

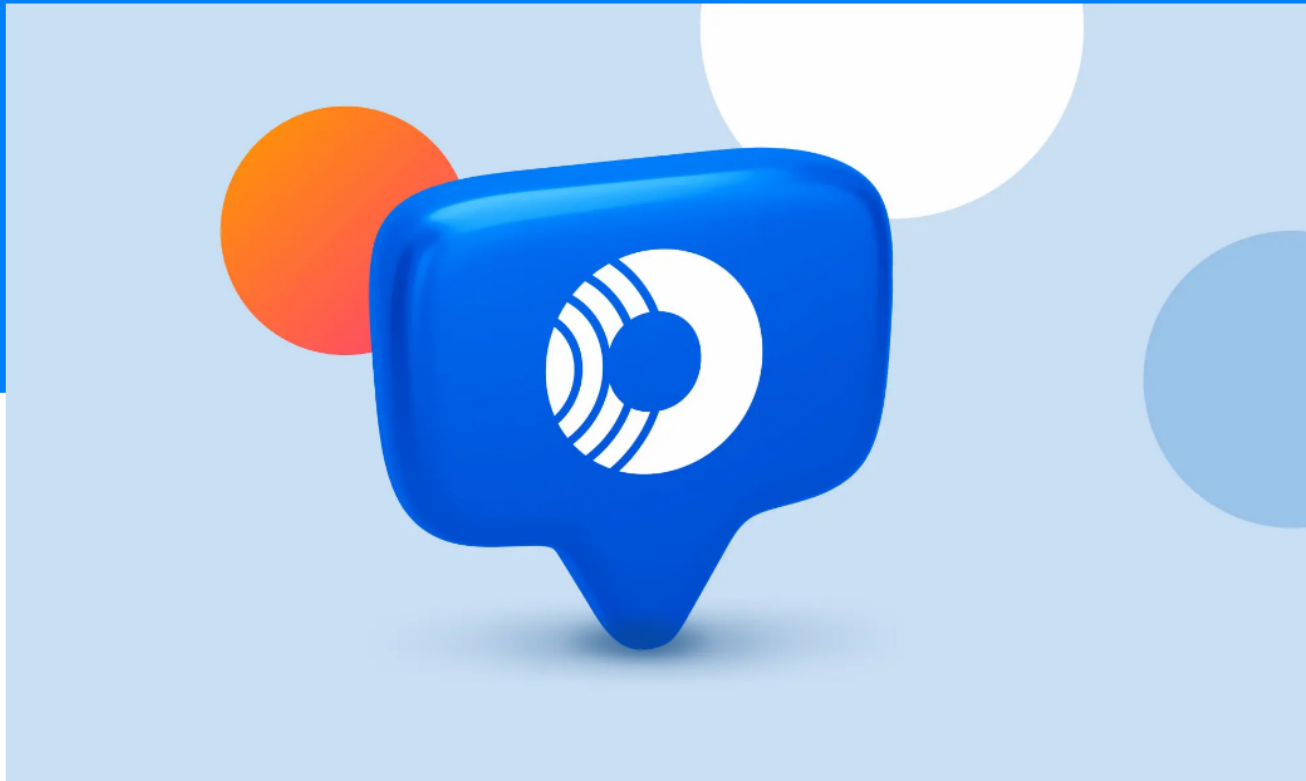
[BLOG](#)
[PRODUCT INFO](#)

FEB 13, 2020

How Orca's Cloud Security Solution Detects Weak Passwords


[Avi Shua](#)

| Reading time: 6 Minutes

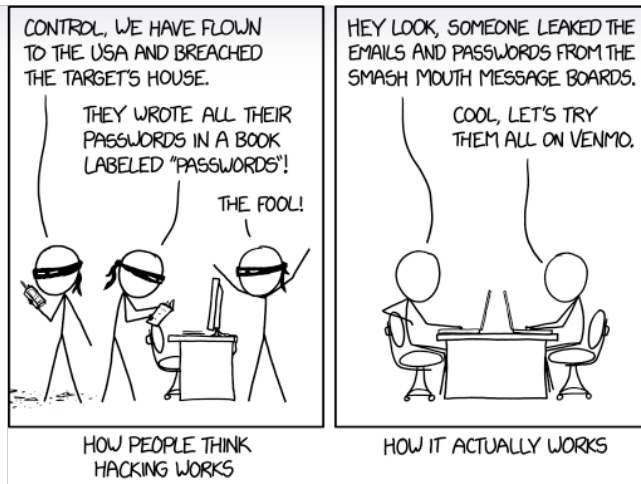


Weak passwords are detrimental to any organization's security. This holds for commonly used passwords, passwords that are complex but are reused across services and applications, and even highly secure passwords that have been leaked.



Orca Security Ltd.
Exhibit 2180
Wiz v. Orca
IPR2024-01190

Ex. 2180-001



(image credit – <https://xkcd.com/2176/>)

We strongly advocate for strong authentication methods on top of passwords, such as biometrics and multi-factor authentication, to boost password security.

Having said that, to be effective, these methods must be applied consistently throughout the entire organization. And enterprises need a way to verify that this is the case.

Often, enterprises will put tremendous effort into ensuring that their main services are secured correctly with multi-factor authentication and certificates while neglecting password security best practices when it comes to 'side services.'

Often, the users of these services and applications are left to their own devices, and as a result end up relying on plain passwords and practicing poor cyber hygiene.

Types of Password-Based Attacks

Password-based attacks come in many shapes. The following common types of attack can be prevented with stronger authentication methods.

Bruteforce Attack

To break into a specific account, a hacker uses a script to attempt to login with all possible password combinations. Brute force accounts don't start randomly; they begin with the easiest-to-guess and most commonly used passwords.

Password Spraying

A more opportunistic type of attack, password spraying attempts to break into any account from a large number of accounts matching the known usernames with a few commonly used passwords.

As a result of massive stolen credential dumps that have been happening recently, high-volume password-spraying campaigns attempting to break into companies' cloud accounts are becoming increasingly common.

Password-spraying attacks are extremely dangerous because they often allow hackers to break into accounts without being locked out or triggering an alert to the IT team.

Because password-spraying attacks don't generate an alarm or lock out a user account, a hacker can continually attempt to match usernames with common passwords until they succeed.





Password-spraying attacks are extremely dangerous because they often allow hackers to break into accounts without being locked out or triggering an alert to the IT team.

Because password-spraying attacks don't generate an alarm or lock out a user account, a hacker can continually attempt to match usernames with common passwords until they succeed.

Credential Stuffing

This attack takes advantage of the fact that many users reuse login credentials across services. An attacker will use leaked username/password combinations from an unrelated service, attempting to login to the company's cloud account with the same credentials.

The attacker is hoping that some fraction of leaked credential users and the targeted organization will have some users in common who are guilty of reusing passwords.

Credential stuffing is challenging to detect. Often, the only indication the victimized company has that they are being attacked is the rise in the overall volume of login attempts.

Even then, the company will have difficulty stopping these attempts without impacting the ability of legitimate users to log in to the service.

When successful, all of the attacks mentioned above can be extremely detrimental to a cloud-based organization.

How Orca Prevents Breaches Due to Weak Passwords

Solving brute force and credential stuffing attacks with SideScanning™ and Fuzzy Search

The screenshot displays the Orca Security console interface. The main panel shows an alert titled 'Weak Password' with a summary, a query, an attack path, and a timeline of events. The timeline includes a failed login attempt, a password change, and a subsequent login. The right sidebar shows the 'BASTION' instance details, including its status, name, and associated cloud accounts.

To stay one step ahead of the hackers and bolster password security, Orca's patent-pending SideScanning™ technology accesses the organization's block storage.

It then attempts to match discovered passwords to commonly used passwords and known leaked password databases.

For common passwords, we also perform offline brute force attacks to test how easy it is for a threat actor to break into the company's accounts.

Next, we perform a fuzzy search on the username in our extensive leaked password database. For the fuzzy search, we use the [Damerau-Levenshtein edit distance algorithm](#).

By fuzzy search, we mean, for example, that for the username `john.doe@acme.com`, we will try to match





to create the company's accounts.

Next, we perform a fuzzy search on the username in our extensive leaked password database. For the fuzzy search, we use the [Damerau-Levenshtein edit distance algorithm](#).

By fuzzy search, we mean, for example, that for the username johndoe@acme.com, we will try to match passwords from john.doe@acme.net, johndoe@gmail.com and so on.

All of the passwords we discover will be checked against the hashed password to see if it matches. We then send an alert to the customer of their breached password and location.

How Does Fuzzy Search Work?

The primary metric for fuzzy search is edit distance.

For example: "cat" and "bat" are edit distance 1 because we only need to substitute c→b. "run" and "burn" are edit distance 2, insert "b" and swap u & r.

We deploy fuzzy search instead of exact search because many users use similar but not identical usernames and passwords across services and accounts.

This happens due to availability, human cognitive limitations, as well as company policies.

For example, the same user might technically not "reuse" an identical password across services and have a relatively strong password, while leaving their account vulnerable and easy to crack, like, Victory@19 and Victory@20.

Our extensive database of leaked credentials contains passwords, usernames, emails, and nicknames. To detect vulnerable passwords, we specifically use the Damerau-Levenshtein distance algorithm.

The algorithm measures how many edits (deletion, inserts, substitutions, and transpositions) are required to transform word1 to word2.

Our fuzzy matching breaks down the target identifiers into words, and then it tries to match those to the target words.

For example, if we had an entry in the database for john.doe@gmail.com, we will break it into "john," "doe," "gmail," "com." We will try to match to "john" "doe" but not to "gmail" & "com" since they are not unique enough.

Solving the Password Reuse Problem with Orca

Thanks to SideScanning™ technology and Fuzzy Search, we can discover vulnerable passwords that are not necessarily an exact match.

We locate similar credentials and notify our customers when those passwords need to be strengthened or if they were involved in an outside breach.

Orca's intelligent alerts give users a better recommendation for their password security, providing a roadmap to tighter security posture.

Real-world examples: An Orca Security customer was running a vulnerable Internet-facing file server that was used to communicate sensitive data with clients. Unfortunately, the admin password for the service was an easy to crack password and username combination.

Orca's SideScanning™ technology located the weak credentials and suggested that the customer change their server passwords in order to secure their data.

In another case, a customer had a bastion server used by employees, which utilized SSH on their production servers.





their server passwords in order to secure their data.

In another case, a customer had a bastion server used by employees, which utilized SSH on their production servers.

One of the employees had his personal email credentials leaked. Orca's SideScanning™ technology was able to match the password to the employee, thereby preventing compromise to the organization.

We've seen that these serious security policy violations happen far more frequently on services where the rest of the security guidelines aren't followed, and therefore, miss the integration and installation of agent based security tools.

SideScanning™ scans every single workload with no per asset integration, which enables organizations to see into their entire cloud infrastructure.

Interested in learning more? [Schedule a demo](#) to see where you are exposed.



Related articles



BLOG

Unveiling Agentless and Dynamic Reachability Analysis to Dramatically Reduce Cloud Risks

Moti Peretz, Ashleigh Lee | Apr 22, 2025



BLOG

CVE is Not Dead, Yet: MITRE CVE Program Status in 2025



Bar Kaduri | Apr 16, 2025

Stay in the loop

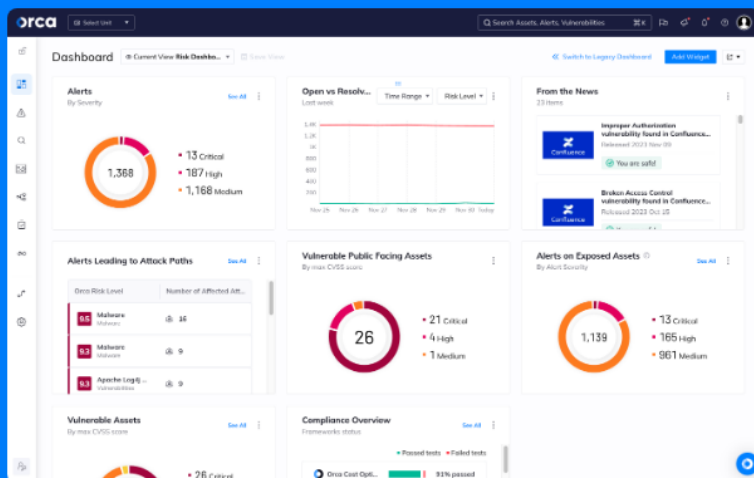
Keep up to date with everything you need to know about cloud security and our latest research

This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

Submit

By submitting my email address I agree to the use of my personal data in accordance with Orca Security [Privacy Policy](#).





PERSONALIZED DEMO

See Orca Security in Action

Gain visibility, achieve compliance, and prioritize risks with the Orca Cloud Security Platform.

[Get a Demo](#)

Platform

CLOUD SECURITY PLATFORM

Cloud Native Application Protection
Vulnerability Management
SideScanning™ Technology
Container and Kubernetes Security
Cloud Security Posture Management (CSPM)
Cloud Infrastructure Entitlement Management (CIEM)
Cloud Workload Protection Platform (CWPP)
AI Security Posture Management (AI-SPM)
Multi-Cloud Compliance and Security
Cloud Detection and Response (CDR)
Application Security
API Security
Data Security Posture Management (DSPM)
Orca Sensor

Solutions

BY SOLUTION

Malware Detection
Sensitive Data Detection
IAM Risk
Lateral Movement Risk

BY INDUSTRY

Financial Services
Technology
Government
Media & Entertainment
Healthcare
Retail

Resources

Library

Product Info
Podcast
Case Studies
Blog
Events

COMPARISONS

Prisma Cloud
Qualys TotalCloud
Lacework
Rapid7
Tenable
Check Point

Company

About
Partners
Reviews
Orca Research Pod
Careers
Newsroom
Media Kit

Contact

Support

Security Portal

User Center

Login

Stay in touch

Get cloud security insights and the latest Orca news

[Submit](#)

Awards & Certifications

- ✓ AWS Advanced Technology Partner Security Competency
- ✓ ISO/EC 27001 Information
- ✓ ISO/EC 27017 Information
- ✓ ISO/EC 27018 Information
- ✓ SOC 2 TYPE II Certified
- ✓ 2022 AWS Global Security Partner





Platform

CLOUD SECURITY PLATFORM

Cloud Native Application Protection

Vulnerability Management

SideScanning™ Technology

Container and Kubernetes Security

Cloud Security Posture Management (CSPM)

Cloud Infrastructure Entitlement Management (CIEM)

Cloud Workload Protection Platform (CWPP)

AI Security Posture Management (AI-SPM)

Multi-Cloud Compliance and Security

Cloud Detection and Response (CDR)

Application Security

API Security

Data Security Posture Management (DSPM)

Orca Sensor

TECHNOLOGY ECOSYSTEM

Integrations

Amazon Web Services

Microsoft Azure

Google Cloud Platform

Oracle Cloud

Alibaba Cloud

Solutions

BY SOLUTION

Malware Detection

Sensitive Data Detection

IAM Risk

Lateral Movement Risk

BY INDUSTRY

Financial Services

Technology

Government

Media & Entertainment

Healthcare

Retail

Resources

Library

Product Info

Podcast

Case Studies

Blog

Events

COMPARISONS

Prisma Cloud

Qualys TotalCloud

Lacework

Rapid7

Tenable

Check Point

Company

About

Partners

Reviews

Orca Research Pod

Careers

Newsroom

Media Kit

Contact

Support

Security Portal

User Center

Login

Stay in touch

Get cloud security insights and the latest Orca news

* Email Address

Submit

Awards & Certifications

- ✓ AWS Advanced Technology Partner Security Competency
- ✓ ISO/EC 27001 Information
- ✓ ISO/EC 27017 Information
- ✓ ISO/EC 27018 Information
- ✓ SOC 2 TYPE II Certified
- ✓ 2022 AWS Global Security Partner of the Year
- ✓ Star Level One: Self-Assessment Cloud Security Alliance
- ✓ CSA Trusted Cloud Provider Cloud Security Alliance

