ALLURE SECURITY

Managed Dark Web Monitoring

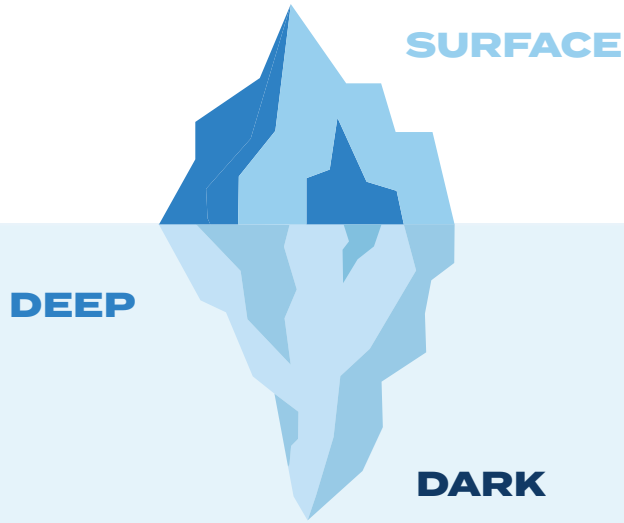
Actionable results curated through comprehensive dark web monitoring

Highlights

- **Detect compromised credentials and leaks of sensitive data**
- **Pre-empt and quickly mitigate scams** by identifying mentions of your brand, assets, products, employees, and users on cybercrime channels, marketplaces, and more
- **Authenticated, account-level access** to more deep and dark web channels for deeper visibility
- **Accelerate response** with curated, relevant results, contextual analysis of cyberattacks, and recommendations for taking action
- **Save time, money, and effort** by receiving only accurate findings with expert curation instead of sifting through petabytes of deep and dark web data
- **Demonstrate your commitment to keeping users safe** by informing them of the exposures of their PII even in breaches unrelated to your organization

Threats to You & Your Users Reside on the Dark Web

Because they allow people to post content and communicate anonymously, cybercriminals use the deep and dark web to discuss, share, and sell information used to carry-out and monetize online scams. It's estimated that more than 90% of the internet's content resides in these hidden layers – looking at the surface web alone is not enough to head off scams targeting your users:



Surface Web: The part of the internet most of us interact with each day through traditional browsers and internet search engines

Deep Web: Generally, internet content that's not indexed by or accessible through search engines (e.g., content requiring authenticated access)

Dark Web: Content hosted on anonymous networks accessible via specialized software such as customized browsers

Detect & Respond to Scam Precursors & Effects

Cybercriminals use deep and dark web communications channels to discuss and sell scam tools, materials, and intelligence. By identifying mentions of your organization in cybercrime forums, marketplaces, and chat groups, you can detect scams before they launch or uncover exposed data from past incidents involving your employees or users.

For example, on deep and dark web channels, fraudsters will post and sell phishing kits ("scams-in-a-box") or phishing services targeting financial institutions and other organizations. Such phishing kits and services give even unsophisticated attackers the ability to target your user base at scale with little effort. Identifying such threats can help you ensure you're prepared for such schemes.

Or, criminals will publish or sell "dumps" of compromised PII, banking credentials, and more. This may be data about your users captured in other breaches but making it easier for scammers to target your customers or members with credential harvesting scams. Knowing this information is exposed can help you be proactive against such threats or make users aware of the potential exposure of their data to demonstrate how seriously you take protecting them.

A Better Way to Monitor the Dark Web

Allure Security managed dark web monitoring provides comprehensive, continuous collection and analysis of the evolving deep and dark web. While this hidden internet's exact size is dynamic, older estimates suggest it exceeds 7,500 terabytes. The scale and specialized tools required put effective monitoring and analysis beyond the reach of most organizations.

Many cybersecurity teams are overwhelmed by the volume of results provided by dark web monitoring tools. And, 65% of CISOs say they lack in-house threat intelligence skills making reams of results laden with false positives inactionable and of questionable value.

A Forrester study estimated that an organization that chose threat intelligence services over building the capability in-house gained an average of $263,250 in annual productivity and realized a 428% ROI. Increased productivity, data breach cost avoidance, reduced fraud losses, and less time spent investigating false positives all factored into the ROI calculation.

Because we provide dark web monitoring as a service; your team receives only relevant, actionable results curated by experienced cybersecurity professionals. Our team includes experts from leading credit bureaus and cybersecurity testing and research firms who have also collaborated with the U.S government to fight cybercrime.

Our managed dark web monitoring service includes the collection of more than 228,000 web pages every hour, adding to a constantly growing dataset. Our service also goes deeper than most providers, going beyond landing pages with authenticated, account-level access. The extent of our dataset combined with expert vetting ensures you can efficiently identify and action mentions of your organization and users on the deep and dark web.

Snapshot of Allure Security's Dark Web Monitoring Data Set

9B+ Email Addresses	**4.9B+** Plain-text Passwords	**38M+** Payment Cards
564M+ Tor Records	**8M+** I2P Records	**52M+** Telegram Chats

Sample Use Cases

- Mitigate consumer account takeover by identifying and taking action on compromised user accounts and payment cards
- Mitigate employee account takeover and unauthorized access to corporate systems and assets by identifying and taking action on compromised employee accounts
- Find and stop threats targeting your executives, employees, and users in the earliest phases of attack by identifying related "chatter," target lists, and other information
- Pre-empt fraud and optimize detection by identifying phishing kits targeting your organization and users for sale on criminal marketplaces

Components of Allure Security Managed Dark Web Monitoring

With our managed dark web monitoring service you receive the following without having to build or maintain your own threat intelligence capabilities:

- Round-the-clock monitoring of the channels and sources listed below including authenticated access to various forums, marketplaces, and more
- Expert validation of the data and findings categories listed below to ensure accuracy and relevance
- Intuitive, actionable reporting that organizes findings along with contextual information telling you why the findings matter to you, how they affect your risk posture, and what you can do about them

Channels and Sources Monitored

Managed dark web monitoring analyzes a wide range of high-risk surface, deep, and dark web channels and sources with authenticated access including but not limited to:

- Paste sites
- Discord
- Telegram
- Internet Relay Chat (IRC)
- FTP servers
- Amazon S3 Buckets
- Cybercrime forums & marketplaces
- Tor, I2P & Zeronet-accessible documents
- OpenNIC - alternative root DNS system (e.g., .chan, .bbs, etc.)

Data & Findings Categories

Allure Security managed dark web monitoring identifies and reports on various types of sensitive data including but not limited to:

- Exposed employee and user credentials
- Domains (email, internal, websites)
- Executives' personal email addresses
- Social Security Numbers
- Common Vulnerability and Exposures (CVE) identifiers
- Public IP addresses & ranges
- Bank Identification Numbers (BINs)
- Payment card numbers
- Cryptocurrency wallet addresses
- Consumer health records
- Brand & keyword mentions

Comprehensive Protection with the Allure Security Suite

Combining Allure Security managed dark web monitoring with GlobalBlock+ and online brand protection-as-a-service, you gain complete detection and mitigation capabilities across all stages of scams targeting your organization and users – before, during, and after.

Before

GlobalBlock+

- One-stop defense against unauthorized parties registering available domains similar to your brand
- Automatically capture domains similar to your brand if they become available, expire, or are deleted

Brand Protection as-a-Service

- Monitor for impersonating content using AI across the web, social media, mobile app marketplaces, and more
- Find and eliminate online scams in testing phases, before a single person falls victim
- Continual monitoring of suspicious domains including those that previously hosted scams

Managed Dark Web Monitoring

- Receive early warning of scams based on chatter, target lists, tools for sale, etc.

During

Brand Protection as-a-Service

- Use AI to identify impersonating content across the web, social media, mobile app marketplaces, and more
- Find and eliminate online scams before a single person falls victim
- Take immediate action to add scams to ecosystem blocklists warning visitors of danger
- Disrupt the monetization of any stolen data by automatically inputting realistic but useless information (decoy data) into phishing forms
- Take down scams in minutes for comprehensive response that renders scams inaccessible

After

Brand Protection as-a-Service

- Continual monitoring of domains even after takedown to ensure they don't come back online
- Decoy data for use in victim tracking, incident investigation, attribution, and more

Managed Dark Web Monitoring

- Identify compromised employee and user accounts to mitigate damage
- Identify compromised payment cards for reissuance