

# ENDPOINT THREAT PROTECTION

DETECT & REMEDIATE MALWARE-EXPOSED IDENTITIES  
TO PREVENT RANSOMWARE

## THE CHALLENGE

Organizations struggle with clear visibility into the identity exposures of their users stemming from malware infections across their entire ecosystem. Hidden risks to business applications from infected devices - managed, under-managed, or BYOD devices - create unnoticed entry points for bad actors. These exposures allow attackers to walk right in your front door, without needing a key - leading to account takeover, ransomware, and other targeted identity-based attacks. Blind confidence in securing access through a device-centric approach leaves security teams vulnerable to the high risk attacks perpetrated as a result of stolen identity data and access.

## PRODUCT OVERVIEW

**SpyCloud Endpoint Threat Protection** supercharges ransomware prevention through a holistic identity threat protection approach. With visibility into the full breadth of exposed identities – past and present, work and personal – caused by hard-to-detect malware infections, security teams can act on a more complete scope of exposures from infostealer malware infections, regardless of the device, or whether it falls within standard corporate controls. By analyzing exposure risks at the holistic identity level, including compromised application credentials and session cookies, security teams gain a clear understanding of the risks and gaps that expose corporate access points. Armed with enriched identity data and automated playbooks, security teams can quickly remediate threats, significantly reducing MTTD and MTTR – stopping cybercriminals from exploiting stolen identity data once and for all.

## BENEFITS AT A GLANCE

### Identify Threats Outside of Corporate Control

Detect exposed identity data and application access from managed, unmanaged, and BYOD devices to adopt a holistic identity threat protection approach

### Illuminate Visibility Into Exposed Access

Identify third-party applications exposed by malware infections, like SSO platforms, security tools, ticketing systems, and more, that could be exploited as entry points for cyberattacks

### Shortcut The Remediation Process

Assess the scope of a potential threat, drastically reduce MTTD and MTTR, and prioritize remediation with direction from the malware infection details to shut down entry points

### Bolster Malware-Infection Response

Address exposed identities directly in existing workflows to enhance your current incident response playbooks by seamlessly integrating into your preferred tools for remediation, triage and orchestration

## POST-INFECTION REMEDIATION: A COMPLETE APPROACH

**SpyCloud's Post-Infection Remediation** introduces preventative, identity-focused steps to malware infection response – designed to negate opportunities for ransomware and other critical threats. Armed with definitive evidence of entry points into the enterprise and enriched identity data, security teams can reset compromised application credentials to prevent their use in future attacks.

With SpyCloud's Post-Infection Remediation approach, you can disrupt cybercriminals attempting to harm your business, significantly shorten your exposure window, and stop malware exposures from becoming full-blown security incidents.

## HOW IT WORKS

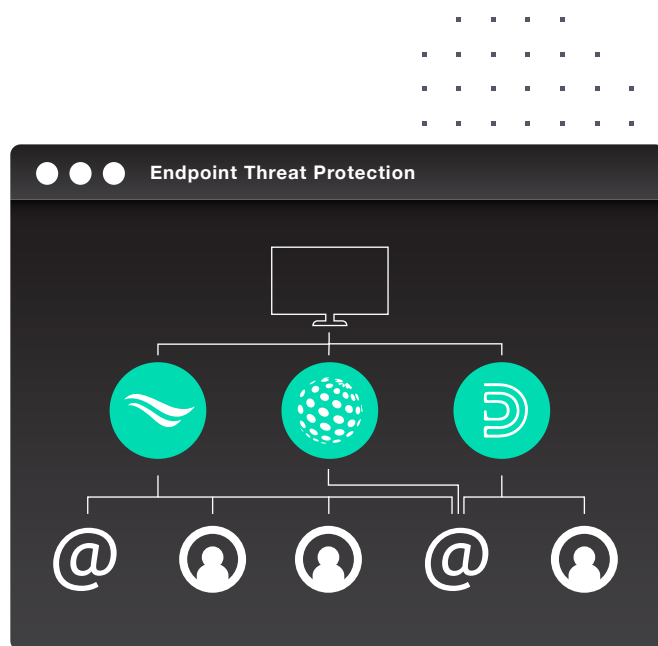
**SpyCloud Endpoint Threat Protection** helps you proactively prevent ransomware, by identifying definitive evidence of identity compromise, including malware-infected devices and exposed application access. Endpoint Threat Protection closes gaps in your malware protection framework to detect and respond to high-priority

**Endpoint Threat Protection identifies infected devices and applications connected to your organization** by monitoring malware records for the target domains and third-party subdomains you choose. For example: mycompany.com, login.mycompany.com.

**Endpoint Threat Protection maps out the infection origination and path with full insight to exposure insight.** This allows you to understand the scope of a potential threat at-a-glance, across all devices, business-critical applications, and users.







**Endpoint Threat Protection provides detailed information on each exposure** to shortcut your investigation steps and enables you to quickly implement Post-Infection Remediation for malware-infected users, devices, and applications.

- ▶ Malware: malware type, infection path, and source
- ▶ User details: username, device name, OS, and IP address
- ▶ Time: date and time of infection, and publish date
- ▶ Application Details: application name and URL
- ▶ Cookies: unique count and name of stolen cookies



## KEY CAPABILITIES

---

-  **EXPOSED APPLICATION VIEW**  
View all third-party applications exposed by each infostealer, including shadow IT apps accessed with personal or corporate email address
-  **MANAGED DEVICES AND BYOD**  
Pinpoint the exact managed or unmanaged device infected by malware that was used to access corporate applications
-  **HIGH FIDELITY ALERTS**  
Get definitive evidence that stolen identity data tied to your organization is in criminal hands, early in the attack lifecycle
-  **INTERACTIVE GRAPHS**  
Visualize the full scope of identity-based risks, including infected devices, users, and applications with enriched data
-  **INTUITIVE PORTAL**  
Analyze details of each malware infection along with powerful visualizations that create an effective exposure remediation plan
-  **STOLEN COOKIES**  
Remove blindspots in ransomware prevention with visibility into unauthorized access to business applications via malware-exfiltrated authentication cookies

## OUT-OF-THE-BOX API WORKFLOW INTEGRATIONS

---

### EDR INTEGRATIONS

Gain instant visibility into corporate devices exposed to malware with SpyCloud's EDR integrations. Detect infections that bypass your existing security measures and tools, preventing malware sprawl.



### SIEM / SOAR INTEGRATIONS

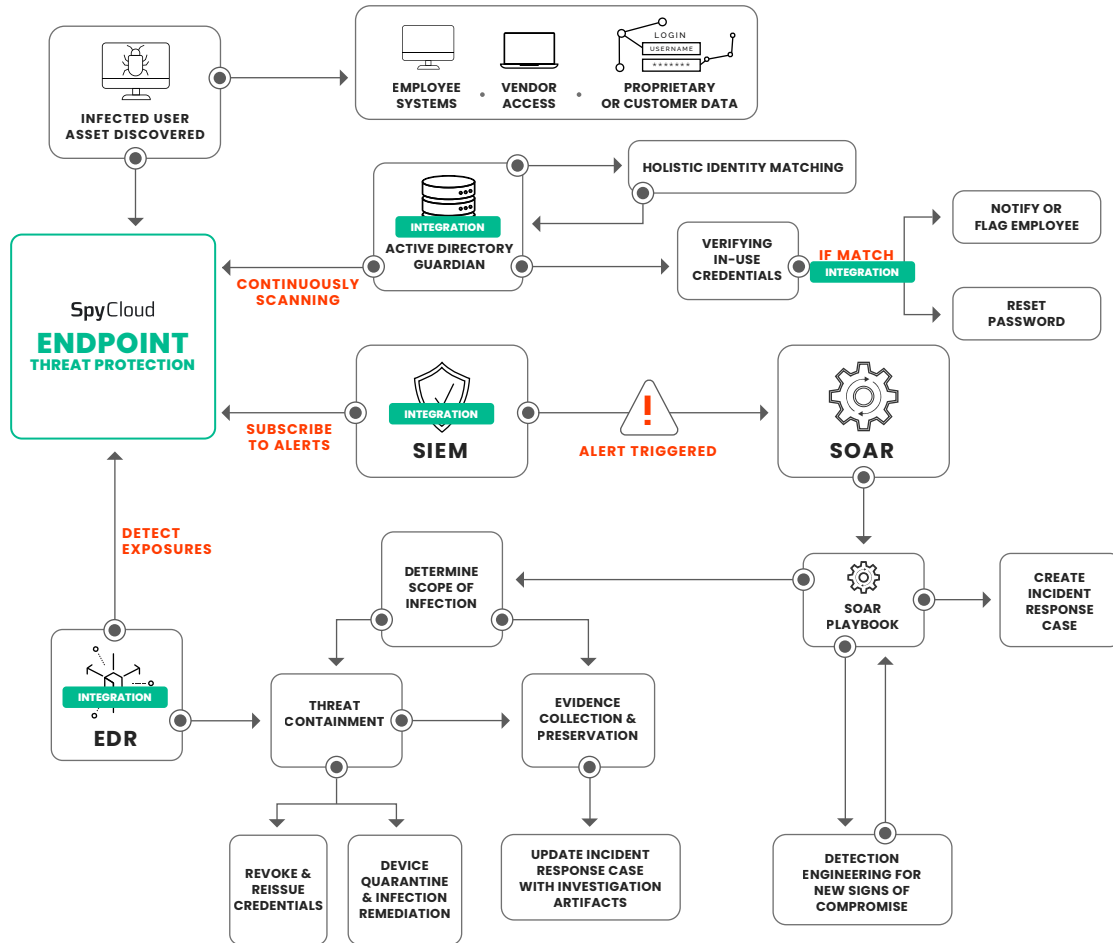
Enrich SIEM and SOAR events with detailed SpyCloud breach and malware data to optimize post-infection remediation workflows. SpyCloud's integrations automatically generate alerts and critical incidents for new exposures tied to your organization. With SpyCloud's integrations, gain extended enrichment and pre-built playbooks to better assess identity threats and automate triage and response.



## EXAMPLE WORKFLOWS FOR MALWARE DETECTION AND REMEDIATION INCLUDE:

- ▶ Using device details, list of applications, cookies names, and usernames to determine if an active employee is exposed
- ▶ Using the infected path and email address to identify the specific employee associated with the malware infection
- ▶ Using hostname, machine OS version, or IP address to correlate malware infections with your corporate managed assets
- ▶ Using subdomain and usernames to target corporate applications to reset credentials and session cookies
- ▶ Using actionable identity data that matches device hostnames, guiding containment, or automatically quarantining high-risk devices

### Post-Infection Remediation Example



## ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics and AI to proactively prevent ransomware and account takeover, detect insider threats, safeguard employee and consumer identities, 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](https://spycloud.com)