ExtraHop

SOLUTION BRIEF

4 Steps to Secure Cloud Migration

The cloud has fundamentally changed the way organizations innovate. The scale and elasticity of cloud resources supercharges agile development, accelerating application development, iteration, and delivery. The cloud also enables organizations to spin resources up and down as needed, rather than forcing them to anticipate those needs in advance.

STEP 1:
Align NetSecOps to Work Better Together

STEP 2:
Perform a Situational Assessment and Identify Your Databases

STEP 3:
Maintain Security During Migration

STEP 4:
Security & Operations Post-Migration

With ExtraHop, you can migrate to the cloud with speed and confidence by taking advantage of key Reveal(x) 360 capabilities:

- Continuous security powered by cloud-scale artificial intelligence
- Discover and classify every asset in your environment
- Identify MS-SQL servers, SAP, Oracle databases, and more to help plan your migration strategy
- Network intelligence from across your hybrid attack surface

Reveal(x) 360 enables you to detect and hunt advanced threats as well as conduct fast forensic investigations designed to ensure you keep migration projects on track and on budget.

STEP 1:
ALIGN NETSECOPS TO WORK BETTER TOGETHER

Ensuring the workloads you migrate to the cloud are still secure without impacting performance is a challenge for many organizations. Traditionally, security and operations teams have been siloed, with neither side having much insight into what the other side is doing. That lack of alignment can lead to waste through duplicated instrumentation and tool sprawl, redundant procurement, and increased overhead for the enterprise.

With Reveal(x) 360, SecOps and IT Ops teams can work together and avoid many of the pitfalls that slow down or stall migration projects. Reveal(x) 360 uses a common data source that both security and IT Ops can leverage for insight to help ensure that migrated workloads are secure and perform as expected, despite the complexity that explosive growth to the cloud can cause. This enables organizations to modernize operations and further digitize transactions with speed and confidence.

STEP 2:
PERFORM A SITUATIONAL ASSESSMENT AND IDENTIFY YOUR DATABASES

Before you can securely migrate to the cloud, you need to have a complete inventory of on-premises workloads. But that's only the beginning. Understanding the complex relationships among those assets is key to ensuring a safe, successful migration. Out of the box, Reveal(x) 360 lights up your environment with continuous, automated asset discovery, classification, and mapping. You can identify MS-SQL servers and determine which if any databases, including Oracle DB, are up for end-of-life.

With Reveal(x) 360, you can monitor roundtrip time and troubleshoot database errors and slow applications. Reveal(x) 360 dramatically expands your visibility into and contextual awareness of workload architecture, including load balancers, app and database servers, storage, and much more by decoding more than 70 enterprise protocols and leveraging 5000 metrics. Armed with this information, you can now begin creating your migration plan. Most organizations choose one or more of the following options:

- **Rehost:** Also known as lift and shift, this method enables you to move applications to the cloud without optimizing for the cloud. Rehosting is the least labor-intensive method for migration.
- **Replatform:** This method, also known as lift and reshape, involves moving on-premises services. One example would be lifting and reshaping an on-premises database to a cloud-hosted database like Amazon DynamoDB.
- **Refactor:** Also referred to as re-architecting, this method requires a complete redesign of application features to take advantage of existing cloud features. One example is refactoring an application to use containerized architecture in the cloud.
- **Relocate:** This method for migrating virtual machines without changing their structure is similar to rehosting. Relocating is fast, but it can make it more difficult to modernize applications and take advantage of certain cloud services.

No matter which migration plan you choose, Reveal(x) 360 can improve visibility and security. Cloud migration is continuous, iterative, and needs to happen on strict timelines to keep digital transformation projects on track. By harnessing the power of network data in hybrid and multicloud environments, Reveal(x) 360 helps ensure that you hit your deadlines and stay on budget.

STEP 3:
MAINTAIN SECURITY DURING MIGRATION

Having an up-to-the-moment understanding of what's been migrated and what still needs to be moved to the cloud is key to maintaining security during digital transformation. As soon as an asset comes online—regardless of whether it's in the cloud or on premises—Reveal(x) 360 discovers it and begins monitoring its behavior to provide security and performance insights at scale.

Refactoring, replatforming, and even rehosting create opportunity for misconfiguration in two key areas.

- **New system components:** When creating new infrastructure, adversaries can abuse misconfigurations and use them to find new places to hide.
- **How new system components communicate:** This type of misconfiguration can expose data more broadly than business needs dictate or regulations allow.

Absent NDR, adopting cloud-native architectures during migration results in a reduction in visibility and situational awareness because:

- **Cloud workloads** are more ephemeral than those in on-premises environments, especially in autoscaling and containerization cases. Reveal(x) 360 automatically analyzes ephemeral workloads, ensuring you understand what is happening in ephemeral environments.
- **Cloud-native telemetry** sources are log-based, which is helpful for post-mortem investigations and root-cause analyses. However, logs are not suited to real-time behavioral detection and response. Reveal(x) 360's ability to detect threats and inefficiencies as they happen shortens and improves the feedback loop to security and DevOps teams, empowering them to remediate with certainty through manual or automated intervention.

“

As soon as an asset comes online—regardless of whether it's in the cloud or on premises—Reveal(x) 360 discovers it and begins monitoring its behavior to provide security and performance insights at scale.

STEP 4:
SECURITY & OPERATIONS POST-MIGRATION

Now that you're in the cloud, the size of your attack surface has likely doubled, and you need to ensure that your environment and assets are secure and performing as expected. Cloud elasticity means that workloads can be spun up or down on demand, which can lead to observability gaps. Plus, you may still have assets operating in an on-premises environment, which can cause gaps. With Reveal(x) 360, security teams can monitor every workload, everywhere, and respond to advanced threats anywhere from a single management pane. Reveal(x) 360 is always on, always monitoring and analyzing network data, and can be quickly installed without the need for agents, providing a frictionless approach to help you stop breaches up to 84% faster and achieve your objectives in the cloud. Additionally, you can prove out performance after migration and provide stakeholders with accurate performance-based SLAs.

Attack Surface Coverage: Regardless of whether you're 100% in the cloud or leveraging a hybrid deployment, Reveal(x) 360 provides unified observability across environments. The same continuous, automated asset discovery, classification, and mapping Reveal(x) 360 supplied before and during your transformation project continues after you've successfully migrated. With Layer 7 visibility and out-of-band SSL/TLS 1.3 decryption at line rate, Reveal(x) 360 eliminates blindspots without introducing security risk or latency. Real-time stream processing for up to 100 Gbps of traffic and up to 1 million IP addresses per sensor ensures you're always up to date about what's happening in hybrid, multicloud, and edge environments. Integrations with CSP-native traffic mirroring features eliminates the need for agents, making Reveal(x) 360 highly elastic and scalable. You can also intelligently respond to incidents through Reveal(x) 360 or via integrations with automated response platforms.

Investigation and Threat Hunting: With a comprehensive understanding of your assets, you'll have the awareness you need to secure your entire environment and deliver safe, reliable user experiences. By combining cloud-scale machine learning with signature-based detections, high-fidelity alerts, and one-click investigation workflows, Reveal(x) 360 enables you to quickly answer complex security and performance questions about specific workloads and cloud zones. With access to the Reveal(x) 360 cloud-hosted record store with 90-day lookback, you will gain access to details that go beyond summary metrics to provide granular, in-depth information.

Network Forensics: Organizations in the cloud must often rely on network flow logs to investigate security incidents and performance issues. While flow data can tell you that two assets have communicated, it cannot provide insight into the conversation. Other tools focus on reactive incident response, meaning users can only go back in time to find packets if a detection or event occurs. Reveal(x) 360 provides continuous packet capture (PCAP), which allows for extended lookback and deep forensic investigations accessible immediately and not dependent on a detection firing. Having always-on incident response allows you to identify advanced attacks like SUNBURST when reactive incident response cannot. And, this all can be done without the need for packet forwarders or agents by integrating with CSP-native packet mirroring features. With Reveal(x) 360, security teams can start and complete forensic investigations from a single, cloud-native solution. Armed with full PCAP—the ultimate source of truth in the cloud—you can now investigate incidents with speed and confidence.

To experience Reveal(x) 360 for yourself, start the live online demo. You can stop a SUNBURST attack, find threats in a real cloud environment, or investigate a simulated attack unfolding in real time. You can also choose to explore the demo on your own. To try Reveal(x) 360 in your own cloud environment, request your free trial today.

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, uses cloud-scale AI to help enterprises detect and respond to advanced threats—before they can compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101