TOP 3 CLOUD SECURITY VULNERABILITIES

1 in 4

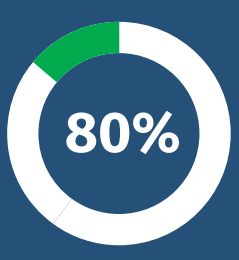
of middle market executives reported a data breach at their company in the last year.[1]

This is the highest level since RSM began tracking data in 2015 and a significant increase from 18% in 2019.

One of the main reasons mid-sized businesses bear the brunt of data breaches is because they don't have the same level of protection as global corporations.

Lightstream has uncovered three common cloud security challenges faced by mid-market IT professionals.

VULNERABILITY #1 IAM (Identity and Access Management)



of hacking-related breaches in 2020 involved the use of lost or stolen credentials.[2]

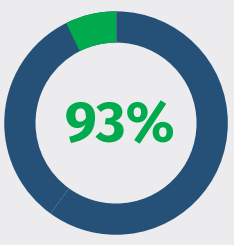
Without IAM tools to identify and confirm users, applications and devices and grant the appropriate authorities and permissions, businesses are at a very high risk.

LIGHTSTREAM RECOMMENDS

- Adopt a zero-trust framework wherein users and devices are not trusted by default
- Create secure passwords and change them regularly
- Consider using multifactor authentication (MFA) whenever possible to add an extra layer of security

VULNERABILITY #2 Filtering and Logging

- What changes are users making?
- Where are we storing that log?
- How do I filter out the important changes from those that aren't?



of breaches that occurred in 2018 could have been preventable with basic security measures.[3]

Most breaches can be avoided with adequate logging and monitoring, which can detect changes or events that create vulnerabilities and allow the company to respond and remediate before the damage is done.

LIGHTSTREAM RECOMMENDS

Prioritize event types when setting up your management system.

Password changes	Unauthorized logins	Login failures	New login events	Malware detection

VULNERABILITY #3 Messaging and Notifications

What is the nature of the violation, who was notified about it, and what – if any – action did that person take?

3 TYPES OF VIOLATIONS

you'll need to deal with when investigating messaging and notification alerts.[4]

Serious violations such as suspicious activity alerts, data leaks, and new app discoveries require immediate response

Questionable violations will require further investigation

Authorized violations or anomalous behavior alerts resulting from legitimate use can be dismissed

LIGHTSTREAM RECOMMENDS

Review all notifications and use them as tools for modifying policies. If harmless events are being considered violations to existing policies, refine policies to receive fewer unnecessary alerts.

A strong cybersecurity strategy is the first step in avoiding the expenses and headaches that come with data breaches. Outsourcing your cloud security to a trusted partner such as Lightstream can help defend your organization against an evolving array of vulnerabilities while freeing up internal IT resources to concentrate on top business objectives.

lightstream

www.lightstream.tech

[1] RSM US Middle Market Business Index Cybersecurity Special Report 2021
[2] 2021 Data Breach Investigations Report | Verizon
[3] 2018 Cyber Incident & Breach Trends Report | Internet Society
[4] Manage alerts raised in Cloud App Security | Microsoft Docs