DATASHEET

SpyCloud

COMPASS

THE ENTERPRISE NORTH STAR IN NAVIGATING RANSOMWARE PREVENTION THROUGH POST-INFECTION REMEDIATION

THE CHALLENGE

Organizations lack end-to-end visibility into the attack surface across their entire technology ecosystem — such as infostealer malware-infected devices, compromised users, stolen cookies, and exposed applications. These entry points allow bad actors to walk right into an organization's network and challenge security teams to effectively reduce the risk of a successful ransomware or cyberattack.

PRODUCT OVERVIEW

Compass delivers a new approach to ransomware prevention that addresses both the reactive and proactive states security teams have to operate within today's modern enterprise – maximizing visibility of an enterprise's attack surface across the entire technology ecosystem to act on malware-compromised devices, users, and applications. Compass empowers teams to prevent targeted cyberattacks by acting on what criminals know about the business from infostealer infections, typically invisible exposures on personal devices, under-managed contractor devices or even managed employee devices accessing the corporate network. With complete coverage and instant discovery of infection impact, SecOps teams can rapidly deploy mitigation tactics that drastically decrease MTTR to eliminate the risk of cybercriminals profiting off of stolen authentication data.

BENEFITS AT A GLANCE

IDENTIFY THREATS OUTSIDE OF CORPORATE OVERSIGHT

Gain visibility into threats outside of corporate control, including unmanaged devices that are used by employees to access shadow IT alongside company applications

ILLUMINATE YOUR ATTACK SURFACE

Identify third-party applications exposed by a malware infection, including SSO, security tools, ticketing systems, payroll systems, and more that could serve as entry points for targeted cyberattacks

SHORTCUT THE INVESTIGATION PROCESS

Assess the scope of a potential threat at-a-glance, reduce MTTD, and quickly prioritize high-risk device and application exposures

BOLSTER MALWARE INFECTION RESPONSE

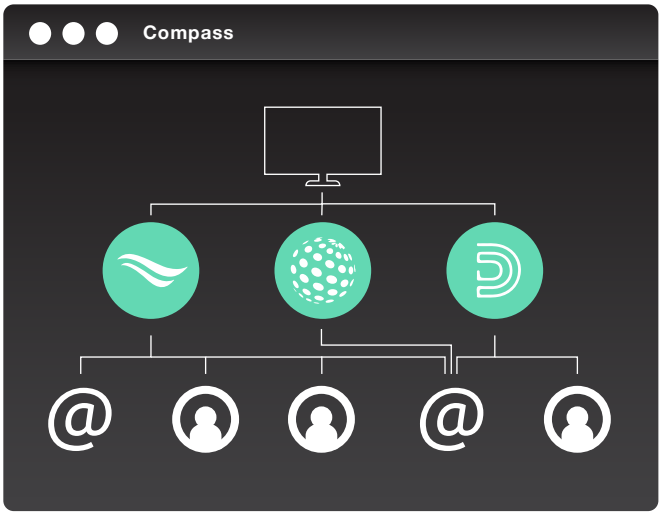
Optimize your incident response and evolve from a machine-centric to an identity-centric malware response process that truly reduces ransomware entry points and decreases MTTR

SpyCloud

POST-INFECTION REMEDIATION: A MORE COMPLETE APPROACH

Post-Infection Remediation is SpyCloud's crucial addition to malware infection response — a series of preventative steps designed to negate opportunities for ransomware and other critical threats. Armed with definitive evidence of entry points into the enterprise from Compass, security teams can reset application credentials and invalidate session cookies siphoned by malware to prevent their use in future attacks. With Compass and Post-Infection Remediation, you can disrupt cybercriminals attempting to harm your business, significantly shorten your exposure window for targeted cyber attacks, and effectively stop malware exposures from becoming full-blown security incidents.

HOW IT WORKS



Compass helps you proactively prevent ransomware by identifying definitive evidence of malware-infected devices, along with exposed users and applications that cybercriminals use to walk right into your network. Fill the gaps in your malware protection framework to detect and respond to high-priority threats to your network.

Compass 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, vpn.mycompany.com, sso.mycompany.com.

Compass maps out what has been exfiltrated by the infection(s), including the credentials and session cookies for critical business applications. This allows you to understand the scope of a potential threat at-a-glance.

Compass provides detailed information on each exposure to shortcut your investigation steps and enables you to quickly implement Post-Infection Remediation.

- 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

SpyCloud

KEY CAPABILITIES

EXPOSED APPLICATION VIEW

View all third-party applications that were exposed by each infostealer, including shadow IT apps accessed with either personal or corporate email address

MANAGED DEVICES AND BYOD

Pinpoint the exact malware-infected managed or unmanaged device that was used to access corporate applications

HIGH FIDELITY ALERTS

Get definitive evidence that stolen data tied to your enterprise is in criminal hands, with alerts of new exposures

INTERACTIVE GRAPHS

Visualize the scope of a potential threat, including infected devices, users, and applications with actionable details

INTUITIVE PORTAL

See thorough details of each infection, along with powerful visualizations that illuminate your remediation action plan

STOLEN COOKIES

View the count and name of stolen cookies associated with your monitored subdomain for the affected applications

Microsoft Sentinel splunk> CORTEX XSOAR BY PALO ALTO NETWORKS tines

OUT-OF-THE-BOX API WORKFLOW INTEGRATIONS

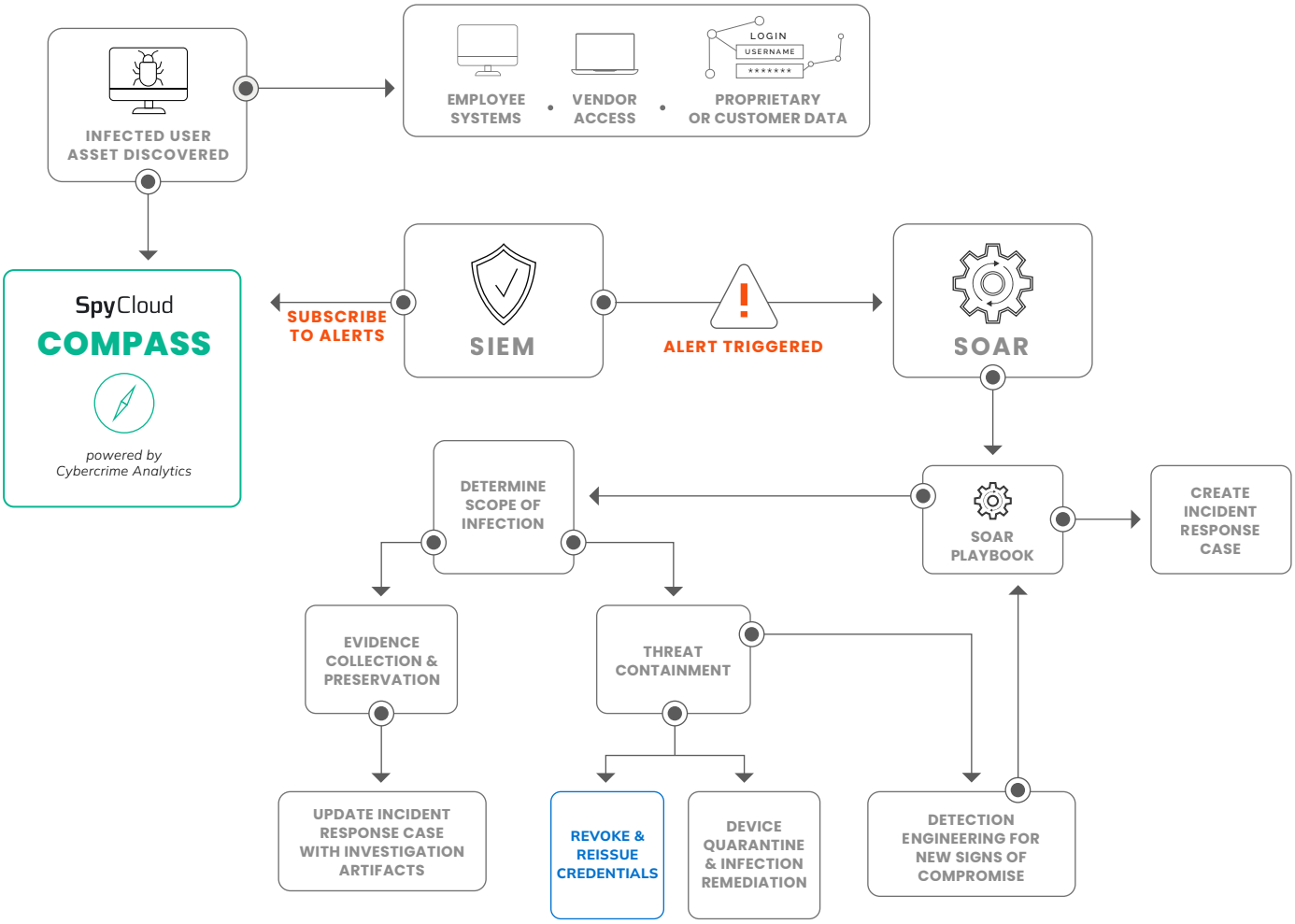
Operationalize Compass data to enrich SIEM and SOAR events with breach and malware information to optimize Post-Infection remediation workflows. SpyCloud automates the creation of alerts and incidents for new breaches and malware infections with Critical Severity. SpyCloud can also integrate with any preferred application via custom integrations.

Example workflows for Compass remediation include:

- Using device details, list of applications, cookies names, and usernames to determine if an employee is infected
- Using hostname, machine OS version, or IP address to correlate malware infections with your corporate managed assets
- Using subdomain and username data to target corporate-hosted or third-party applications to reset credentials

SpyCloud

Example of a Compass Post-Infection Remediation workflow



ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to protect businesses from cyberattacks. Its products operationalize Cybercrime Analytics (C2A) to produce actionable insights that allow enterprises to proactively prevent ransomware and account takeover, safeguard employee and consumer identities, and investigate cybercrime incidents. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to nearly 200 cybersecurity experts whose mission is to make the internet safer with automated solutions that help organizations combat cybercrime.

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