aqua

TEAM nautilus
Aqua Research Team

Cloud Security Report

Cloud Configuration Risks Exposed

May 2021

Table of Contents

Executive summary

The industry's largest public cloud providers continue to add unique services; configuration responsibilities for individual cloud service accounts remain distributed; and multi-cloud environments continue to gain in popularity. These developments make it hard to achieve and maintain proper and consistent configuration for cloud service accounts.

This report summarizes 12 months of anonymized cloud service configuration data from real production environments observed by Aqua Security. The data outlines the configuration challenges faced by teams that use cloud service accounts for their applications. The insights and findings from this report include trends, as well as important security implications and guidance for avoiding and protecting against common issues.

Key findings

There are numerous security posture issues across infrastructure as a service (IaaS) and platform as a service (PaaS) accounts, which suggests a wide-ranging lack of understanding of proper infrastructure configuration.

- 8% percent of small and midsize business users fixed every detected issue, versus only 1% of enterprise users.
- More than 50% of organizations get alerts about misconfigured services that have left ports open to the world. But only 68% of these issues were fixed — and even then, the average time to do so was 24 days.
- Over 40% of users had at least one misconfigured Docker API, and remediation took an average of 60 days after identification.

Recommendations to reduce threat exposure

- Treat all API issues as critical. Institute a formal remediation process to prioritize issues, no matter the size of your organization.
- Avoid applying a single storage policy on multiple instances.
- Adopt a layered approach with a variety of identity access management (IAM) controls, such as multi-factor authentication (MFA) and identity federation.
- Implement cloud security posture management (CSPM) with a cloud workload protection platform solution for complete coverage.

Overview

During a 12-month period, we conducted an in-depth analysis of Aqua CSPM usage data. In a conventional Aqua CSPM data collection model, we collect and store infrastructure data, segmented by a user identifier. This raw data contains the responses from cloud provider API calls, which are then reviewed in aggregate. For our analysis, we reviewed the actions that users took to address issues identified in these reports.

This data shows how effectively users can reduce their infrastructure risk exposure after being alerted to an issue. The data revealed some interesting results, the first being that 84% of users were able to detect and remediate misconfiguration issues using CSPM, issues that otherwise would have gone unnoticed without manual involvement.

84% of users reported that they were able to detect & remediate misconfiguration issues using CSPM

For the bulk of our analysis, we divided Aqua CSPM users into two groups based on the volume of cloud resources they scanned. Users who scanned between one and several hundred resources were included in our SMB (small and midsize business) user group, while users who scanned from several hundred up to a few hundred thousand resources were included in our enterprise user group.

SMB user group scans 1 to 100s of resources. Enterprise users scan 100s to over 100K resources

The data revealed SMB users resolved an average of 40% of detected issues. Conversely, enterprise users resolved 70% of detected issues. We speculated that the difference was a matter of available resources, because enterprise users are most often affiliated with larger organizations and have more resources.

So, why do we need more data about user experiences in resolving cloud infrastructure issues in the first place? A recent survey by global market intelligence firm IDC showed that almost 80% of respondents had at least one cloud security breach over the preceding 18 months. In addition, 67% of the participants noted that their main IaaS and PaaS security concerns were misconfigurations.

80% of respondents had at least 1 cloud security breach

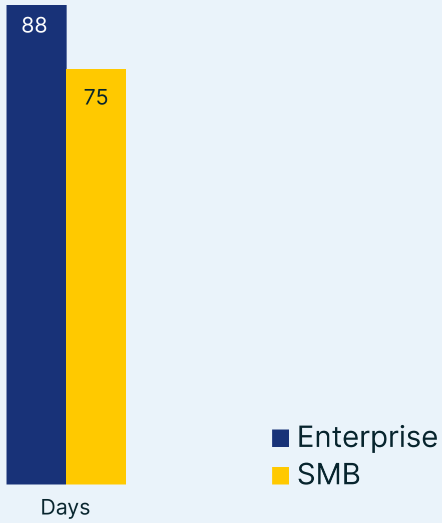
Verizon's 2020 Data Breach Investigations Report showed that cloud misconfiguration errors had increased from 10% in 2017 to 40% in 2019. When you consider that a single cloud misconfiguration can expose organizations to severe cyber risk, such as data breaches, resource hijacking, and denial of service, etc. — the consequences are all too real to ignore.

Although cloud native applications bring the benefit of "shift left," allowing more agility by giving more people access to define the environment, that approach means that many organizations are moving away from a centralized approach to security. Where once there was only a small, highly skilled team of security practitioners making all configuration changes, now a modern, decentralized approach is common. Now development teams are making configuration decisions or applying services which can have dramatic implications for the security posture of your production environment.

Analysis

Even though virtually any open issue could turn into a cybersecurity threat, few users fixed every issue. One possible reason for this is that enterprise users might need a better triage process to prioritize issues. Without a good process, it’s easy to be overwhelmed by the endless number of security issues being identified. Since smaller organizations usually have fewer monitored cloud resources, their security practitioners often have fewer issues to fix, but organizations of any size could benefit from an improved triage method.

Time to resolution »
Even with seemingly fewer resources, SMB users found a way to resolve issues more quickly.



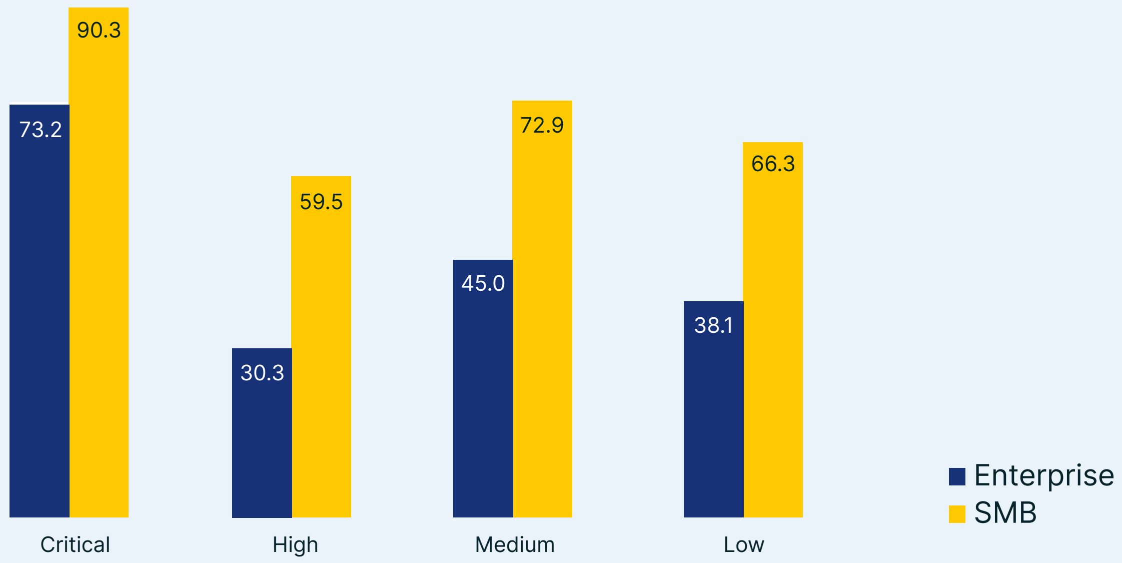
To no one’s surprise, users usually resolved critical issues first. However, medium and low risk issues received more attention in total than high-risk issues. Since Aqua CSPM allows the user to tweak the configuration of plugins to change the severity of the rules, we surmised that some users must have raised the threat level for a few medium- and low-risk alerts that were high-risk in their environment.

About 8% of SMB users fixed all issues detected, & only about 1% of enterprise users

We then analyzed the changes users made. We converted the nominal ranks to figures; Low Severity - 1, Medium - 2, High - 3, Critical - 4. . We then calculated the average change of the severity score. We found that the average change was +1.235, which is quite significant in this context, as users tended to give higher risk scores than some of the CSPM rules. For instance, they changed low scores to medium or high.

Remediation rates based on issue severity

Both Enterprise and SMB users were more likely to fix critical issues



How was CSPM used to resolve security gaps? As we now know, a misconfiguration of cloud settings can lead to serious issues, so we focused on the following:

- Storage bucket and blob misconfigurations
- IAM misconfigurations
- Data encryption issues
- Exploitable services behind open ports
- Container technology exploitation

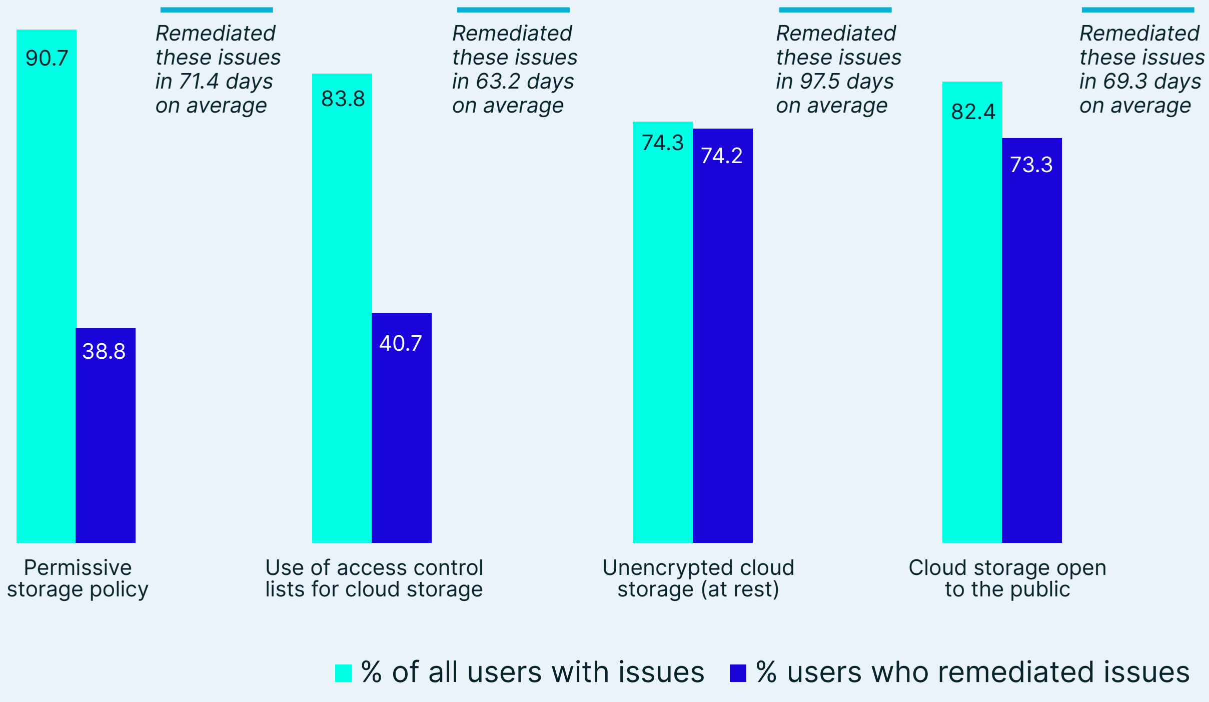
Storage (bucket and blob) misconfiguration

In the wild, there are many examples of cloud storage bucket and blob breaches. For instance, a misconfigured cloud storage bucket exposed Pfizer drug safety reports, 0×00sec reported that an S3 bucket was publicly accessible for 63 days, and more than 54,000 scanned New South Wales driver’s licenses were found in open cloud storage.

We analyzed our users’ data and found the following information (further analysis based on user type is available in the appendix).

Type of storage issue and time to remediate

Users were most likely to remediate unencrypted cloud storage (at rest) but doing so took the most time.



Remediated these issues in 71.4 days on average

Remediated these issues in 63.2 days on average

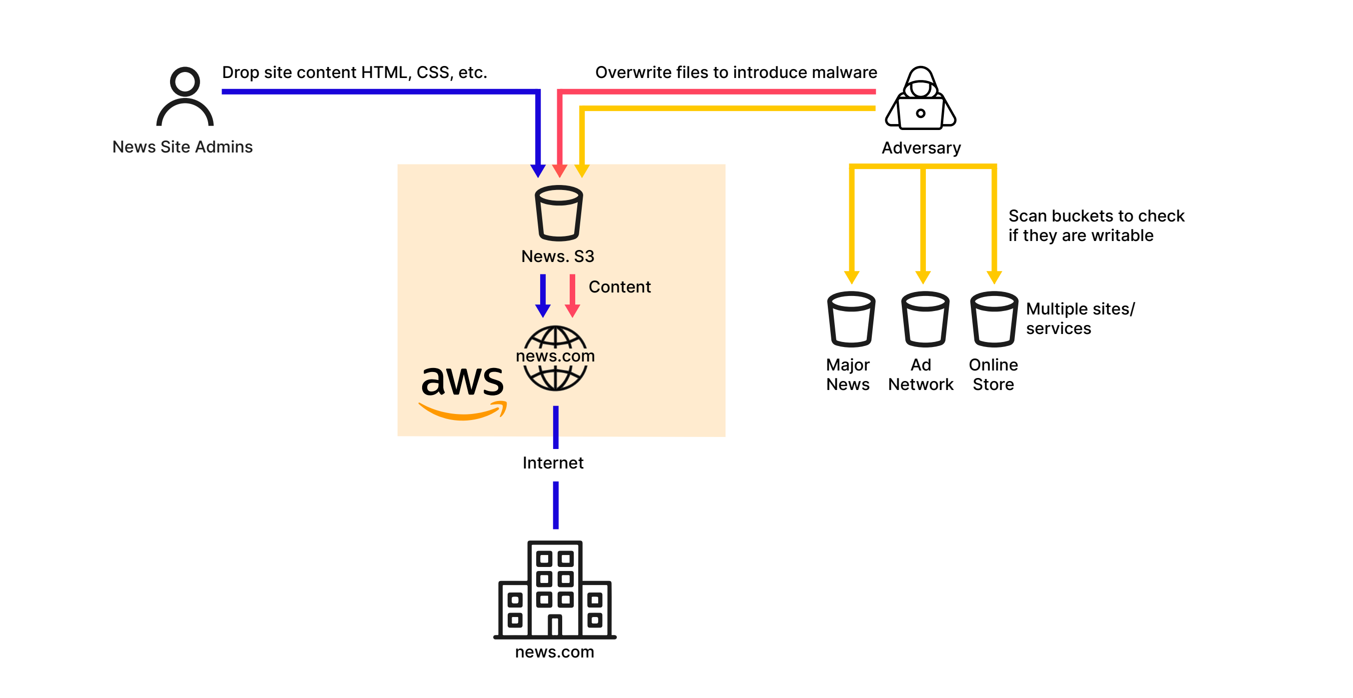
Remediated these issues in 97.5 days on average

Remediated these issues in 69.3 days on average

Buckets exposed to the world

82.4% of environments had "open to the internet" issues

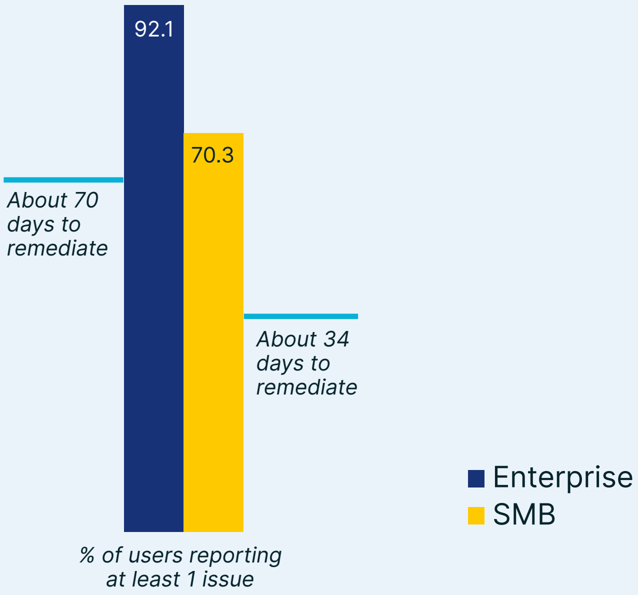
Due to misconfigurations, open access to the public is one of the main reasons for cloud storage bucket and blob breaches. Every major cloud service provider (CSP) uses a default configuration that is set to private, so public access is prohibited. However, our data shows that many organizations change these configurations as part of their ongoing operations and business logic. These changes may include inbound traffic being open to "0.0.0.0/0," "::/0," or all protocols and ports.



Exposed Buckets

Both SMB users and enterprise users reported at least one issue with exposed buckets. Enterprise users fixed more issues, but they took twice as long to do it.

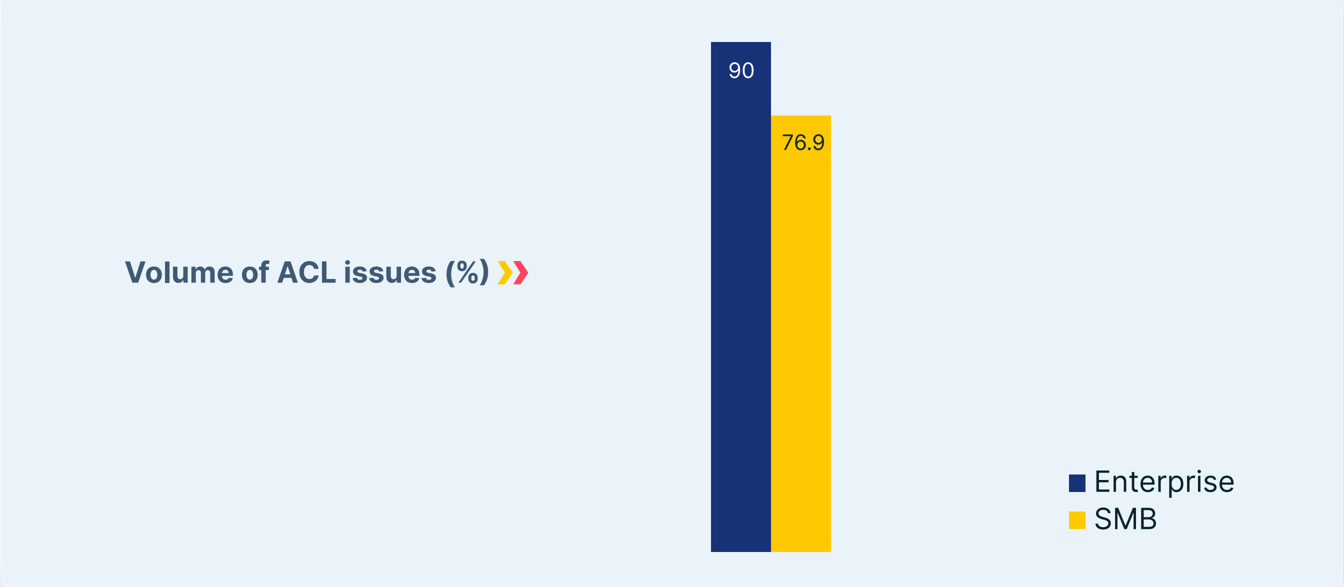
Issues and days to remediate ❯❯
for exposed buckets



It seems that despite the risks, open public access is important enough for their deployments that many businesses change these default settings. And although enterprise users put more effort into mitigating most issues, it takes them longer to do it.

Misconfigured access control lists (ACLs)

Misconfigured ACLs are another common cause of data breaches in cloud storage buckets and blobs. Essentially, there are two types of ACLs: one allows the user to control access at the bucket level, and the second allows the user to control access at the object level. Either way, ACLs are considered a legacy access control mechanism that predates IAM. For instance, Amazon’s S3 best practices recommend using bucket policies or IAM to control data access, rather than ACLs.
The problem with ACL policies is that they can allow full control or read and write control, which adversaries can exploit to gain full access.



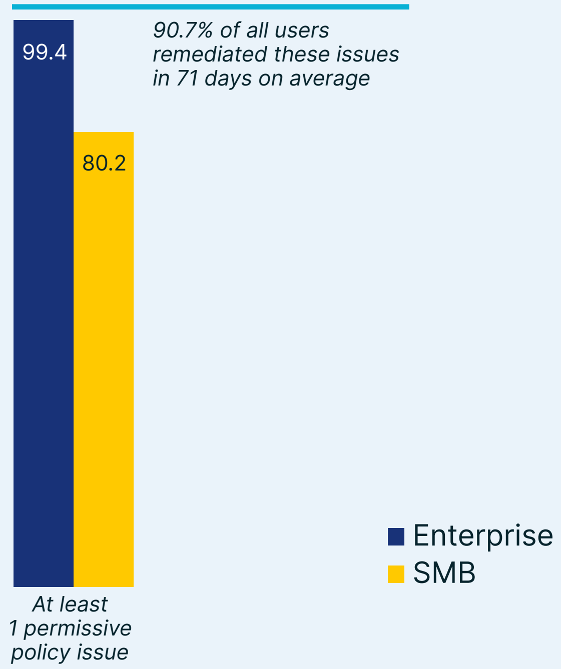
SMB users remediated only 21.0% of ACL issues, and enterprise users remediated only 41.2% — considerably fewer than bucket issues, which suggests that security practitioners may view ACL threats as less severe. It took an average of two months for both groups to remediate ACL issues.

Only 21% of SMB & 41.2% of enterprise users fixed ACL issues

Permissive storage policies

Storage policies are designed to specify the end-user's permissions and apply them to the entire storage instance. By applying a single policy on multiple instances, the organization can leave itself open to threats. Such a practice does not align with least-privilege principles, since some of the end users will end up with more privileges than they need. These types of issues include permissive policies that allow end users unlimited access and actions.

Permissive Policy Issues (%) ❯❯
An overwhelming number of organizations (99.4%) had at least one permissive policy issue.



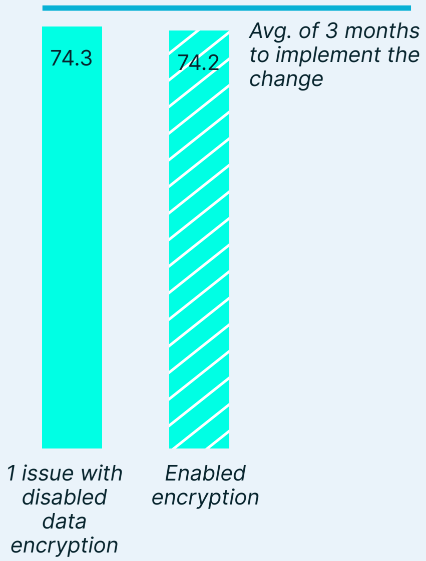
We can conclude that users either see permissive policy issues as higher risk than ACL issues, or are simply more aware of them. Remediation rates were much higher for permissive policy issues than for ACL issues.

Unencrypted cloud storage

A few cloud providers offer encryption of data at rest by default. Azure and Google Cloud Platform (GCP) also provide data encryption by default for all data at rest — if uploaded to storage. AWS users must enable their data encryption. Once encryption is enabled, all data uploaded to Amazon S3 is encrypted at rest. Most CSPs also support the HTTPS protocol, so users can encrypt data in transit when uploading to, or downloading from, cloud storage.

Data Encryption (%) ❯❯

We found that users with disabled data encryption eventually enabled encryption, but it took an average of 3 months.



IAM misconfigurations

User access to cloud resources is managed by the cloud provider's IAM controls and is a key factor in cloud security. When accessing the cloud provider's environment for the first time, the default user is a superuser (root/admin user) with maximum privileges. The IAM controls allow that user to apply least-privilege principles to other users and manage role-based access.

IAM controls also offer other security features to protect the cloud account and resources, such as MFA and identity federation. We found the following information (further analysis based on user type is available in the appendix).

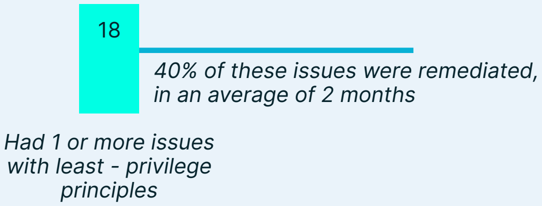
Credentials best practices

Adversaries are constantly reinventing their techniques to obtain cloud credentials. To avoid threats that could compromise access to your identity, cloud CSP IAM best practices recommend the following.

Observe the least-privilege principle. Users should be granted only the minimum permissions required to complete their tasks. Root users should be reserved for critical administrative activity:

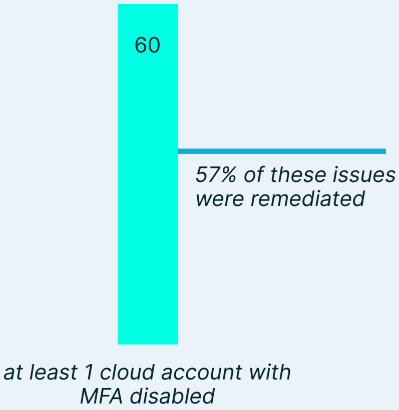
Least privilege issues (%)

Some users had one or more issues that were out of scope with least-privilege principles - specifically, they overused root user. Fewer than half of these users remediated these issues, and it took them 2 months.



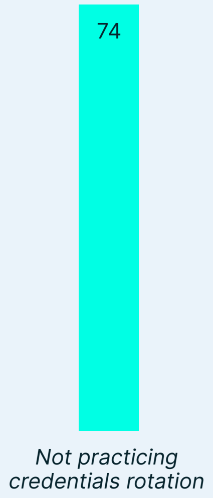
Use MFA. MFA should be turned on when users access cloud resources

More than half of organizations had at least 1 cloud account with MFA disabled, with just over half being remediated.



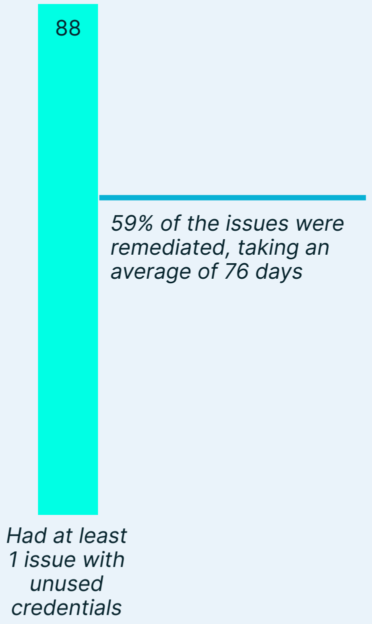
Establish strong password and rotate credentials. Organizations should enforce a strong password policy on cloud resources and secrets:

Password rotation (%) ❯❯
Passwords and access keys should be rotated and changed regularly. This limits collateral damage from a password leak.



Audit and remove unused credentials. Users should have only one set of passwords and access keys — period:

Unused credentials (%) ❯❯
Most users had at least one issue with unused credentials.



Data encryption issues

As mentioned earlier, data encryption is another important layer of security, but it does lead to some organizational tension between security and business goals. Too much data encryption can be expensive, and it often slows down operations, while too little may lead to sensitive information being exfiltrated in plaintext.

An experienced attacker can easily break weak cryptographic ciphers or protocols

Best practices recommend encrypting sensitive data at rest, in transit, and in processing. Organizations must verify that their encryption protocols are strong enough to endure brute force and man-in-the-middle (MITM) attacks as data traverses the internet.

We analyzed our user data and found the following information regarding vulnerable transport layer security (TLS) versioning, unencrypted data in traffic, unencrypted cloud services (data at rest), and unencrypted data bases (data at rest) (further analysis based on user type is available in the appendix):

Amount of data encryption issues and remediation times

While the top encryption issue is unencrypted cloud services, the issue with the lowest remediation rate is unencrypted data in traffic

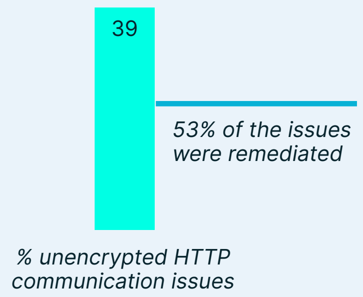
	TLS versions	Unencrypted data in traffic	Unencrypted cloud services	Unencrypted databases
% of users who had issues	5%	39%	55%	30%
% of users who remediated the issues	60%	53%	72%	83%
Average number of days to remediate	65	65	66	28

Unencrypted data in traffic

Many end-users had issues with unencrypted HTTP communication, potentially exposing their communications to a MITM attack. Only half of the issues were remediated.

In 2020, the US Computer Emergency Readiness Team (US-CERT) released a threat alert **for the healthcare sector regarding MITM attacks. Without corrective action, an attack could have resulted in malicious code injections, data leaks, or data forging.**

Amount of issues with unencrypted HTTP communication



Vulnerable TLS version

TLS is a cryptographic protocol designed to provide communications security over a computer network. Conceptual flaws in the TLS protocol can lead to major cyber-attacks. Attackers will often combine protocol downgrades, session resumption, and connection renegotiation in their attacks. Unfortunately, we found organizational cloud resources that still relied on outdated versions of TLS.

Exploitable services behind open ports

Since ports that are open to the world represent a common misconfiguration, we concentrated our data analysis on rules that were triggered on ports allowing all inbound network traffic — i.e., ports that accept traffic from “0.0.0.0/0” (IPv4) or “::/0” (IPv6). These are ports are open to any communication.

An open port is not necessarily dangerous. In fact, open ports are essential for internet communication, because services often need to listen for inbound packets to perform their jobs. However, these open ports can be exploited if the listening service is misconfigured or unpatched, or has poor network security rules.

To manage this risk, security best practices recommend opening ports only if necessary. Also, controlling the opening and closing of the ports should be done using a firewall. You should also close any ports that are not workable for inbound or outbound communication to reduce the attack surface. We found the following configuration issues (further analysis based on user type is available in the appendix).

Exploitable Services:

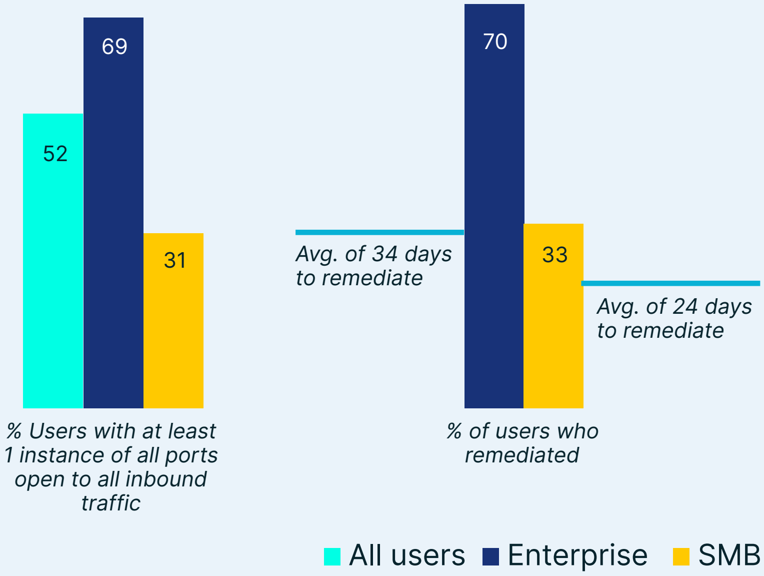
Type of cloud security issue	% of users who had issues	% of users who remediated the issues	Days to remediate (avg.)
Open FTP (20,21)	28.8%	52.7%	55.4
Open SSH (22)	64.4%	54.1%	48.1
Open Telnet (23)	25.3%	52.0%	56.0
Open SMTP (25)	32.0%	50.6%	57.4
Open DNS (53)	36.3%	49.9%	54.8
Open RCP	37.7%	53.1%	54.3
Open NetBIOS	27.4%	53.9%	55.8
Open SMB (445)	31.5%	53.0%	55.0
Open databases (Elasticsearch, MySQL, etc.)	37.4%	58.7%	47.0
Open RDP	49.6%	45.5%	66.0
Open VNC	35.3%	51.1%	57.9
All ports open to the world	51.9%	68.5%	24.3
Open SaltStack master 4505	35.9%	88.9%	79.5
Open Docker API in ports 2375 & 2376	40.6%	89.8%	65.2

All ports are open to the world

Having all ports open and listening to inbound network traffic simply isn't a common business need, so the results we found were surprising.

Open ports (%) »

Half of users had at least one case (e.g., Amazon EC2) with all ports open to all inbound traffic. And more than twice as many enterprise users than SMB users had such issues. Enterprise users were more attentive to this risk, but it took less time for SMB users to remediate.

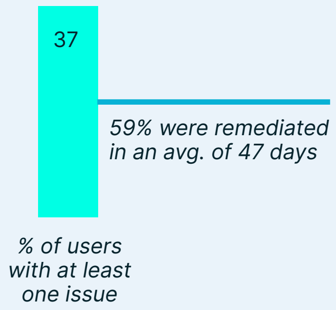


Open databases

A seasoned adversary can hack their way into a misconfigured database in just a few hours. We recommend that practitioners raise the priority of these issues. Database management best practices recommend limiting the incoming traffic to an organization's private network or specific IP ranges. Database access usually can be protected by several layers, including credentials and firewall network rules.

Misconfigured database % »

Unfortunately, the time to remediation for exposed databases provides plenty of time for adversaries to hack into these databases.



Open SaltStack master (port 4505)

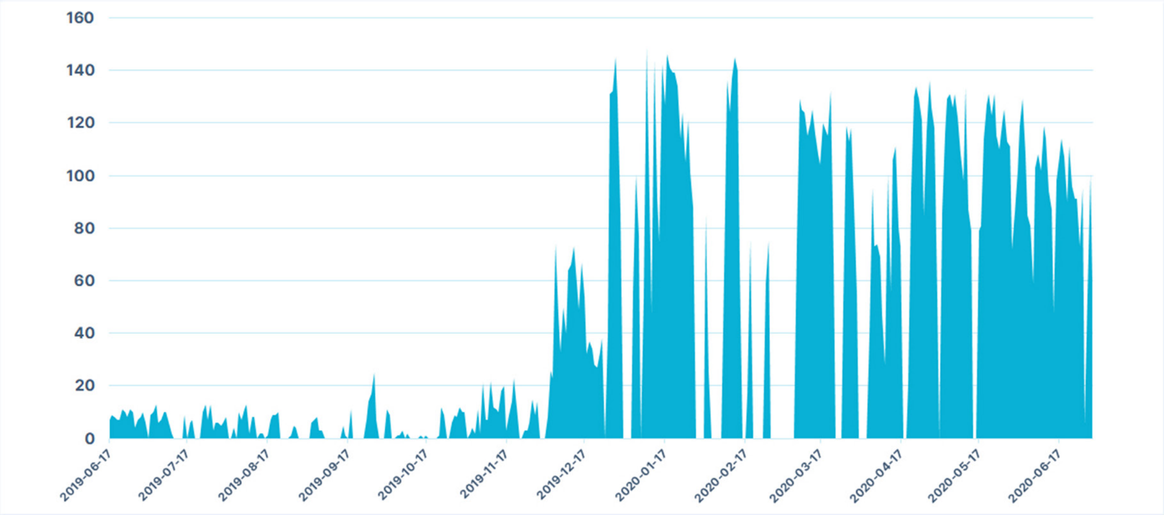
In May 2020, we published a blog post about two high-severity CVEs in the SaltStack platform. These vulnerabilities can allow attackers to remotely execute commands on the Salt leader node, which results in a full compromise of the host and can expose sensitive information in the cloud environment.
To address this, Aqua CSPM released three new plugins that detect exposure in cloud instances open to incoming public traffic (i.e., if ports 4505 and 4506 are open to “0.0.0.0/0”). **We found that 36% of users applied the plugins to fix open SaltStack issues.**

Container technology exploitation

Misconfigured Docker daemons

Keeping containerized applications safe requires specialized knowledge — knowledge that is in short supply — so it should come as no surprise that attacks exploiting this knowledge gap are on the rise.

A comparison between the second half of 2019 and the first half of 2020 reveals that since the beginning of 2020 the volume of attacks has dramatically increased.



We found the following misconfigurations in container-related services (further analysis based on user type is available in the appendix):

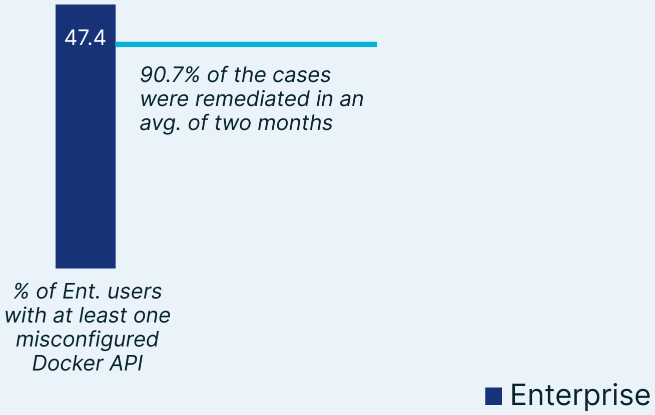
	% of users who had issues	% of users who remediated the issues	Avg number of days to remediate
Misconfigured Docker API (ports 2375 and 2376)	40.6%	89.8%	65.2
Permissive Kubernetes access control policy	16.7%	66.5%	41.1
Kubernetes vulnerable version	21.9%	77.1%	41.4
Permissive Kubernetes network policy	35.2%	64.9%	44.9

Open Docker API (port 2375)

Cyberattacks against cloud native environments often target and exploit vulnerable hosts. To do this, adversaries are actively scanning for exposed Docker API ports. The main threat posed by these attacks is crypto mining, a process that methodically siphons resources from unsuspecting victims — resources that would otherwise be used to support your business objectives.

Misconfigured hosts »

We found that these were a common problem for many organizations.



Almost half of enterprise users had at least one misconfigured Docker API. However, we believe it’s taking too long to remediate, since attackers are continually refining their attacks to find exploitable hosts faster than security groups can close them.

Kubernetes configurations

Although we’ve seen relatively few stories concerning attacks in the wild targeting Kubernetes clusters, the threat is growing. The following is a breakdown of data associated with the Kubernetes configurations we tested.

Vulnerable Kubernetes versions

Some of these versions contained severe vulnerabilities that could allow adversaries to gain access across the cluster, compromise sensitive data, or cause network denial of service. For instance, CVE-2018-1002105 will enable attackers to perform privilege escalation to gain full admin privileges on a cluster, compromise sensitive data, or cause network denial of service.

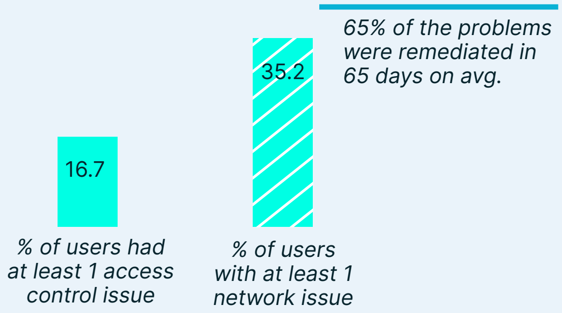
Updating to the latest Kubernetes version is crucial to avoid known and patched vulnerabilities. Old versions may allow attackers’ initial access, privileged escalation, and lateral movement across the cluster.

Permissive Kubernetes access and network policies

Permissive Kubernetes policies allow attackers to find initial access or iterate across the cluster.

Kubernetes Access ❯❯

We did find a few users with ACL or network policy issues, but most of those issues were remediated within 65 days on average.



Summary

We know that not all cloud journeys are created equal. Some organizations adopt a multi-cloud approach to increase efficiency and maintain flexibility and independence, others adopt a single environment to keep things more manageable.

However, whatever path you choose, it can still be complex and difficult to secure properly. This complexity, in single or multi-cloud environments, often leads to service configuration issues that can unnecessarily expose organizations to threats — and the "blast radius" of damage resulting from misconfigurations can be much greater than for the traditional OS or on-premises workloads.

To manage this, we recommend solutions that go beyond host-based security tools. This requires a CSPM solution that operates at the cloud provider control plane level, something that can leverage APIs from the underlying public cloud vendor. This is important because it provides needed visibility into the configuration of the cloud services.

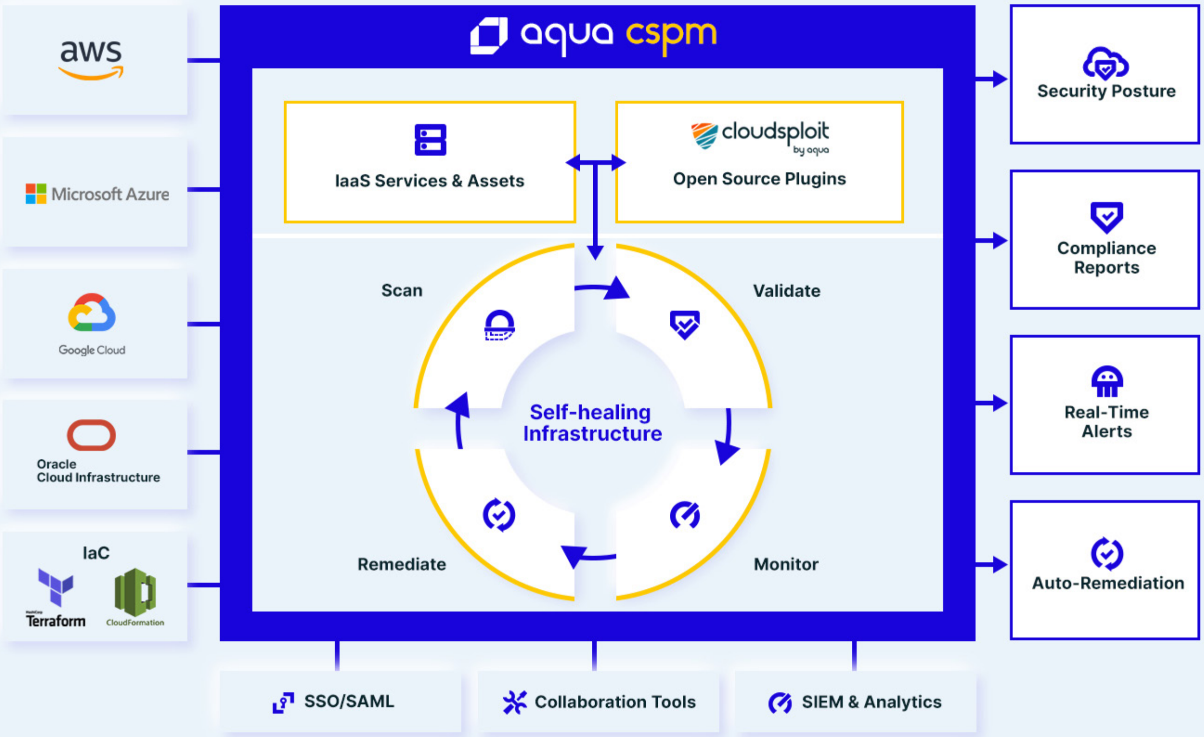
With automated capabilities to validate hundreds of settings across regions and accounts, Aqua's CSPM tool can assess your current security posture against best practices, policies, and compliance frameworks and help to:

- Identify misconfigured storage blobs and buckets that are exposed publicly
- Find compute and database resources with unintended public access settings
- Ensure the encryption in transit and at rest across cloud services
- Enforce user policy definitions to ensure least-privileged access to resources
- Detect changes to critical resources such as firewall rules, logging groups, or account settings
- Catch activity in unused or unexpected cloud provider regions or locations

Aqua Cloud Security Posture Management

Aqua CSPM is the cloud security auditing, monitoring, and remediation solution that scans your entire public cloud infrastructure for potential security risks, including misconfigurations, malicious API calls, and insider threats. With each scan, it securely connects to your cloud account through the APIs of the underlying cloud provider, collects the necessary data, and then checks it for potential risks and misconfigurations. Aqua CSPM has a plugin for virtually any configuration — or lets you easily build your own — to check specific settings and compare it to the corresponding best practice. In the case of misconfiguration, it offers manual, guided or automated remediation.

With Aqua CSPM, organizations can ensure their infrastructure security posture by detecting thousands of potential threats in their cloud accounts. And to amplify the benefits of CSPM, it is critical to weave infrastructure security into your complete cloud native security strategy — embedding security across your entire application lifecycle from the build process through the run-time environment. By combining cloud workload protection for VMs, containers, and serverless with cloud infrastructure best practices, you can achieve full-stack security.



Appendix

Type of cloud security issue	% of users who had issues			% of users who remediated the issues			Average number of days to remediate		
	SMB users	Ent. users	All users	SMB users	Ent. users	All users	SMB users	Ent. users	All users
Cloud storage (buckets and blobs)									
Permissive storage policy	80.2%	99.4%	90.7%	19.8%	39.2%	38.8%	50.2	71.6	71.4
Using ACLs for cloud storage	76.9%	90.0%	83.8%	21.0%	41.2%	40.7%	55.3	63.3	63.2
Unencrypted cloud storage (at rest)	57.7%	88.9%	74.3%	49.5%	74.8%	74.2%	76.8	97.8	97.5
Cloud storage open to the public	70.3%	92.1%	82.4%	50.5%	73.9%	73.3%	34.0	69.8	69.3
Cloud identity and access management									
Multi-factor authentication disabled	60.2%	61.3%	60.8%	31.1%	60.0%	56.8%	41.7	67.0	65.2
Deviating from least-privilege principle	12.9%	22.0%	17.8%	24.9%	44.8%	40.0%	38.0	59.6	55.8
Not practicing credential rotation	57.5%	87.4%	73.6%	53.8%	74.5%	73.9%	65.2	72.3	72.1
Unused credentials	80.0%	94.9%	88.2%	34.7%	59.7%	58.5%	49.6	77.0	76.3
Data encryption issues									
Vulnerable TLS version	1.1%	8.8%	5.2%	79.2%	59.3%	60.4%	12.0	69.5	65.3
Unencrypted data in traffic	17.8%	59.4%	39.2%	50.3%	52.9%	52.8%	21.6	67.6	65.3
Unencrypted cloud services (data at rest)	42.6%	67.3%	54.7%	53.1%	73.7%	71.8%	32.0	68.2	65.7
Unencrypted databases (data at rest)	11.9%	44.1%	29.5%	49.9%	84.5%	83.4%	29.3	27.8	27.8
Exploitable Kubernetes									
Misconfigured Docker API (ports 2375 and 2376)	18.6%	47.4%	40.6%	57.1%	90.7%	89.8%	54.4	65.4	65.2
Kubernetes access control	12.1%	23.5%	16.7%	41.7%	75.3%	66.5%	21.4	45.0	41.1
Kubernetes vulnerable version	6.8%	35.4%	21.9%	57.6%	77.9%	77.1%	20.4	42.0	41.4
Kubernetes network policy	30.2%	42.5%	35.2%	42.2%	71.8%	64.9%	24.0	48.6	44.9
Exploitable services behind open ports									
Open FTP (20,21)	13.1%	42.8%	28.8%	35.4%	54.1%	52.7%	21.3	57.2	55.4
Open SSH (22)	51.4%	76.8%	64.4%	27.1%	55.7%	54.1%	29.8	48.6	48.1
Open Telnet (23)	9.8%	40.9%	25.3%	33.6%	53.5%	52.0%	20.7	57.8	56.0
Open SMTP (25)	16.6%	44.7%	32.0%	30.9%	52.5%	50.6%	22.4	59.4	57.4
Open DNS (53)	18.8%	52.0%	36.3%	31.1%	51.8%	49.9%	29.1	56.4	54.8
Open RCP	19.6%	52.7%	37.7%	31.8%	55.0%	53.1%	28.0	55.6	54.3
Open NetBIOS	12.7%	39.5%	27.4%	25.0%	56.5%	53.9%	38.7	56.5	55.8

Type of cloud security issue	% of users who had issues			% of users who remediated the issues			Average number of days to remediate		
	SMB users	Ent. users	All users	SMB users	Ent. users	All users	SMB users	Ent. users	All users
Exploitable services behind open ports									
Open SMB (445)	14.9%	46.6%	31.5%	30.0%	55.2%	53.0%	28.3	56.4	55.0
Open databases (Elasticsearch, MySQL, etc.)	19.4%	52.3%	37.4%	32.2%	60.5%	58.7%	33.5	47.4	47.0
Open RDP	31.9%	65.5%	49.6%	34.4%	46.3%	45.5%	31.9	67.7	66.0
Open VNC	16.8%	54.0%	35.3%	32.1%	52.7%	51.1%	27.9	59.4	57.9
All ports open to the world	30.9%	69.1%	51.9%	33.3%	70.3%	68.5%	34.4	24.0	24.3
Open SaltStack master (4505)	14.5%	49.7%	35.9%	73.2%	90.3%	88.9%	39.5	82.3	79.5

Team Nautilus focuses on cybersecurity research of the cloud native stack. Its mission is to uncover new vulnerabilities, threats and attacks that target containers, Kubernetes, serverless, and public cloud infrastructure — enabling new methods and tools to address them.

TEAM
nautilus
Aqua Research Team