livingsecurity

BUSINESS RISK

ACCOUNT COMPROMISE

22% Of U.S. adults have been victims of account takeover.[1]

Challenge

An exponential increase in the number of consumers using fintech services and digital channels has increased the global attack surface making it more lucrative for Account Takeover (ATO), or online identity theft to occur. Fraudsters steal personally identifiable information (PII) through successful social engineering, credential stuffing, account enumeration, and account validation attempts. Account Takeovers can be very dangerous and the damage can be damaging to the individual as well as their employing organization.

Solution

Living Security's Unify, a Human Risk Management solution, captures relevant insights and data points to arm security teams with the intelligence to decrease human risk exposure and observe the workforce taking a proactive defense.

Capabilities:

- Understand the users with weak or common passwords.
- Identify credential reuse patterns across multiple accounts.
- Learn who is clicking links and downloading attachments from unfamiliar sources.
- Track MFA usage.

Outcome

As a result of tracking and surfacing these insights your organization will **feel confident that you are protecting your brand's reputation and employees from harm.**

[1] Javelin Strategy

Actionable insights improve cyber culture and reduce human risk including the ability to:

- Decrease the number of cyber incidents.
- Boost confidence in your defenses
- Improve security awareness of users.
- Reduce negative impacts to the brand.

Integrations

Connect the following technology with Unify to understand, track, and reduce successful account takeover attempts from occurring among your workforce.

- Single Sign-on
- Multi-Factor Authentication (MFA)
- Password Manager
- Breach Data

View featured integration providers

Insights Uncovered

Surface intelligent insights to drive change in your organization and reduce the likelihood of a successful Account Takeover.

- Credential compromise & management
- Account logon analytics
- MFA enrollment usage
- Training performance

Account Compromise

- **Identify segments & individuals** susceptible to Account Takeover
- **Identify methods of Account Takeover** pose the largest risk
- **Create a targeted remediation plan** to address these pockets of risk

Objectives

- **Reduce likelihood of account takeover**
- **Decrease compromised credential dwell time**
- **Reduce enterprise credential reuse**
- **Increase password manager installation & usage**

Behavior Change

- Usage of **weak or common passwords**
- **Credential Reuse** across multiple accounts
- **Clicking links** & **downloading attachments** from unfamiliar sources
- **Multi-factor Authentication** Usage

Insights

- **Credential Compromise** & Management
- **Account Logon** Analysis
- **MFA Enrollment** Usage
- Training **Performance**

Integrations

- **Single Sign-On** (e.g. Okta, Sailpoint)
- **Multi-Factor Auth** (e.g. Duo, Okta, Ping)
- **Password Manager** (e.g. 1Password)
- **Breach Data** (e.g. SpyCloud, HIBP)

LEARN HOW
TO MEASURABLY REDUCE YOUR ORGANIZATION'S HUMAN RISK

Get Started!

About Living Security

Living Security's mission is to transform human risk to drive dramatic improvement in human behaviors, organizational security culture, and infosec program effectiveness. With our Human Risk Management platform, Living Security engages each employee with innovative and relevant context and content, while simultaneously providing the ability for leadership to identify, report on and directly mitigate the risk brought on by human behavior. Living Security is trusted by security-minded organizations like MasterCard, Verizon, MassMutual, Biogen, AmerisourceBergen, Hewlett Packard, and Target.

livingsecurity