



Cloud (in)security:

Your guide to stronger
cloud security with NDR

In 2020, digital transformation across all sectors accelerated at lightning speed out of sheer necessity — including rapid migrations to the cloud. Now, as we take a breath after the storm and revisit those decisions, it's time to take another look at the fundamentals of cloud security for your IT infrastructure.

Once just a subchapter of a larger enterprise cybersecurity strategy, cloud security now is often the whole book. [IDG has found](#), for instance, that 92% of an organization's IT environment is at least somewhat in the cloud today. For the greater good of cybersecurity, everyone must ask,

“





HOW CAN CLOUD SECURITY RISE TO THE TOP OF THE AGENDA OF OR, AT THE VERY LEAST, CATCH UP IN THE POST-PANDEMIC ENTERPRISE?

”



This guide will help you take several steps back in order to move many steps forward on behalf of your enterprise's holistic efforts to embrace the business-centric promises of the cloud: scalability, agility, efficiency, improved user experiences, and reduced cost.

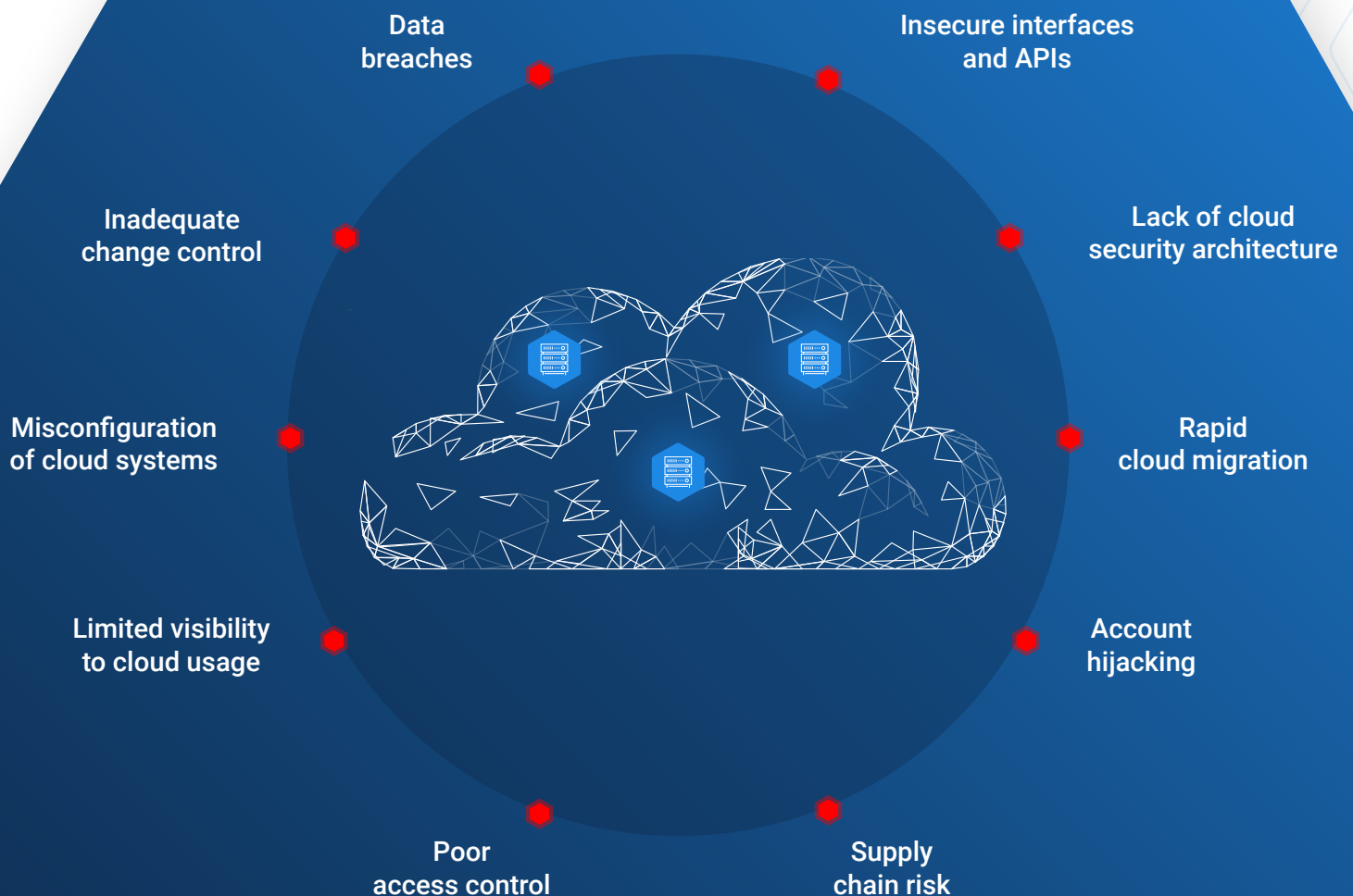
Specifically, you will learn the following:

-  Common cloud security vulnerabilities and challenges
-  How to achieve greater visibility in the cloud
-  What threat-sharing means for stronger cloud security
-  How to achieve defensive economies of scale through Collective Defense



What are the top cloud vulnerabilities?

Protecting data, applications, and assets in the cloud starts with understanding common vulnerabilities associated with cloud security. Although cloud service providers (CSPs) have gone to great lengths to secure cloud infrastructure, adversaries are taking advantage of security weak spots that enterprises themselves are responsible for tightening up (per the CSP's shared responsibility models), including misconfigurations, poor access control, and insecure APIs.









Tackling a top vulnerability: **misconfiguration**

In its [guidance to cloud security](#), the U.S. National Security Agency (NSA) lists the top four classes of cloud vulnerabilities as:

-  Misconfiguration
-  Poor access control
-  Shared tenancy vulnerabilities
-  Supply chain vulnerabilities

Misconfigurations and weak access controls, however, are just the gates at the cloud. It goes without saying that you can't achieve in-depth cloud security if you don't know what is in the cloud: complete visibility is critical. Network detection and response tools that leverage behavioral analytics provide this missing visibility.

IronNet partner **Unlimited Technology** advises a “RED PEN” approach to avoiding misconfigurations:

-  Restrict Access by least privilege
-  Encrypt all data at rest & flight
-  Disable cloud resources that are not needed
-  Prevent Access to privileged accounts
-  Ensure encryption keys are rotated
-  Need NDR and HBM for 100% visibility into Layer 2 and 3



Watch the “Cloud (in)security: Avoiding common cloud misconfigurations” on-demand webinar.



Gaining better visibility in the cloud

What level of visibility in the cloud do you need? You should be able to answer these three questions at all times to ensure that you can see any anomalous activity in your cloud environment (whether public, private, hybrid, or multi-cloud):

1

What's on your network?

2

Who's on your network (i.e., are the right people accessing)?

3

What's happening on your network?



To answer these questions successfully, you need to be able to see the raw network flows to and from the cloud. Although all CSPs offer logging and monitoring tools to capture a history of all API calls (e.g., the caller's identity, source IP address, and request parameters), only fine-tuned detection capabilities for determining anomalous behaviors within the network traffic will truly secure what's in the cloud.

Seeing the truth in the traffic with NDR

Network detection and response (NDR) solutions driven by behavioral analytics enable you to see the truth in the traffic from network data, including both network logs and sensor-based traffic, closing the known visibility gap that plagues full-on cloud adoption.

With AWS and Azure integrations, for example, IronNet's [IronDefense](#) can access cloud logs to detect and analyze threats and provide anonymous, correlated context that no single enterprise would have on its own. This capability gives the enterprise the visibility it needs to take timely and relevant action on what they now are able to see with IronDefense, instead of being left in the dark.

Confusion about who is responsible for cloud security can lead to security gaps. **Remember this: the security “of the cloud” falls on the CSP’s shoulders, whereas the responsibility of securing assets and data “in the cloud” falls on the enterprise itself.** Armed with cloud analytics to spot anomalies on the network, enterprises — not the CSP — still must charge ahead with seizing this approach to fill this visibility gap as expected of the shared responsibilities models outlined by [AWS](#) and [Azure](#), for example.

 Understanding shared responsibility models

99%

of cloud security failures through 2025 are expected to be the customer's fault not the CSP's

GARTNER

Read more





Is the cloud more secure than on-prem?

With NDR that leverages behavioral analytics, you can actually boost visibility into your network activities – and potentially malicious behaviors – versus on-premise visibility. Behavioral analytics can reveal two types of visibility:

1

Visibility of user activity inside your cloud resources (that is, what users are doing)

2

Visibility of interactions between the machines in the cloud (both those within the enterprise's cloud space and those interacting outside the cloud), using approaches such as traffic mirroring

“

IT security practitioners are likely to turn to [NDR] to gain better visibility into their own cloud traffic. In fact, 80% of respondents noted their awareness that NDR technology can be applied to cloud traffic. Among those respondents, 48% see as its primary value the ability to detect threats and anomalies in real time.”
(EMA Cloud Research Report).



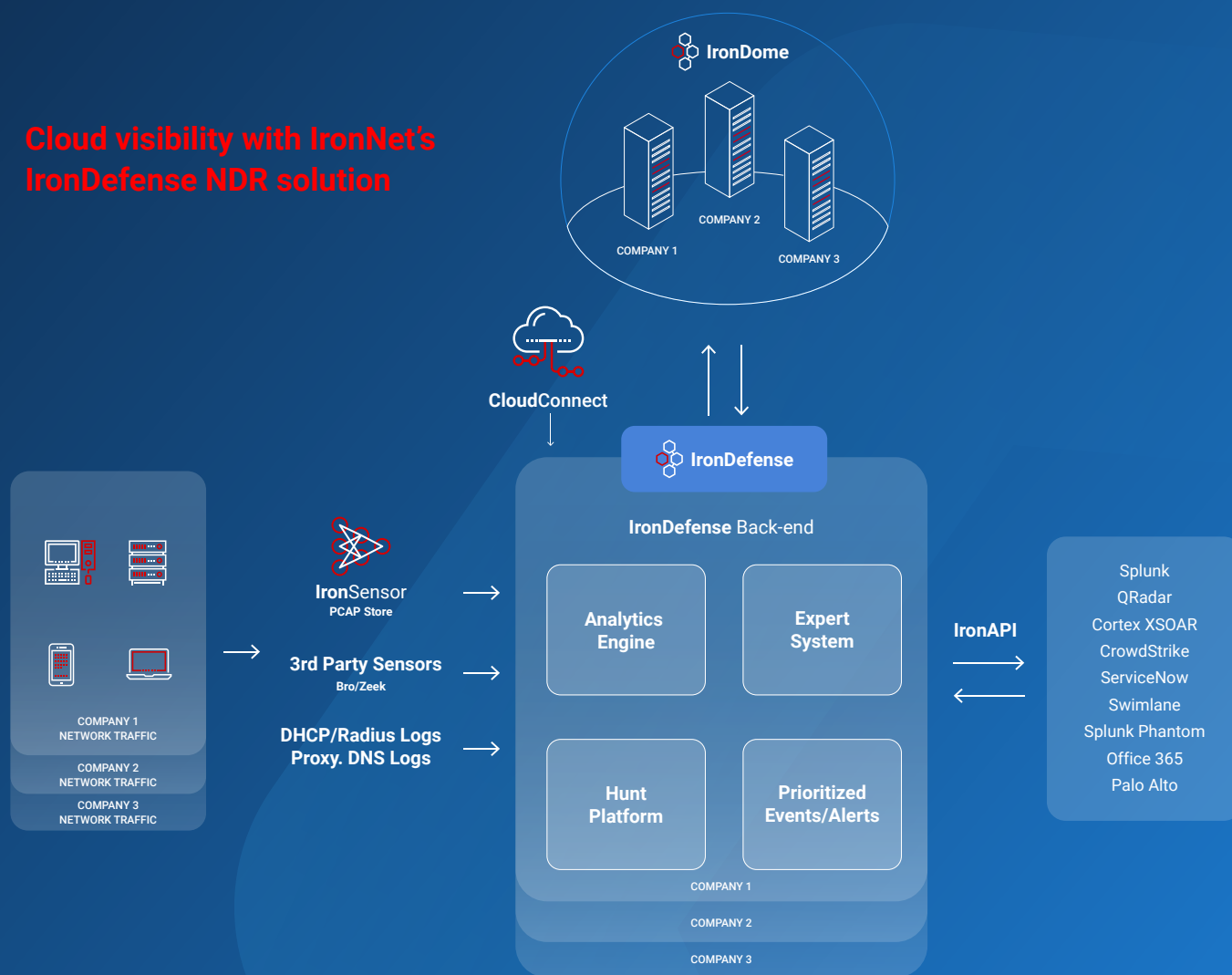
Read more



GAINING BETTER VISIBILITY IN THE CLOUD

Some would argue that the cloud is, in fact, more secure given that you can see only the machine-to-machine interactions with on-premise infrastructure. In cloud environments, by contrast, both logs (e.g., AWS VPC, Azure NSG) and sensors (AWS virtual sensor) enhance this visibility.

Cloud visibility with IronNet's IronDefense NDR solution



In the cloud, regardless of the provider, it is impossible for someone with access to your enterprise's account to secretly create something in your account. You have full control over anything created in the account (vs. someone sneaking into the building and installing a device in an on-prem data center). Because of the abstraction between you and CSP data centers, moreover, your enterprise would not be affected should an (highly unlikely) on-prem compromise hit the CSP data center.



Four tips for **enhancing** **cloud security**



Cloud security tip #1: **Set a baseline for normal**

It is crucial to set baselines around what constitutes normal network behavior to and from the cloud. Being able to get granular and understand what is truly moving around your network is the only way you are going to be able to set a baseline in order to catch out-of-place activity down the line such as potential data access and data leakage after cloud migration.

Armed with this baseline from logs, you can leverage network behavioral analytics to automatically audit this baseline on a regular basis to check and validate this ground level of truth. Threat hunting — informed by data both within and beyond the individual enterprise — adds another layer of validating potential anomalies against what you expect on the network. It is in this way that [Network Detection and Response solutions that leverage algorithms based on machine learning and hunt capabilities](#) and enrichments can amplify basic log-based cloud security controls.

2

Cloud security tip #2: **Invest in cloud-specific analytics**

Not always included in the CSPs' analytics platforms, cloud analytics can strengthen your cloud security posture even more. For example, the IronNet cloud analytics used in the [IronDefense](#) NDR solution can differentiate between bot traffic and human traffic, as well as detect suspicious human activity such as privilege escalation. Visibility of the raw traffic adds a layer to a defense-in-depth approach, eliminating the huge blind spot that deters many from embracing the benefits of cloud computing.



Superior behavioral detection for Microsoft Azure

IronDefense scales from small companies to Fortune100 companies to deliver unmatched behavioral detection across Azure, on-premise, or multi-cloud environments.



IronNet and AWS
working together to
improve cloud security

IronNet offers a set of CloudTrail Analytics that complement and enhance the offerings of Amazon GuardDuty account compromise analytics. GuardDuty offers a number of network traffic analytics that are only for the AWS instance, while IronNet focuses on increasing the enterprise's visibility into their enterprise network while offering an enhanced set of analytics through the IronDefense offering.

[Get the details](#)



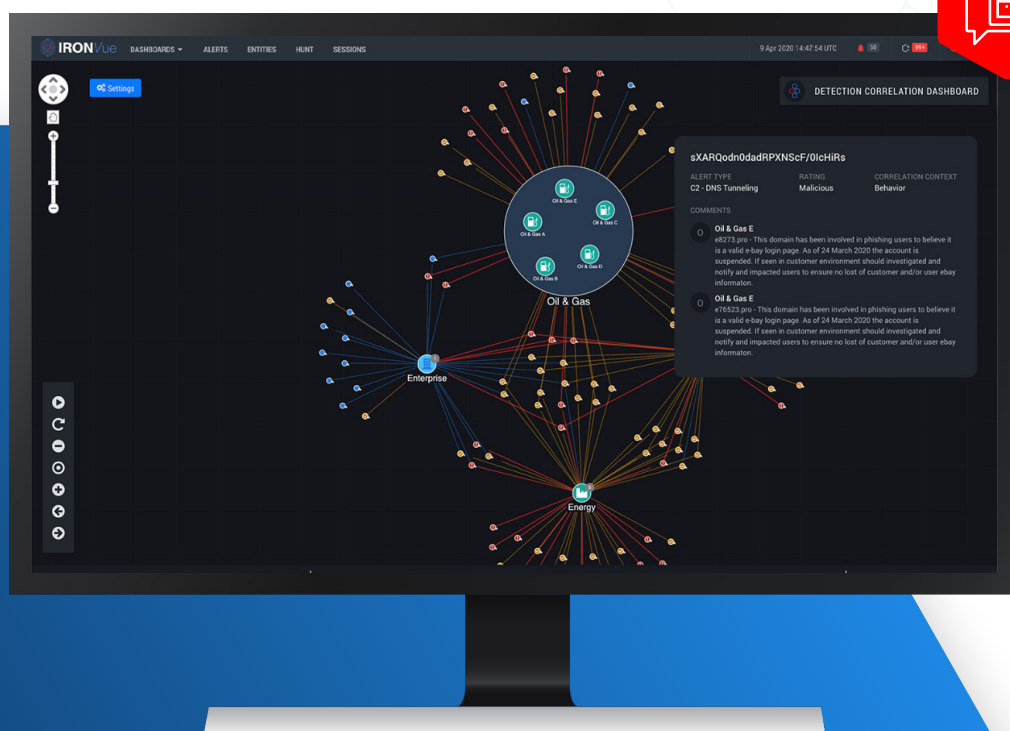
[Get the details](#)



3

Cloud security tip #3: **Improve your threat response with real-time threat sharing**

The visibility enabled by behavioral analytics can be expanded through real-time threat sharing. IronNet's [Collective Defense platform](#) builds a dynamic, comprehensive picture of the threat environment, much like radar for cyberspace, based on real-time, anonymized alert correlation across any participating member environments. These correlations are the basis of the dynamic threat picture that makes much greater visibility possible at any given time.



4

Cloud security tip #4: **Speed up response time with crowdsourced peer insights**

A Collective Defense approach allows community members to share threat context, prevalence, and expert commentary about how to triage and respond (much like Waze but for cyber). By banding together and working together with peers in real time, Collective Defense communities are better able to pool and optimize resources so they can achieve “defensive economies of scale.”

87%

**of organizations
willing to share
threat information
with industry peers**

To improve cloud security, most organizations that use threat intelligence feeds to identify and secure threats are open to sharing if doing so improves their own ability to detect cloud threats.

**EMA CLOUD
RESEARCH REPORT**




With cyber criminals and nation-state adversaries waiting to pounce on cloud security gaps, no company can afford what essentially was a “cross-our-fingers” approach to cloud security. Adapting

perimeter defenses and on-premise controls as a quick fix will never work for either an immediate or a long-term cybersecurity posture. Nor can companies rely on trusted, public cloud security providers to cover cloud security for them; that onus is one shared with the enterprise as explained by CSP shared responsibility models.

In other words, it is up to the enterprise — the CSP customer — to secure their environment in the cloud with the same level of vigilance as on-prem computing environments.

Collective Defense, powered by behavioral analytics, gives companies the missing visibility that has deterred many from taking the leap to the cloud, empowering them to approach their digital transformation with confidence, with cloud as a business enabler instead of the great unknown.

 **CLOUD WITH CONFIDENCE**

 **IronNet has partnered with AWS, Azure, and AWS GovCloud as part of its broader security ecosystem.**



[Learn more about our cloud partners](#) →

Connect with IronNet today to discover the power of Collective Defense informed by behavioral analytics.

IronNet.com →

