2021 SAAS RISK REPORT

This report covers key trends and challenges organizations face when trying to control unsupervised identities and shadow privileges that can put data at risk across a fragmented SaaS & IaaS environment.

ABOUT THE REPORT

Data was gathered from the following SaaS/IaaS supported by Varonis **DatAdvantage Cloud:**

Google box GitHub okta

zoom slack salesforce

Jira Software aws amazon S3

200K
identities

Hundreds of millions
of cloud assets

HIGH-IMPACT CLOUD IDENTITIES

43%

of all cloud identities sit abandoned and unused—and exposed

IMPACT

Unused identities that are abandoned by users who are no longer using a cloud service are sitting ducks for account takeovers and therefore substantially increase an organization's attack surface.

RECOMMENDATION

Unused identities, which multiply quickly, need to be continually monitored and identified so that they can be immediately removed from all operation-critical SaaS apps and cloud services.

3 out of 4

cloud identities belonging to external contractors remain active after they leave the organization

IMPACT

Most ex-contractors have not been fully de-provisioned when they leave, which typically means that they retain access to the organization's cloud services where they can continue to access—and potentially steal—IP and data.

RECOMMENDATION

When a contractor leaves, their identities, privileges, and access must be fully cataloged for complete removal. In addition, their activities over the 60 days prior to termination should be audited for potential data theft or other compromises.

1 out of 4

identities in SaaS apps and **half** in IaaS services are non-human

IMPACT

Non human identities include APIs, serverless applications, virtual machines, etc. Unlike human identities, they are under threat of compromise 24x7 because they are always logged in and are typically overlooked by security teams since they operate in the background.

RECOMMENDATION

Like human identities, non-human ones need to be closely monitored to ensure they haven't been compromised and that their permissions are not overly-broad in relation to the functions that they are required to perform.

MISCONFIGURED CLOUD PRIVILEGES

44%

of cloud user privileges are misconfigured

IMPACT

Users often have overly-broad privileges which are mis-assigned due to a security team oversight or malicious activity. This can open up an organization to account takeovers and data exfiltration.

RECOMMENDATION

User privileges must be continuously monitored for misconfigurations and unauthorized changes so that overly-broad privileges can be right sized and least privileged access effectively enforced.

3 out of 5

privileged cloud users are shadow admins

IMPACT

Shadow Admins are privileged users who have unauthorized privileged access acquired outside of the security team's purview. They can perform admin-level changes that can cause damage across a cloud service.

RECOMMENDATION

Shadow Admins should be monitored the same way that you monitor your regular admins, though in most cases their privileges need to be right-sized to their role and aligned with the privileges of the non-privileged user group to which they are assigned.

HIGH RISK CLOUD ACTIVITIES

15%

of employees are transferring business-critical data to their personal cloud accounts

IMPACT

Business critical data doesn't always stay in sanctioned cloud services. Employees often transfer data to rogue cloud services — including personal accounts. At best this means the data resides outside of your security team's control, and at worst is an indicator that the data has been stolen.

RECOMMENDATION

Security teams need to enforce usage policies that prevent documents from being transferred out of sanctioned apps to private accounts.

16%

of all cloud users perform privileged actions and **20%** of them have access to sensitive corporate data

IMPACT

Privileged actions — ones typically reserved for admins but are often performed by Shadow Admins — should be of highest concern to organizations, especially if the perpetrators also have access to large amounts of data. These actions can negatively impact the entire cloud service or a major part of the experience for everyone, not just a single user or data set.

RECOMMENDATION

Security teams should constantly review all identity privileges to identify Shadow Admins and right-size their permissions to the minimum needed to do their jobs or remove their access if it is determined that their privileges were escalated for malicious purposes.

CLOUD SECURITY CHECKLIST

Reduce your cloud blast radius by ensuring employees have the minimum access needed to do their job. This requires continually mapping access control lists across your disparate cloud services to pinpoint and revoke excessive privileges.

Monitor user activity for anomalies or out-of-policy activity. Pay close attention to privileged users abusing admin privileges for non-admin related activities that can place your organization at high risk.

Eliminate shadow identities by monitoring account activity (or lack thereof). Remove or disable human and non-human identities, such as application tokens that are inactive to limit your attack surface and avoid account takeover.

Perform entitlement reviews regularly so that business unit leaders can see who has access to their data and applications and revoke permissions that are no longer needed.

Employ cross-cloud threat detection to ensure you can spot malicious activity that spans multiple cloud apps. Some SaaS providers have built-in logs and alerts, but can only see a fraction of an attack. Unified SaaS monitoring gives you more robust threat models and makes investigations faster.

Audit cloud sharing configuration settings. This will help prevent accidental oversharing or leakage of business-critical data. A sensitive file carelessly dropped into a folder with broad sharing rights can result in a data breach.

Set up processes for off-boarding remote employees and contractors. This can be a challenge when cloud services are managed outside of your SSO. Adopt a unified, cross-service IAM solution that allows you to revoke permissions when employees or contractors leave the company.