Adlumin

DARKNET EXPOSURE MODULE

24/7 Search for Leaked Accounts on the Deep and Dark Web

Adlumin's **Darknet Exposure Module** has the ability to extend defensive capabilities beyond your firewalls, endpoints, and security devices into Russian ID theft forums and the criminal underground. Adlumin protects all domain accounts with automatic notifications and password resets if a business account is leaked.

Credential Theft

Stolen credentials and account takeover are growing at an alarming speed. According to the 2019 Verizon Data Breach Report, 80 percent of hacking-related breaches leveraged compromised and weak credentials. Additionally, the National Institute of Standards and Technology (NIST) has set requirements for federal systems to check passwords against exposed credentials, and they encourage non-governmental organizations to do the same.

Key Features

- Ability to force a password reset for a high or critical risk account before next sign-on
- Alerts users about where your data was found on the web
- Available on Adlumin's platform at no extra cost
- Doesn't require any action by security staff
- Immediately notifies users with leaked account information
- Provides insight on how to avoid leaked information in the future
- Users can review, search, and analyze all breach events in the database

Adlumin

Surface, Deep & Dark Web

The **surface web** is anything that can be indexed by a typical search engine like Google, YouTube, or Bing.

The **deep web** is an underground internet, or the portion that is not indexed by traditional search engines, and is much larger than many realize. In fact, major sites like Facebook, Wikipedia, etc. found through a search engine make up less than one percent of the internet.

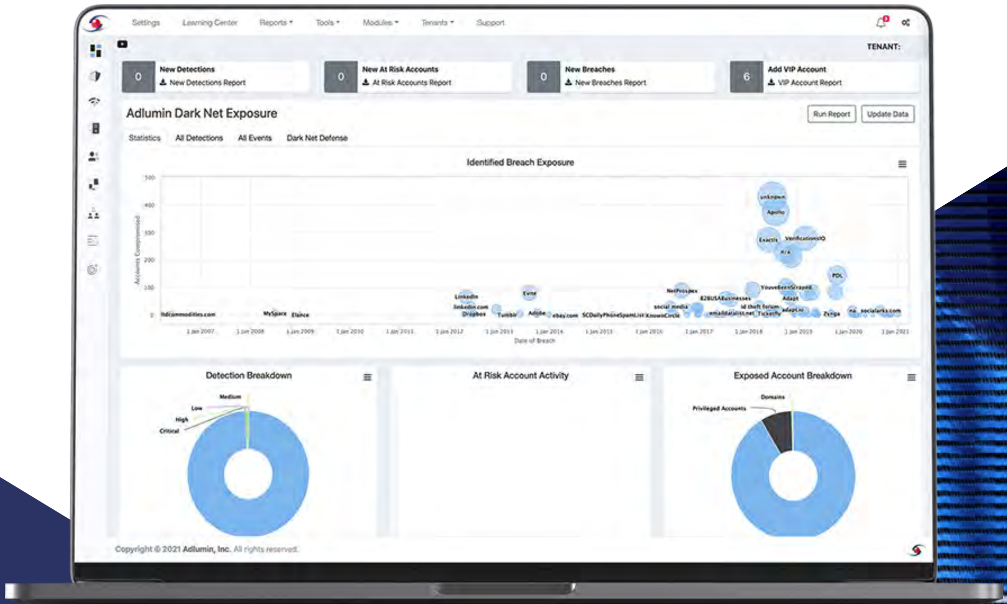
The **dark web** is a subset of the deep web, which is intentionally inaccessible from normal browsers. It is hidden by The Onion Router (TOR) network but is accessible via a TOR browser.

Deep & Dark Web Leaked Account Scanning

The Adlumin platform and OEM partners work collectively with data to measure risk associated with specified data breaches or credential leaks to help prevent account takeovers and credential stuffing attacks. For **critical** (*privileged accounts*) and **high** (*unprivileged accounts*) severity breaches, our platform also determines when a leaked account is potentially useable on the protected network. Adlumin can initiate an automated victim notification (to include the user and security team), and force a password reset of the business domain account that was leaked.

How Adlumin Protects Customers Against Breaches

Adlumin knows the exact date and time that every account on your network last changed its password. Our security analytics platform enhances that data with information about if (and when) your account(s) were exposed on the internet (e.g. deep or dark web). If an account was exposed and the last password change precedes the exposure date, it is at extreme risk for being used by an intruder to access your network.



0	New Detections New Detections Report
0	New At Risk Accounts At Risk Accounts Report
0	New Breaches New Breaches Report
6	Add VIP Account VIP Account Report

Adlumin Dark Net Exposure