How to Ensure Data Privacy in Public Clouds

The trend of enterprises moving applications, data and infrastructure to public clouds is unrelenting. Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform and a variety of other service providers are all becoming critical hosting providers for organizations worldwide (see Figure 1). The transition is a strategic move by companies to transform infrastructure operations, improve the customer experience and reduce costs.

But this transition also leads to an increased security "footprint" that must be safeguarded by an organization's cybersecurity team. Spreading data across multiple hosting centers complicates DDoS mitigation strategies, leading to seams between these clouds that modern cybercriminals are quick to exploit. Radware's annual global industry survey garnered responses from hundreds of C-level executives worldwide to understand the impact that cloud computing is having on organizations and to identify best practices and strategies to keep your organization's most prized digital assets secure.

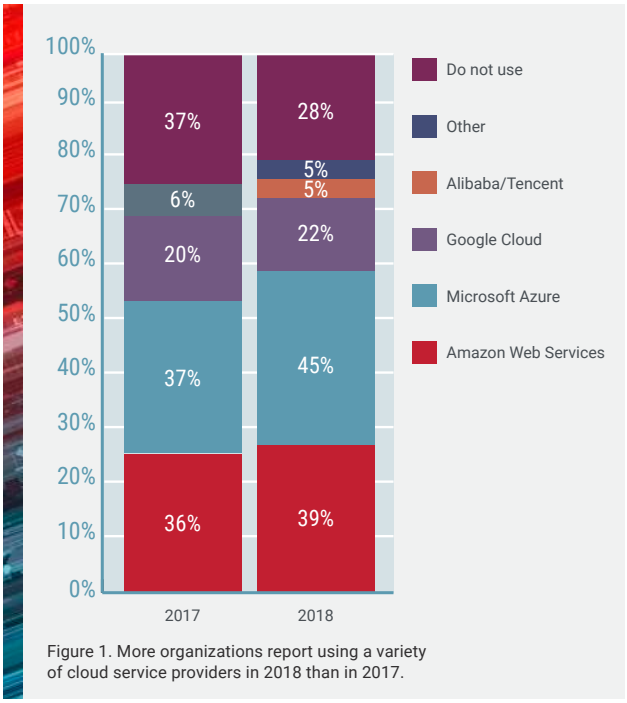


Figure 1. More organizations report using a variety of cloud service providers in 2018 than in 2017.

Using Public Cloud Providers	2018
Yes	**70%**
Yes, customized	29%
Yes, but I handle some aspects	22%
Yes, their default setting	19%
Our IT handles selection, implementation and configuration	23%
I rely on a local cloud provider for security management	5%
Other	2%

Figure 2. Reliance on public cloud infrastructure providers to secure cloud applications.

Most enterprises spread data and applications across multiple cloud providers, typically referred to as a multicloud approach. While it is in the best interest of public cloud providers to offer network security as part of their service offerings, every public cloud provider utilizes different hardware and software security policies, methods and mechanisms, creating a challenge for the enterprise to maintain the exact same policy and configuration across all infrastructures. Public cloud providers typically meet basic security standards in an effort to standardize how they monitor and mitigate threats across their entire customer base. Seventy percent of organizations reported using public cloud providers with varied approaches to security management (see Figure 2).

Moreover, enterprises typically prefer neutral security vendors instead of overrelying on public cloud vendors to protect their workloads. As the multicloud approach expands, it is important to centralize all security aspects.

When Your Inside Is Out, Your Outside Is In

Moving workloads to publicly hosted environments leads to new threats, previously unknown in the world of premise-based computing. Computing resources hosted inside an organization's perimeter are more easily controlled. Administrators have immediate physical access, and the workload's surface exposure to insider threats is limited.

When those same resources are moved to the public cloud, they are no longer under the direct control of the organization. Administrators no longer have physical access to their workloads. Even the

most sensitive configurations must be done from afar via remote connections. Putting internal resources in the outside world results in a far larger attack surface with long, undefined boundaries of the security perimeter.

In other words, when your inside is out, then your outside is in.

External threats that could previously be easily contained can now strike directly at the heart of an organization's workloads. Hackers can have identical access to workloads as do the administrators managing them. In effect, the whole world is now an insider threat.

In such circumstances, restricting the permissions to access an organization's workloads and hardening its security configuration are key aspects of workload security.

Promiscuous Permissions Leave You Exposed

Cloud environments make it very easy to grant access permissions and very difficult to keep track of who has them. With customer demands constantly increasing and development teams put under pressure to quickly roll out new enhancements, many organizations spin up new resources and grant excessive permissions on a routine basis. This is particularly true in many DevOps environments where speed and agility are highly valued and security concerns are often secondary.

Over time, the gap between the permissions that users have and the permissions that they actually need (and use) becomes a significant crack in the organization's security posture. Promiscuous permissions leave workloads vulnerable to data theft and resource exploitation should any of the users who have access permissions to them become compromised. As a result, misconfiguration of access permissions (that is, giving permissions to too many people and/or granting permissions that are overly generous) becomes the most urgent security threat that organizations need to address in public cloud environments.

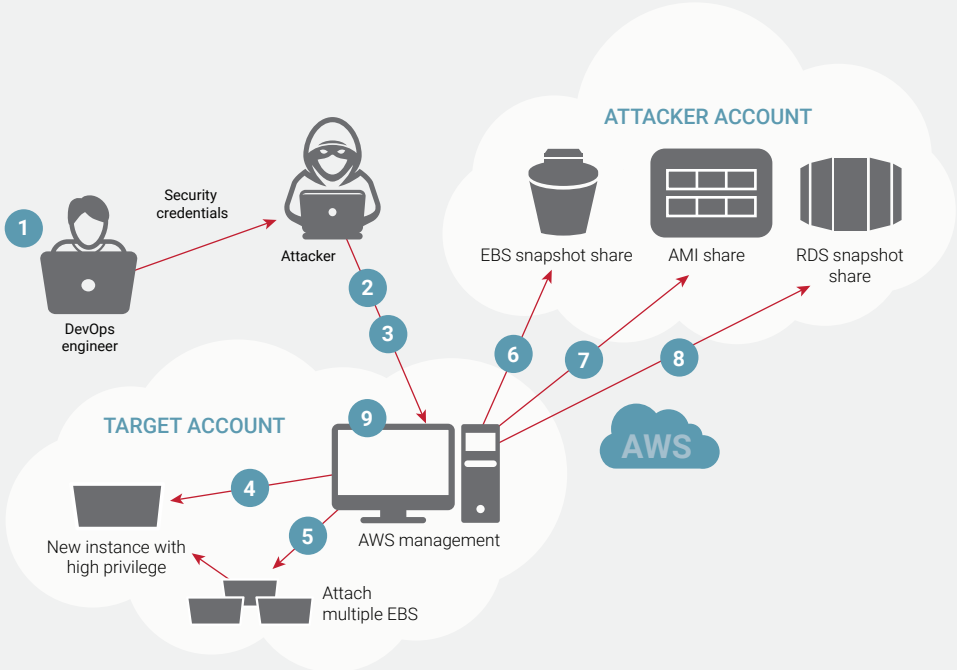
The Glaring Issue of Misconfiguration

Public cloud providers offer identity access management tools for enterprises to control access to applications, services and databases based on permission policies. It is the responsibility of enterprises to deploy security policies that determine what entities are allowed to connect with other entities or resources in the network. These policies are usually a set of static definitions and rules that control what entities are valid to, for example, run an API or access data.

One of the biggest threats to the public cloud is misconfiguration. If permission policies are not managed properly by an enterprise will the tools offered by the public cloud provider, excessive permissions will expand the attack surface, thereby enabling hackers to exploit one entry to gain access to the entire network.

Moreover, common misconfiguration scenarios result from a DevOps engineer who uses predefined permission templates, called *managed permission policies*, in which the granted standardized policy may contain wider permissions than needed. The result is excessive permissions that are never used. Misconfigurations can cause accidental exposure of data, services or machines to the internet, as well as leave doors wide open for attackers.

For example (see Figure 3), an attacker can steal data by using the security credentials of a DevOps engineer gathered in a phishing attack. The attacker leverages the privileged role to take a snap-



1. Spear phishing attack, AWS credentials stolen
2. Enumerate AWS permissions
3. Describe environment assets
4. Run new instance with high privileged role
5. Attach multiple EBS to the newly created machine
6. Share EBS snapshot (and the data in it) to public and create volumes on attacker account
7. Share AMI to public and create machines on attacker account
8. Share RDS snapshot to public and create RDS machines on attacker account
9. Unshare all resources

Outcome: Data Exfiltration

Figure 3. In this example, an attacker steals legitimate credentials from a DevOps engineer to deeply infiltrate the public cloud network to steal data.

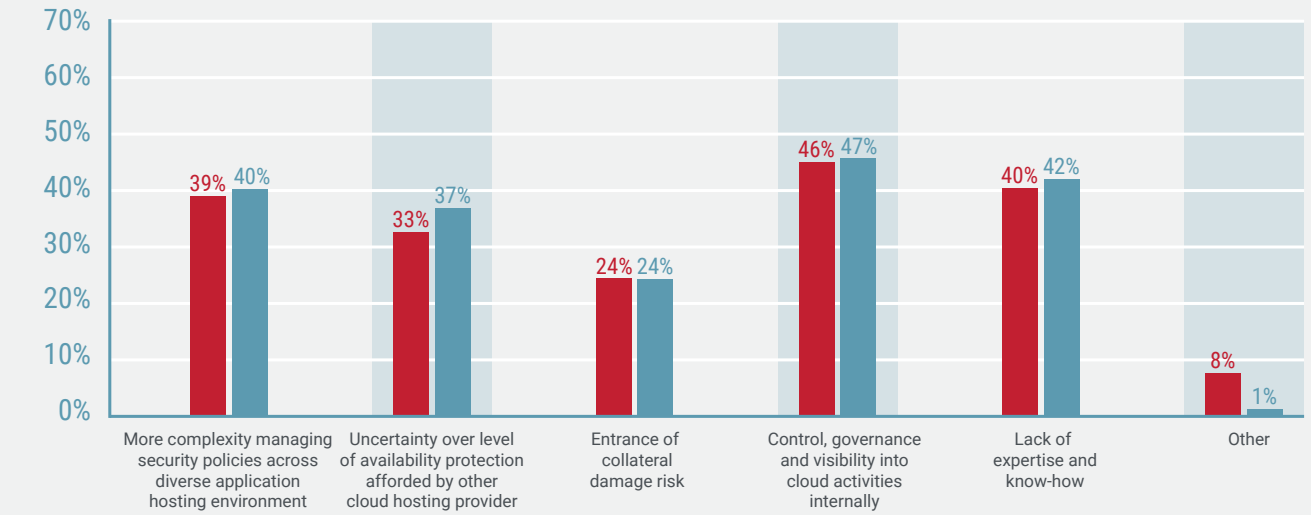


Figure 4. Security challenges associated with migrating applications to the cloud (2017–2018).

shot of elastic block storage (EBS) to steal data, then shares the EBS snapshot and data on an account in another public network without installing anything. The attacker is able to leverage a role with excessive permissions to create a new machine at the beginning of the attack and then infiltrate deeper into the network to share AMI and RDS snapshots (Amazon Machine Images and Relational Database Service, respectively), and then unshare resources.

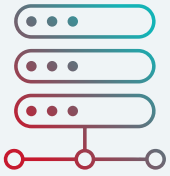
Year over year in Radware's global industry survey, the most frequently mentioned security challenges encountered with migrating applications to the cloud are governance issues followed by skill shortage and complexity of managing security policies (see Figure 4). All contribute to the high rate of excessive permissions.

Cause and Effect

The main causes of misconfigurations vary. In many cases, enterprises simply lack visibility into the cloud environment and resources and do not understand what they are responsible for to determine, maintain and update permissions. Or, because applications and services are very dynamic with frequent (many times daily or weekly) changes, permissions are misconfigured because the enterprise DevSecOps is not keeping pace. Sadly, shortage in human capital and expertise also has an impact. Recruiting, training and retaining security professionals are constant challenges in today's market. It gets even worse when the enterprise has a multicloud approach in which the operation teams need to understand and control multiple, diverse environments. As a result, many enterprises go to cloud service providers expecting to offload these concerns. However, the liability to protect sensitive data while managing the customer experience does not go away.

The negative impact of misconfigurations that the trust enterprises have with their customers can be high:

- Unauthorized access to systems
- Exposure of sensitive data to the public
- Unauthorized access to data and resources
- Violation of compliance standards
- Service disruption
- Erosion of confidence



Data/Storage

Public exposure of S3 buckets or excessive permission to S3 buckets

Network/Machines

Public exposure of machines and databases or excessive network permission to assets

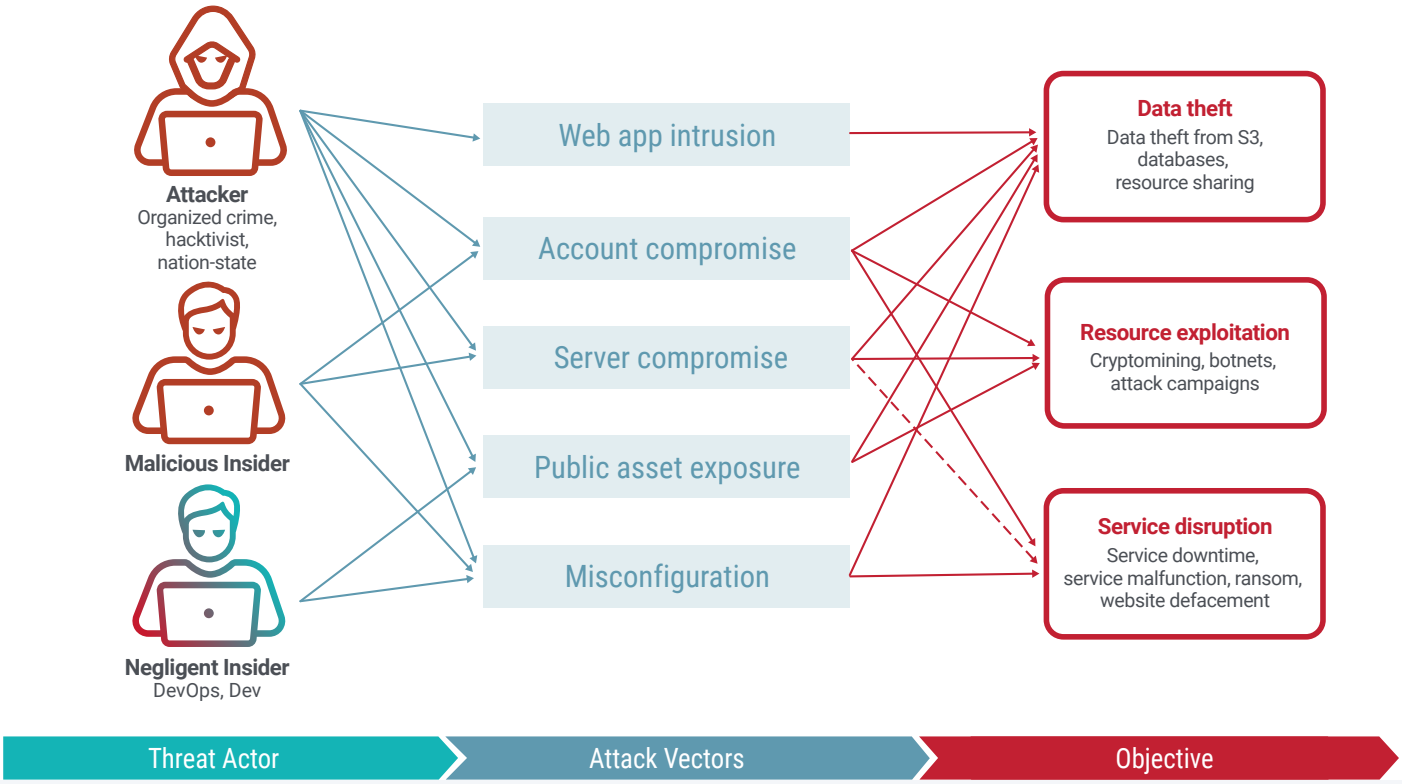
User/Roles

Excessive permission policies for users/roles/user groups to access cloud resources

Figure 5. Misconfigurations are apparent in several areas in the cloud.

Attacking the Cloud

For attackers, misconfigurations in the public cloud can be exploited for a number of reasons. Radware created a public cloud threat map (see Figure 6) that identifies types of attackers, what attack vectors they use and their motivations for launching attacks.



Threat Actor: Attackers such as cybercriminals, hacktivists and nation-state-sponsored attackers have malicious intent. Malicious insiders are legitimate users who exploit their legitimate privileges to cause harm. Negligent users are legitimate users such as Dev/DevOps engineers who make configuration mistakes, or essentially any corporate employee with access that practices low security hygiene. The latter has the higher risk potential among the threat actor personas.

In the cloud environment, the **Negligent Insider** controls the environment from the **outside world**. When your inside is out, then your outside is in. With this situation, excessive permissions essentially become promiscuous permissions.

The Radware global industry survey revealed that 75% of organizations run information security-related employee education programs to reduce the risk of negligent users.

Attack Vectors: Threat actors utilize multiple attack vectors to launch attacks depending on the ultimate objectives.

Objective: Radware's *2018–2019 Global Application & Network Security Report* revealed that the purpose of more than a third of cyberattacks was data theft. Sensitive PII resided in S3/databases/repositories, and resources are shared between accounts. Other attacks were meant to exploit cloud resources for endless compute power, commonly to perform cryptocurrency/cryptojacking activity.

Figure 6. The Radware public cloud threat map.

Typical attack scenarios include several kill chain steps, such as reconnaissance, lateral movement, privilege escalation, data acquisition, persistence and data exfiltration. These steps might be fully or partially utilized by an attacker over dozens of days until the ultimate objective is achieved and the attacker reaches the valuable data.

Web application intrusion (25%) and misconfiguration (21%) were the biggest threats to a company's cloud environment (see Figure 7). DDoS attacks and credential theft were more of a concern in EMEA and APAC. Credential theft has been a major factor in recent data leaks.

Removing the *Mis* from Misconfigurations

To prevent attacks, enterprises must harden configurations to address promiscuous permissions by applying continuous hardening checks to limit the attack surface as much as possible. The goals are to avoid public exposure of data from the cloud and reduce overly permissive access to resources by making sure communication between entities within a cloud, as well as access to assets and APIs, are only allowed for valid reasons.

For example, the private data of six million Verizon users was exposed when maintenance work changed a configuration and made an S3 bucket public.

Only smart configuration hardening that applies the approach of "least privilege" enables enterprises to meet those goals. The process requires applying behavior analytics methods over time, including regular reviews of permissions and a continuous analysis of usual behavior of each entity, just to ensure users only have access to what they need, nothing more. By reducing the attack surface, enterprises make it harder for hackers to move laterally in the cloud.

The process is complex and is often best managed with the assistance of an outside security partner with deep expertise and a system that combines a lot of algorithms that measure activity across the network to detect anomalies and determine if malicious intent is probable. Often attackers will perform keychain attacks over several days or months.

Taking Responsibility

It is tempting for enterprises to assume that cloud providers are completely responsible for network and application security to ensure the privacy of data. In practice, cloud providers provide tools that enterprises can use to secure hosted assets. While cloud providers must be vigilant in how they protect their data centers, responsibility for securing access to apps, services, data repositories and databases falls on the enterprises.

Hardened network and meticulous application security can be a competitive advantage for companies to build trust with their customers and business partners. Now is a critical time for enterprises to understand their role in protecting public cloud workloads as they transition more applications and data away from on-premise networks.

The responsibility to protect the public cloud is a relatively new task for most enterprises. But, everything in the cloud is external and accessible if it is not properly protected with the right level of permissions. Going forward, enterprises must quickly incorporate smart configuration hardening into their network security strategies to address this growing threat.

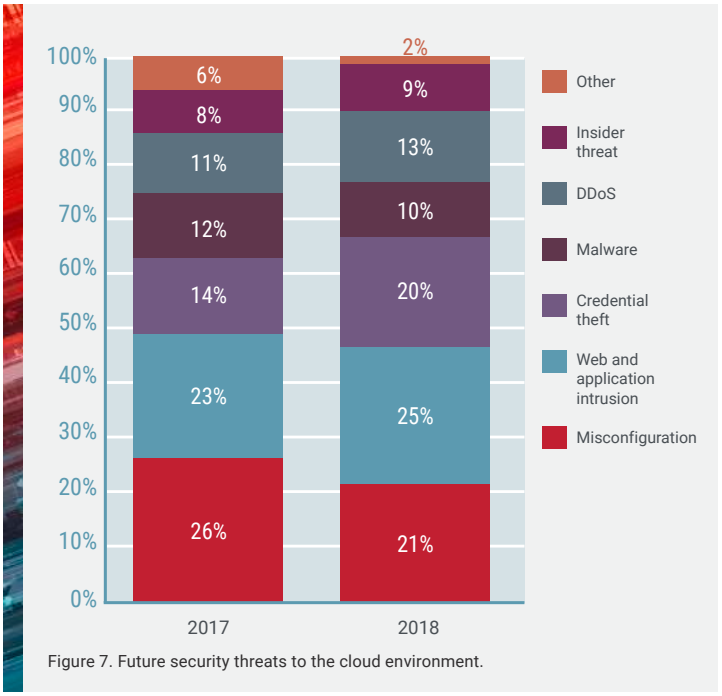


Figure 7. Future security threats to the cloud environment.

Unwarranted permissions are the #1 threat to workloads hosted on public clouds. Detection, mitigation, and algorithmic configuration is the key to keeping nefarious users out and cloud-based workloads secure.

LEARN MORE ABOUT RADWARE'S CLOUD WORKLOAD PROTECTION SERVICE.