SpyCloud

CHECKLIST FOR PREVENTING IDENTITY-BASED ATTACKS

A proactive approach to holistic identity threat protection

Cybercriminals are exploiting the massive digital trail users leave online across their personal and professional lives. This vast trove of exposed identity data – from usernames, passwords, and personally identifiable information (PII) to device info, session cookies, and more – is scattered across the darknet, waiting to be weaponized against your organization.

While your enterprise is limited to the data you manage within your infrastructure, threat actors don't have these boundaries. They harvest identity data from **breaches, malware, and phishing campaigns**, stitching the pieces together to impersonate users and bypass your defenses.

To fight back, defenders must correlate exposed identity data across time, systems, and users to stop targeted attacks before they happen. A **holistic** view of your current and past employees, suppliers, and consumers' exposure can help you better prevent identity-related attacks.

IDENTITY EXPOSURE IS MASSIVE

SpyCloud has recaptured more than **795 billion** total stolen assets, including valuable identity data from the criminal underground that can be used to fuel cybercrime.

THE TRUE SCALE OF EMPLOYEE IDENTITY EXPOSURE IS VASTLY UNDERESTIMATED

A traditional approach to identity exposure uncovers an average of only 11 records, 1 unique username, and 7 stolen credential pairs per corporate user, compared to **146 records, 22 unique usernames, and 141 credential pairs** uncovered with a holistic identity approach.

CONSUMER IDENTITY EXPOSURE IS MIND-BOGGLING

Each consumer has on average, **229 exposed records** ranging from Social Security numbers and dates of birth to financial data, including 52 unique usernames, 27 unique emails, 227 credential pairs, and more.

MALWARE-EXFILTRATED DATA CREATES HIDDEN RISKS

About **1 in 2 corporate users** has already been a victim of an infostealer malware infection, which silently infiltrates devices and extracts identity data attackers use for account takeover, fraud, ransomware, and other cybercrimes.

HOLISTIC IDENTITY THREAT PREVENTION CHECKLIST

Use this checklist to adapt your prevention strategy in the face of threat actor tactics.

- [ ] **Educate employees about modern identity threats**

  Train and educate employees about common identity attack vectors like phishing emails and malicious attachments. Make sure security teams are aware of new infostealer malware technology like **LummaC2 Stealer** that can exfiltrate sensitive data, including active sessions and cookies, passwords, autofill information, and even desktop files.

- [ ] **Enforce strong passwords to protect employee and customer accounts**

  Enforce **strong password practices**, like banning commonly used or easily guessable passwords that include words like your company or even popular culture references. Encourage using a password manager to create and store strong passwords for corporate accounts and automatically detect and reset exposed passwords.

- [ ] **Monitor for stolen cookies, enforce MFA, and enforce timebound user sessions**

  It's crucial to have access to compromised session cookie data associated with your domains so you can invalidate sessions and prevent session hijacking attacks. Implement MFA in combination with limited session length for additional layers of protection, plus automatically terminate user sessions after a specific time to shorten the window of opportunity for attackers to bypass MFA using stolen cookies.

- [ ] **Build holistic identity intelligence into your onboarding and user login workflows**

  Understanding the comprehensive exposure of users, employees, and customers enables you to verify legitimate users and account access holistically and detect possible fraud during new account signups. Use the same data to understand the risk of your users whose data has been exposed and can be used to perpetrate fraud and account takeover.

- [ ] **Remove blindspots in personal and unmanaged devices**

  If you can't implement security policies to prevent network access from personal devices, **detect any malware-infected devices** outside corporate control used by employees, contractors, and vendors. Unknown malware-exfiltrated data of your users leaves your organization vulnerable to malicious access.

- [ ] **Shut down third-party application entry points**

SpyCloud research shows that a single malware infection can expose access to as many as **25 business applications**. Prevent criminals from exploiting this access by resetting compromised credentials of applications beyond your primary domain, including password managers, CRMs, chat programs, ticketing systems, HR and payroll platforms, and other jumping-off points that could be used to gain access and escalate privileges across the network.

- [ ] **Monitor your partners and supply chain for darknet exposures**

Use identity threat intelligence to uncover entry point risks related to your vendors, partners, and suppliers and prioritize your security controls. Notifying your vendors early about the significant malware, phishing, and breach exposures affecting them helps them avoid follow-on attacks that target their organization and yours.

- [ ] **Optimize your Zero Trust policy engine**

Traditional Zero Trust implementations authenticate users only during initial access to the network, which doesn't account for identities that are exposed outside your corporate view by malware and other threats. Integrate exposure insights into your **Zero Trust policy engine** so you can continuously monitor for compromised identities and remediate threats automatically.

- [ ] **Accelerate incident response investigations**

During an incident, it is critical to rapidly correlate selectors like emails or usernames to broader identity data – PII, system details, and access patterns – to uncover initial access vectors and assess the scope of the attack. Automated holistic identity analytics speeds up investigations dramatically, shaving hours off the clock and enabling faster, deeper insights even from junior analysts.

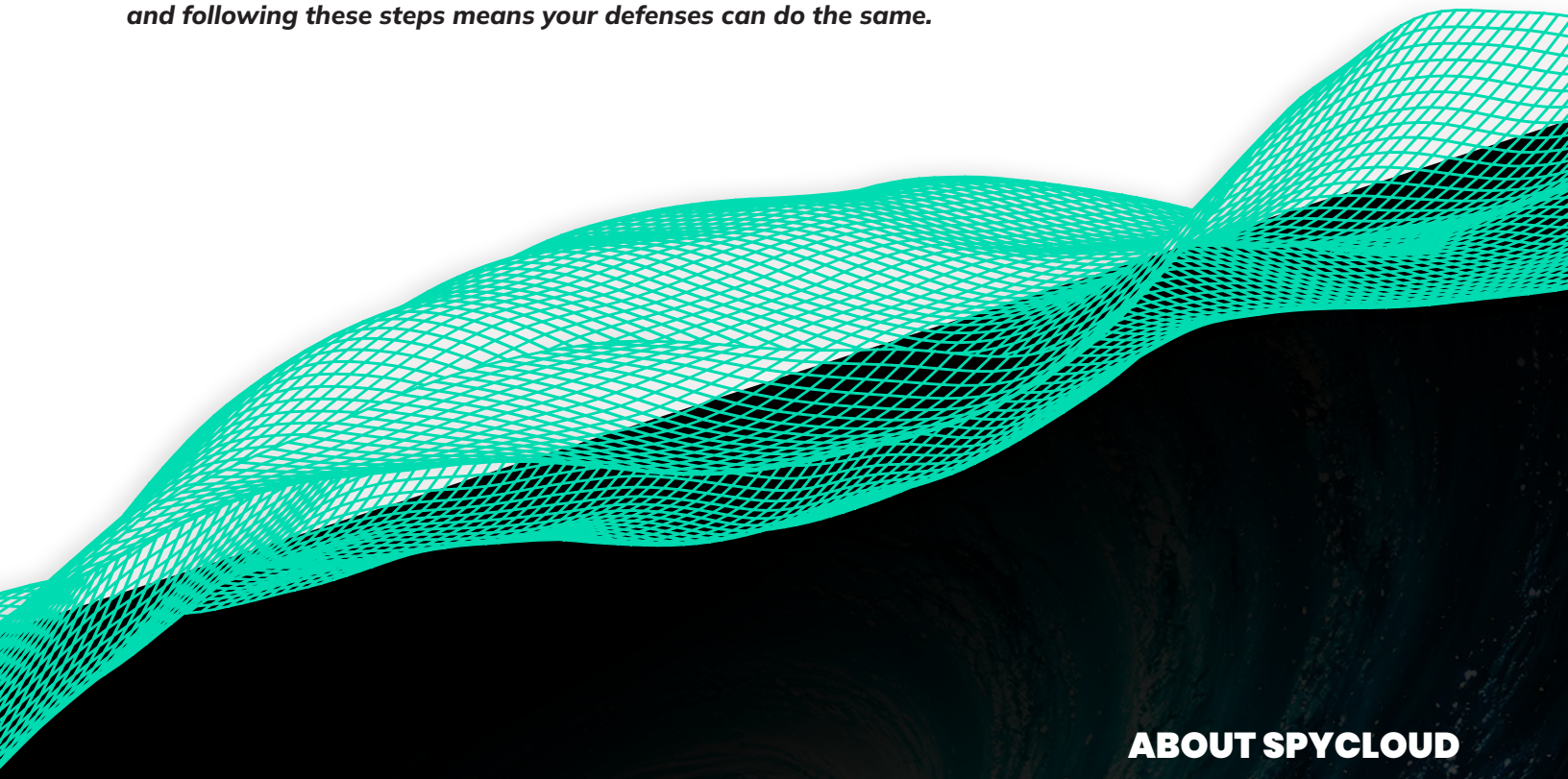
- [ ] **Automate remediation workflows**

Where possible, integrate high-priority breached, phished, and malware-exfiltrated data into automated workflows within your SIEM, SOAR, IdP, and EDR platforms to remediate identity exposures quickly and prevent targeted attacks.

- [ ] **Shift to holistic identity threat protection**

Identity-centric threat protection enables you to protect holistic identities in ways that weren't possible before. A comprehensive view of data exposed from breaches, malware infections, and phishing campaigns correlated to users across all their online personas – past and present – puts you on an even footing with threat actors who are using this data against your enterprise.

Detect and remediate exposed identities of employees, vendors, and contractors early, automating remediation as much as possible. This approach will reduce your unseen and unknown risks and make stolen data useless to threat actors. Cybercriminals have moved beyond user accounts – ***and following these steps means your defenses can do the same.***



ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics to proactively prevent ransomware and account takeover, safeguard employee and consumer accounts, and accelerate cybercrime investigations. SpyCloud's data from breaches, malware-infected devices, and successful phishes also powers many popular dark web monitoring and identity theft protection offerings. Customers include seven of the Fortune 10, along with hundreds of global enterprises, mid-sized companies, and government agencies worldwide. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to protect businesses and consumers from the stolen identity data criminals are using to target them now.

To learn more and see insights on your company's exposed data, visit **spycloud.com**