiplier for security operations teams. ReliaQuest GreyMatter is a cloud-native Open XDR platform that brings together telemetry from any security and business solution, whether on-premises or in one or multiple clouds, to unify detection, investigation, response, and resilience. ReliaQuest combines the power of technology and 24/7/365 security expertise to give organizations the visibility and coverage they require to make cybersecurity programs more effective.



Hundreds of Fortune 1000 organizations trust ReliaQuest GreyMatter to operationalize security investments, ensuring teams focus on the right problems while closing visibility and capability gaps to proactively manage risk and accelerate initiatives for the business. ReliaQuest is a private company headquartered in Tampa, Fla., with multiple global locations.

FOR MORE INFORMATION, VISIT:
www.reliaquest.com or contact us.

RELIAQUEST
Make Security Possible™

(800) 925-2159 www.reliaquest.com info@reliaquest.com