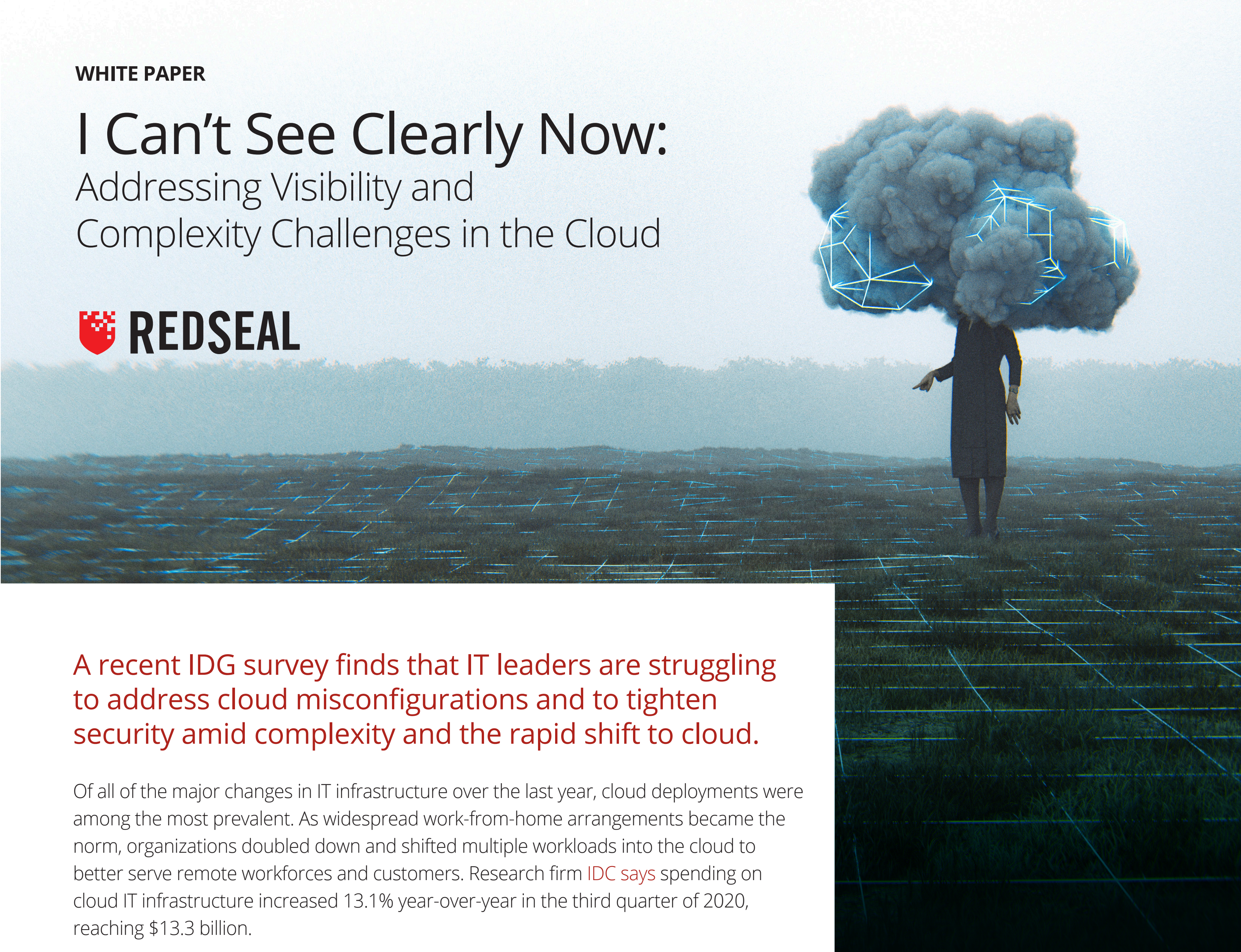
SPONSORED CONTENT CIO FROM IDG

WHITE PAPER

I Can't See Clearly Now:

Addressing Visibility and Complexity Challenges in the Cloud

REDSEAL



A recent IDG survey finds that IT leaders are struggling to address cloud misconfigurations and to tighten security amid complexity and the rapid shift to cloud.

Of all of the major changes in IT infrastructure over the last year, cloud deployments were among the most prevalent. As widespread work-from-home arrangements became the norm, organizations doubled down and shifted multiple workloads into the cloud to better serve remote workforces and customers. Research firm IDC says spending on cloud IT infrastructure increased 13.1% year-over-year in the third quarter of 2020, reaching $13.3 billion.

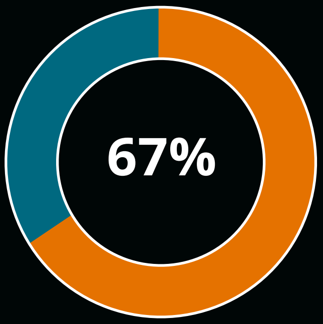
Those findings are echoed by a recent IDG survey of US-based IT and security leaders, in which 97% of respondents said their organizations' cloud deployments increased over the past 12 months.

Yet, these investments come with significant security challenges. Two-thirds (67%) cite difficulty keeping up with security best practices as attack surfaces change. Additionally, 57% report difficulty meeting external and internal compliance mandates.

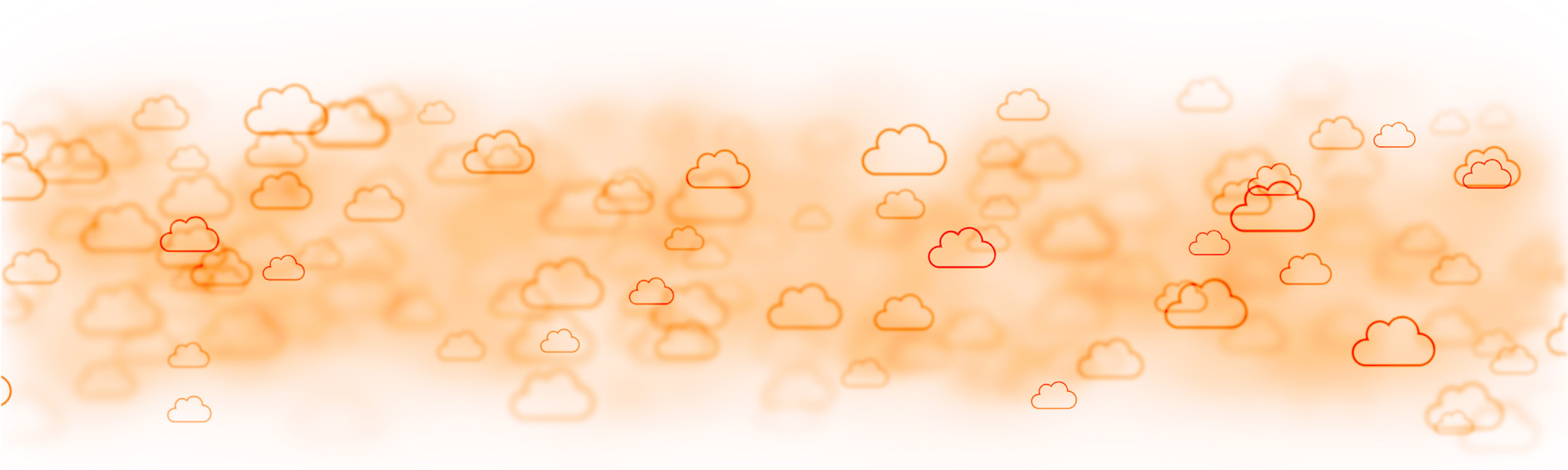
At the same time, the cloud is a favorite target of cybercriminals. Cloud breaches continue to grow and expose records and sensitive data. For example, cloud-based email servers are a top target. In fact, last year 96% of mail server breaches were cloud-based servers, according to the 2021 Verizon Data Breach Investigations Report.

What is getting in the way of optimal, secure cloud deployments? The IDG survey looked at the challenges presented by a lack of visibility into the attack surface in cloud deployments and the inhibitors to a more proactive approach to security. It also examined priorities for investment among IT leaders to address the pressing issues with cloud security.

67% of companies say they struggle to keep up with security best practices as attack surfaces change



Source: IDG



Taming Cloud Complexity Chaos

Over the last two years, amid widespread changes to work environments, many IT leaders were asked to do more with the cloud in order to meet the needs of both employees and customers—and they invested in cloud and the tools needed to manage them. But the shift from mostly on-premises tools to a mixture of cloud environments in a short amount of time has stressed IT teams and complicated their workloads. As a result, security for an organization's critical resources is now complex and difficult to manage—leading to anxiety around managing these high-stakes environments.

This complexity is largely due to the volume of tools needed to manage cloud environments. Survey respondents report they're using an average of seven security tools to protect critical resources. The most commonly used ones are related to network security policy management, firewalls, and security evaluations.

Even with all of these resources to manage their clouds, IT teams often rely on manual processes to defend against automated misconfiguration threats. Most respondents (85%) report that at least 25% of their cloud management workloads (e.g., cloud configurations, updates, and changes) consist of manual processes.

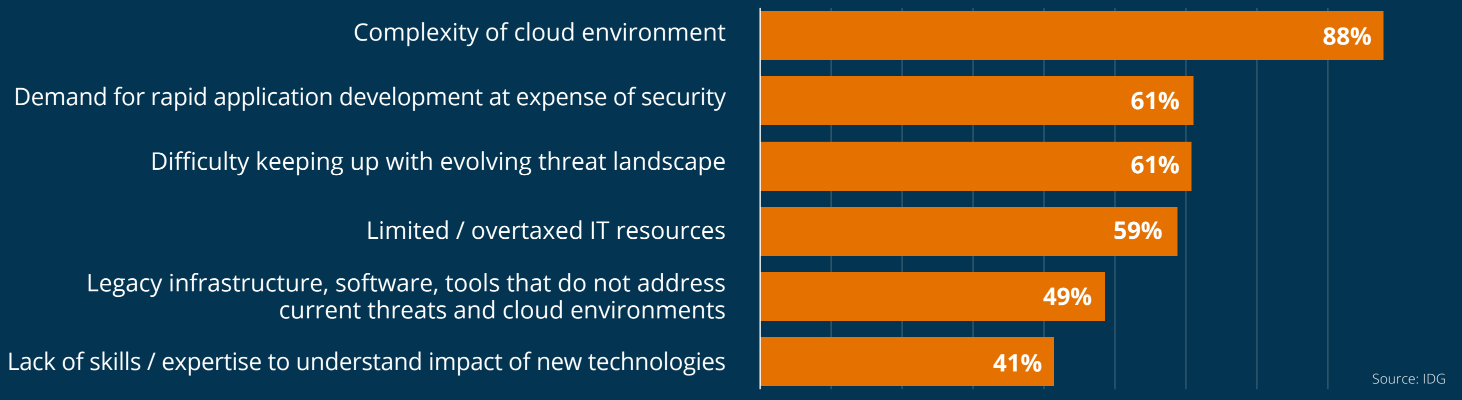
Yet, an overreliance on manual approaches to managing cloud misconfiguration can open the door to other problems. Chief among those concerns is human error in missing or mis-categorizing critical misconfigurations.

Misconfigurations can lead to vulnerabilities and cloud security risks. According to the NSA, cloud misconfiguration is the top risk in a cloud security environment. These gaps can lead to data breaches or other types of attacks in which a bad actor takes advantage of a misconfiguration to access corporate systems.

Unfortunately, getting to a more secure place in the cloud may seem out of reach for many IT teams. The survey finds that the complexity of existing cloud environments is inhibiting a more proactive cloud security approach at 88% of organizations (see Figure 1).

Simply put, just managing an overwhelming complicated cloud infrastructure means staying on top of threats and misconfigurations, which is nearly impossible under the current circumstances. What teams need is an automated approach to identifying misconfigurations.

Figure 1. Challenges That Inhibit a Proactive Cloud Security Approach



Source: IDG

Visibility Challenges Strain Security Efforts

As a result of complexity in cloud deployments, true visibility is also a challenge. Without insights into the infrastructure stack, IT leaders are hard-pressed to secure what they can't see. All of the IDG respondents said that gaining visibility into the entire attack surface is a problem, and 89% said it is highly challenging.

To accurately identify and locate assets that have been unintentionally exposed to the internet, the ability to bring data together from various environments into one comprehensive, dynamic visualization is essential.

IT teams also need the ability to confirm which vulnerabilities in the cloud pose the most risk so they can be remediated first. In fact, the survey finds when considering cloud security investments, 100% of respondents place critical or high importance on the ability to prioritize resource vulnerabilities based on risk.

In addition, a significant emphasis is placed on the ability to:

- Ensure cloud deployments meet security standards (99%)
- Verify compliance with security policies in real-time (96%)
- Locate resources that are unintentionally exposed to the internet (87%)

True visibility means teams can verify that network devices and cloud environments meet security best practices, validate cloud network segmentation policies, and continuously monitor compliance with internal policies and external regulations.

However, a majority of respondents (89%) indicate their organizations are lacking some visibility into potential vulnerabilities across physical and cloud environments. They are flying blind in a complex environment and have a significant gap in understanding exactly where they are exposed.

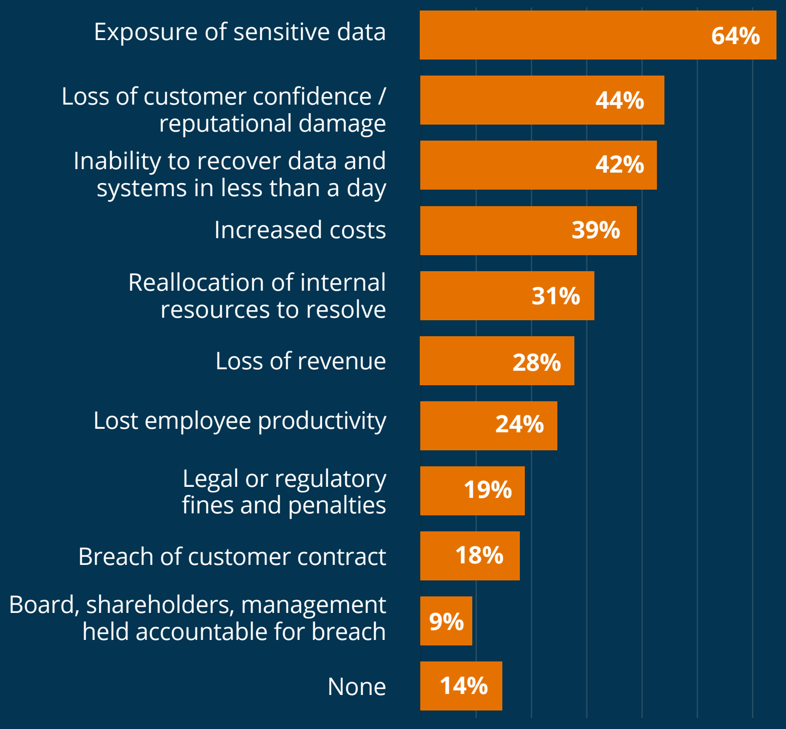
Crisis of Confidence: How Lack of Visibility Impacts IT Teams

The complexity and lack of visibility measurably affect IT leaders' confidence in their cloud deployments. They express a clear concern that critical resources will be impacted, and sensitive data inadvertently exposed, as a result of cloud misconfigurations. The survey results reveal current investments are not working when it comes to security and management in the cloud. Just 13% report IT security investments are well-aligned with the environments in which they operate; 87% report adjustments need to be made.

This lack of confidence in current cloud investments can be seen in the obvious level of concern among IT teams when it comes to the potential fallout of misconfigured cloud infrastructure, such as data leaks and breaches. Nine in 10 respondents (93%) are highly concerned about the potential impact of cloud misconfigurations.

Nearly two-thirds (64%) report that sensitive data has been exposed as a result of cloud misconfigurations. Respondents indicate their organizations have suffered an average of 3 negative effects resulting from cloud misconfigurations.

Figure 2. The Effects of Cloud Misconfigurations



Source: IDG

The Liability in Cloud Vulnerability

Most IT and security teams have several objectives: to keep business running; to enable the company to innovate and move forward; and when it comes to risk mitigation, to protect critical assets and keep the company secure.

The IDG survey found that IT leaders are concerned about the current status of cloud deployments in their environment, and most want to make investments that better align tools with visibility and simplicity. As they look to the future and consider priorities in the next year, nine in 10 survey respondents (91%) report their organizations are seeking a more comprehensive cloud security solution. The message is obvious: Cloud isn't just a focus for investment, it is an essential area that needs attention immediately.

What are IT and security leaders prioritizing when they evaluate solutions? With the rapid-paced adoption of container technology, 75% of organizations say Kubernetes security is a critical or very important priority. The ability to analyze Kubernetes configurations gives security teams the answers to key questions—such as whether there are overly permissive user and service accounts, if there are services exposed outside the cluster, or nodes are exposed to the internet.

The results make clear that security is increasingly seeking to collaborate with devops throughout the software development lifecycle (SDL) to learn the basics of containerized applications and define policies that ensure a stronger security posture.

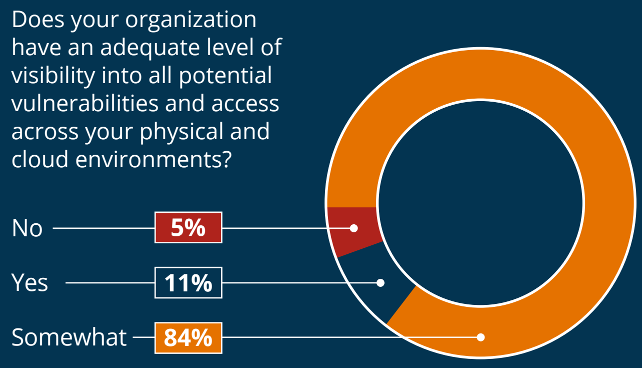
Securing Today's Cloud Environments

Better visibility is now critical to keep IT teams on top of what they need to know before an attack or breach occurs. And only with a strategy informed by risk-based exposure can security teams ensure the most important gaps are identified and remediated.

IT teams require resources that will keep their organizations from missing the exposed critical resources they are working so hard to protect, and that can help inform them about where to prioritize remediation. Unfortunately, traditional security tools can't solve the ongoing challenges with managing and securing today's cloud environments.

A modern cloud strategy requires automation to handle cloud scale and complexity.

Figure 3. Visibility Into Vulnerabilities



Does your organization have an adequate level of visibility into all potential vulnerabilities and access across your physical and cloud environments?

RedSeal has spent years helping organizations with their cloud solutions and deployments.

Visit **www.redseal.net** to learn more about aligning your cloud investments with your security and IT priorities.

ABOUT REDSEAL (redseal.net)

RedSeal — through its cloud security solution and professional services — helps government agencies and Global 2000 companies measurably reduce their cyber risk and show where their resources are exposed to the internet.

Only RedSeal's award-winning cloud security solution can bring all network environments– public clouds (AWS, Microsoft Azure, Google Cloud Platform and Oracle Cloud), private clouds, and on premises — into one comprehensive, dynamic visualization. RedSeal verifies that networks align with security best practices; validates network segmentation policies; and continuously monitors compliance with policies and regulations. It also prioritizes mitigation based on each vulnerability's associated risk. The company is based in San Jose, California.

REDSEAL
1600 Technology Drive, 4th Floor, San Jose, CA 95110
+1 408 641 2200 | 888 845 8169 | redseal.net | info@redseal.net
November 2021