

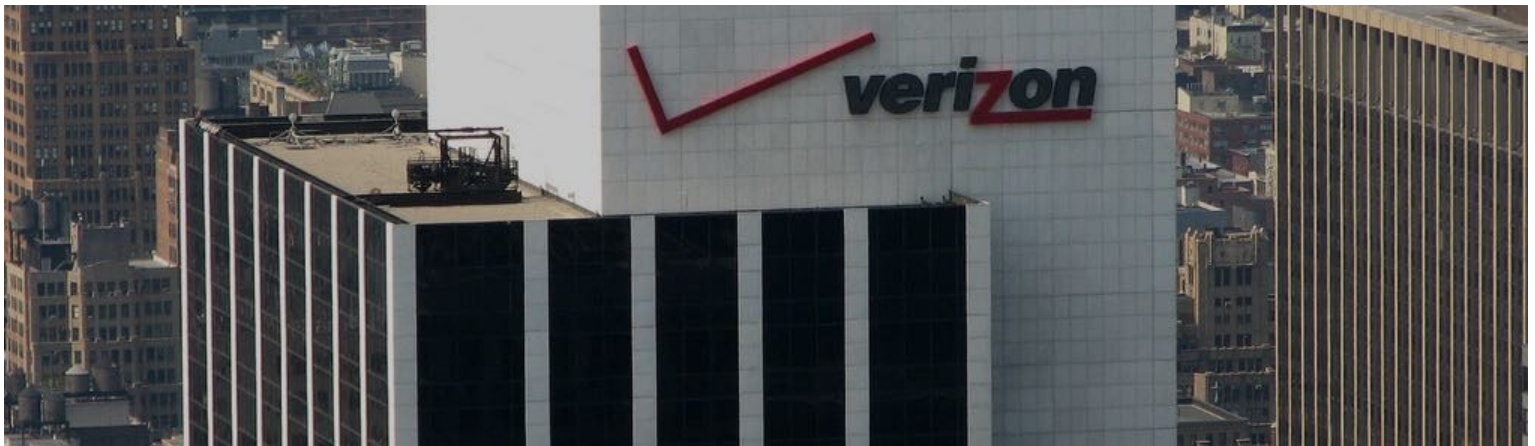


[MSSP Alert](#)

Managed Security Services Providers (MSSP) News, Analysis and Cybersecurity Research

- [Login](#)
- [Subscribe to our Newsletter](#)
- [Follow us on Twitter](#)
- [Connect with us on Facebook](#)
- [Join our LinkedIn Group](#)
- [Subscribe to our RSS feed](#)

☒ Subscribe To Our Daily Enewsletter:



[Verizon Suffers Second Data Leak on Amazon AWS Cloud](#)

[Confidential Verizon information exposed on Amazon Web Services \(AWS\) cloud, Kromtech Security Research Center says. Second Verizon-AWS leak this year.](#)

by Joe Panettieri • Sep 22, 2017

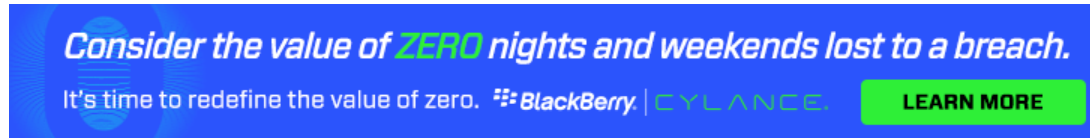
Is it a case of incompetence, laziness or poor cloud services design? Whatever the case, someone in the Verizon Communications business ecosystem has once again left confidential information exposed on Amazon Web Services (AWS), according to [Kromtech Security Research Center](#).

According to the report:

“On September 20th, Kromtech Security researchers discovered publicly accessible Amazon AWS S3 bucket containing around 100MB of data attributing to internal Verizon Wireless system called DVS (Distributed Vision Services)...

Although no customers data are involved in this data leak, we were able to see files and data named “VZ Confidential” and “Verizon Confidential”, some of which contained usernames, passwords and these credentials could have easily allowed access to other parts of Verizon’s internal network and infrastructure.”

Ouch. The AWS bucket belonged to a Verizon Wireless engineer and it did not belong to nor was it managed by Verizon itself, according to the report. Kromtech alerted the engineer about the exposed data, and the situation was immediately rectified.



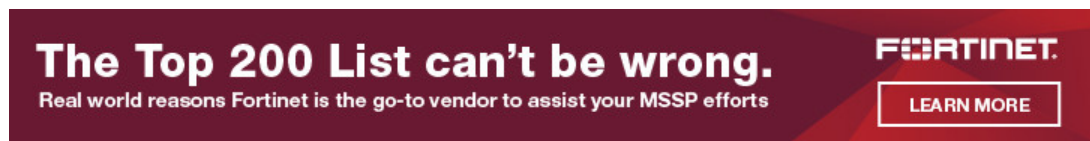
Consider the value of **ZERO** nights and weekends lost to a breach.
It's time to redefine the value of zero. BlackBerry | CYLANCE **LEARN MORE**

Amazon AWS Cloud Data & Security Leaks: Quite Common

A growing number of Amazon-related cloud data leaks have been reported in recent months. In each case, the issue typically involved users who poorly configured their AWS accounts, rather than an Amazon cloud design bug.

AWS cloud leak victims in 2017 have included:

- [14 million Verizon records were left exposed](#) in an earlier leak unrelated to this one
- [Sensitive personal files of thousands of U.S. military and intelligence personnel](#)
- [4 million Time Warner Cable customer records were exposed](#)
- [WWE database leak with 3 million customer records](#)
- [A Republican database with information on 200 million voters](#)
- [Dow Jones suffered a similar AWS exposure](#)



The Top 200 List can't be wrong.
Real world reasons Fortinet is the go-to vendor to assist your MSSP efforts **LEARN MORE**

Holding AWS Account Owners Accountable?



Zohar Alon

Security experts are calling public cloud users to more effectively monitor and manage their account settings.

“Given the high number of incidents involving exposed S3 buckets that we have seen in the past few months, it is baffling that every organization is not carefully looking into the configurations and exposure levels of their storage in the cloud.” said Zohar Alon, co-founder and CEO, [Dome9](#). “Protecting data in the cloud from accidental exposure and theft is a business priority.

Moreover, companies need to be held highly accountable for their lack of security on the public cloud, Alon asserted. So far, that certainly hasn’t been the case.

Related MSSP Lists and Content

- [Top 100 Managed Security Services Providers: MSSP Research and List](#)
- [Gartner Magic Quadrant for MSSPs](#)
- [Gartner Top 10 Cybersecurity Consulting Companies](#)

- [Top 100 Vertical Market MSPs](#) (ChannelE2E Rankings)
- [Top 50 Amazon Web Services MSPs](#) (ChannelE2E Rankings)

[Return Home](#)



No Comments

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website


☐ Save my name, email, and website in this browser for the next time I comment.

☐ Notify me of followup comments via e-mail. You can also [subscribe](#) without commenting.

- [Privacy Statement](#)

All contents © 2020 MSSP Alert and After Nines Inc.

**PURPOSE-BUILT
CYBER-SECURITY
FOR MSPs**




Layered security saves you time, money, and resources

TRIAL NOW

WEBROOT
an aquantix company

**PURPOSE-BUILT
CYBER-SECURITY
FOR MSPs**



Layered security saves you time, money, and resources

TRIAL NOW

WEBROOT
an aquantix company