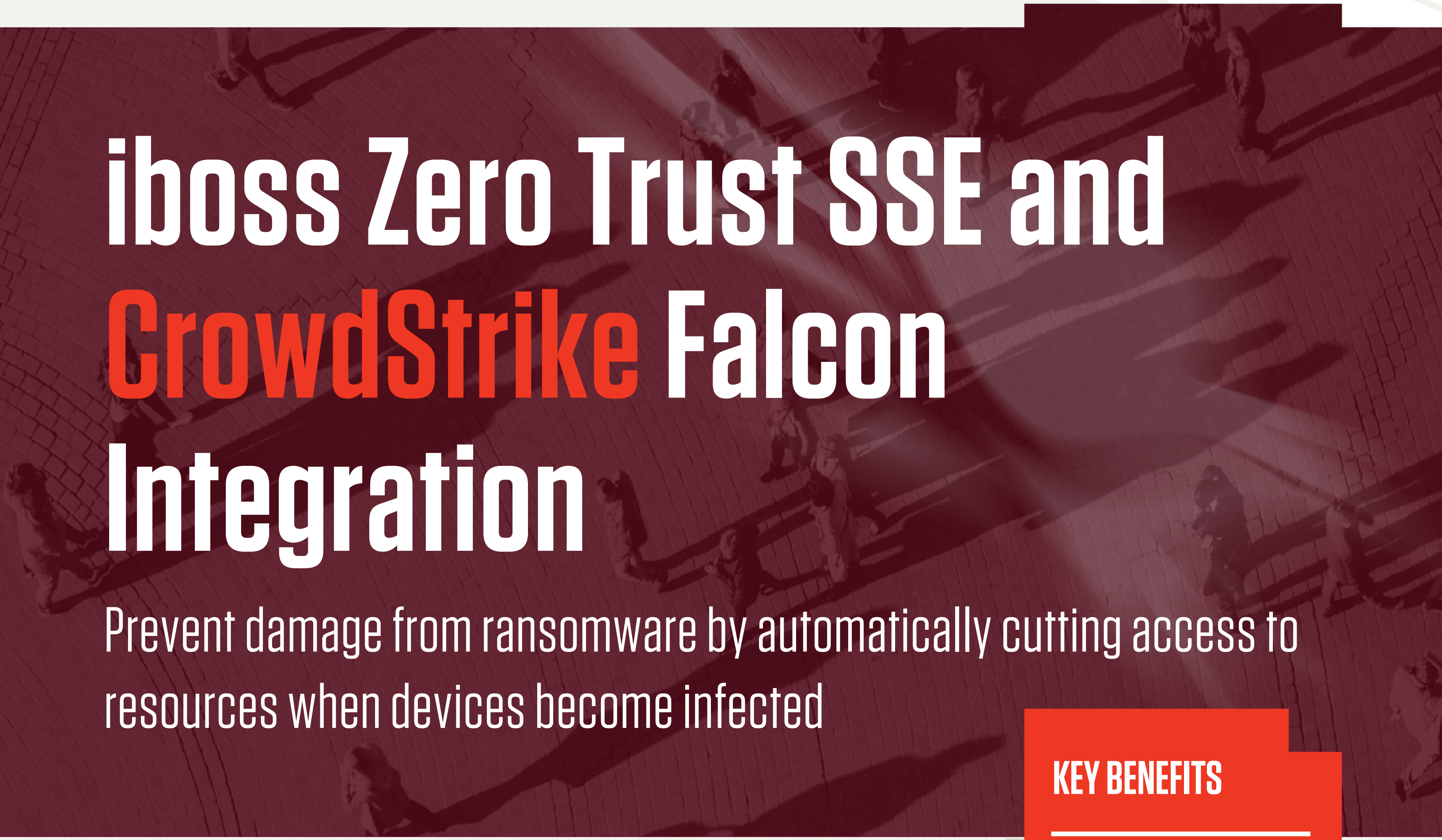
Solution Brief



iboss Zero Trust SSE and CrowdStrike Falcon Integration

Prevent damage from ransomware by automatically cutting access to resources when devices become infected

CHALLENGES:

Long after a device becomes infected, ransomware continues to damage and encrypt sensitive data due to a lack of human resources that can respond to infections quickly. Attackers continue to hijack sensitive data for ransom as they gain access to unauthorized resources without being noticed. With sensitive applications, services, and data scattered across SaaS, cloud infrastructure, and onsite environments causing an increase in attack surface area, it is becoming more challenging to protect valuable assets from breaches and data loss.

Meanwhile, providing remote users access to apps and data from secure devices is critical for reducing risk and meeting compliance, but it can be difficult to automatically take action and cut access to sensitive resources if a device becomes infected or does not meet compliance requirements. For example, security teams may have a lack of visibility and control to ensure the firewall is on, the disk is encrypted, and the device's endpoint protection solution is configured correctly.

KEY BENEFITS

- Automatically cut off access to sensitive enterprise resources when a device becomes infected or an incident risk is high based on the CrowdStrike CrowdScore incident rating
- Automatically cut off or isolate access when the Falcon ZTA risk score indicates high risk
- Automatically cut off or isolate access if a device does not have critical Falcon settings enabled

SOLUTION:

The iboss Zero Trust SSE has been integrated with the CrowdStrike Falcon® platform to deliver automatic actions including the ability to cut off access to sensitive resources when a device becomes infected or is high risk. The iboss Zero Trust SSE provides Zero Trust network access (ZTNA) and security service edge (SSE) capabilities to control access to enterprise resources while applying a cloud access security broker (CASB), malware defense, compliance policies, and data loss prevention (DLP), generating logs for every interaction between users, devices, and sensitive resources. The integration leverages the CrowdStrike Falcon Zero Trust Assessment (ZTA) risk score, which indicates device and user risk, including the likelihood of compromise, and the CrowdStrike CrowdScore®, which assigns scores to incidents according to the incident's severity level.

The iboss Zero Trust SSE integrates with both Falcon ZTA and CrowdScore to ensure that access to sensitive applications and data can be automatically terminated by iboss when scores reach critical levels. This automation requires no additional human intervention as iboss takes immediate action when CrowdStrike detects risk to protect applications and data from damage. iboss seamlessly allows you to control access to sensitive enterprise resources following the NIST 800-207 Zero Trust Architecture principles, leveraging continuous adaptive access trust algorithms that ingest signals from CrowdStrike to trigger automated actions such as cutting off user access to sensitive resources when a device becomes infected.

In addition, with iboss's native browser isolation capabilities, the iboss Zero Trust SSE can automatically add an additional layer of security in front of sensitive apps and data when required. For example, if the Falcon ZTA score indicates a high-risk user or device, the iboss Zero Trust SSE will automatically convert all resource accesses so that they can only be performed through a browser-isolated session. The Falcon ZTA signals are also incorporated into the iboss Zero Trust SSE continuous adaptive access Trust Algorithms, allowing security professionals to adapt access abilities, such as isolating or terminating access, to specific resources depending on which CrowdStrike Falcon capabilities are configured and enabled on a device. The iboss Zero Trust SSE also logs every transaction to every sensitive resource to give the security operation center (SOC) teams the ability to see command and control (C2) infection callbacks and detect potential exfiltration of data from protected applications.

KEY BENEFITS

- Automatically cut off access to sensitive enterprise resources when a device becomes infected or an incident risk is high based on the CrowdStrike CrowdScore incident rating
- Automatically cut off or isolate access when the Falcon ZTA risk score indicates high risk
- Automatically cut off or isolate access if a device does not have critical Falcon settings enabled
- Get log events for every access to sensitive resources to detect data exfiltration attempts
- Apply CASB, malware defense, compliance policies, and DLP to every transaction to complement Falcon's on-device protections

USE CASES / BUSINESS VALUE:

USE CASE / CHALLENGES	SOLUTION DESCRIPTION	BENEFITS
Automatically cut off access to enterprise resources when CrowdStrike Falcon flags a device as infected or compromised.	Leveraging the CrowdScore, the iboss Zero Trust SSE can automatically cut off access to resources when a CrowdStrike Falcon incident reaches a critical level.	Reduce the time between infection and response to minimize the risk of damaging data and applications when a device becomes infected, and reduce overhead for SOCs through automated response actions such as removing access.
Automatically cut off or isolate access to enterprise resources when a device is not compliant or becomes high risk based on the Falcon ZTA rating.	Integration with CrowdStrike Falcon enables the iboss Zero Trust SSE to take action when the Falcon ZTA score indicates high risk; actions can include automatically cutting off access to sensitive resources or adding a pane of glass in front of resources using Browser Isolation.	Reduce the risk of breaches, data loss, and attacks due to high-risk users and devices by automatically and quickly changing access abilities to sensitive enterprise-owned applications, data, and services. Easily isolate sessions to prevent the downloading of data from applications when a user or device is deemed risky.
Automatically re-enable access to enterprise resources when CrowdStrike Falcon incidents are cleared without adding steps or overhead to the SOC.	The iboss Zero Trust SSE automatically clears incidents triggered by CrowdStrike Falcon when those incidents are cleared within the Falcon dashboard, restoring access to enterprise-owned resources automatically.	Automatically grant or deny access to enterprise-owned applications, data, and services while using existing incident workflows created around the CrowdStrike Falcon dashboards.

PAIN POINT

- **Infected Devices Damage Data**

When devices are detected to be infected by CrowdStrike, access to sensitive applications and data must be terminated.

iboss Solution

✓ **Automatically Cut Access When Infections Occur**

The iboss Zero Trust SSE can automatically terminate access based on CrowdStrike incidents that have high risk CrowdScores.

USE CASE / CHALLENGES	SOLUTION DESCRIPTION	BENEFITS
Add a pane of glass to separate users and devices from sensitive resources when users or devices are non-compliant and fail asset posture checks.	The iboss Zero Trust SSE incorporates Falcon ZTA signals and into the iboss continuous adaptive access Trust Algorithms so that if any CrowdStrike Falcon configuration or posture check fails, access to sensitive resources can be cut off or isolated by the iboss Zero Trust SSE.	Ensure that only compliant users and devices can access sensitive resources to meet compliance requirements for device settings such as having the firewall on, the disk encrypted, or the CrowdStrike Falcon agent actively running on the device.
Continuously log for visibility of every user, device, and resource interaction.	The iboss Zero Trust SSE acts as a gatekeeper to all enterprise resources and generates log events for every transaction to applications, data, and services.	Detect data exfiltration attempts and infected device callbacks while users and devices interact with enterprise resources, reducing risk from breaches and data loss.
Apply CASB, malware defense, compliance policies, and DLP to every network transaction to complement on-device protection from CrowdStrike.	The iboss Zero Trust SSE inspects all transactions, including looking inside HTTPS connections, to apply security controls, and prevent breaches.	Reduce risk of breaches and data loss by ensuring sensitive data remains within trusted and approved applications. Ensure that data can only be transferred to enterprise-owned devices and those devices running the CrowdStrike Falcon agent.

PAIN POINT

- **Non-Compliant Devices are High Risk**

When devices are not compliant due to failed CrowdStrike Zero Trust Risk Score assessments, access to sensitive resources should be isolated behind a VDI-like pane-of-glass..

iboss Solution

✓ **Use Browser Isolation to Separate Data**

The iboss Zero Trust SSE includes Browser Isolation to separate non-compliant users from resources based on CrowdStrike Zero Trust Risk Score signals.

KEY BENEFITS:

- Automatically cut off access to sensitive enterprise resources when a device becomes infected or an incident risk is high based on the CrowdStrike CrowdScore incident rating
- Automatically cut off or isolate access when the Falcon ZTA risk score indicates high risk
- Automatically cut off or isolate access if a device does not have critical Falcon settings enabled
- Get log events for every access to sensitive resources to detect data exfiltration attempts
- Apply CASB, malware defense, compliance policies, and DLP to every transaction to complement Falcon's on-device protections

PAIN POINT

- **Need to Adapt Access Based on Risk**

When users and devices access sensitive resources, CASB and DLP controls must be applied that are based on CrowdStrike incidents and Zero Trust Risk Score signals.

iboss Solution

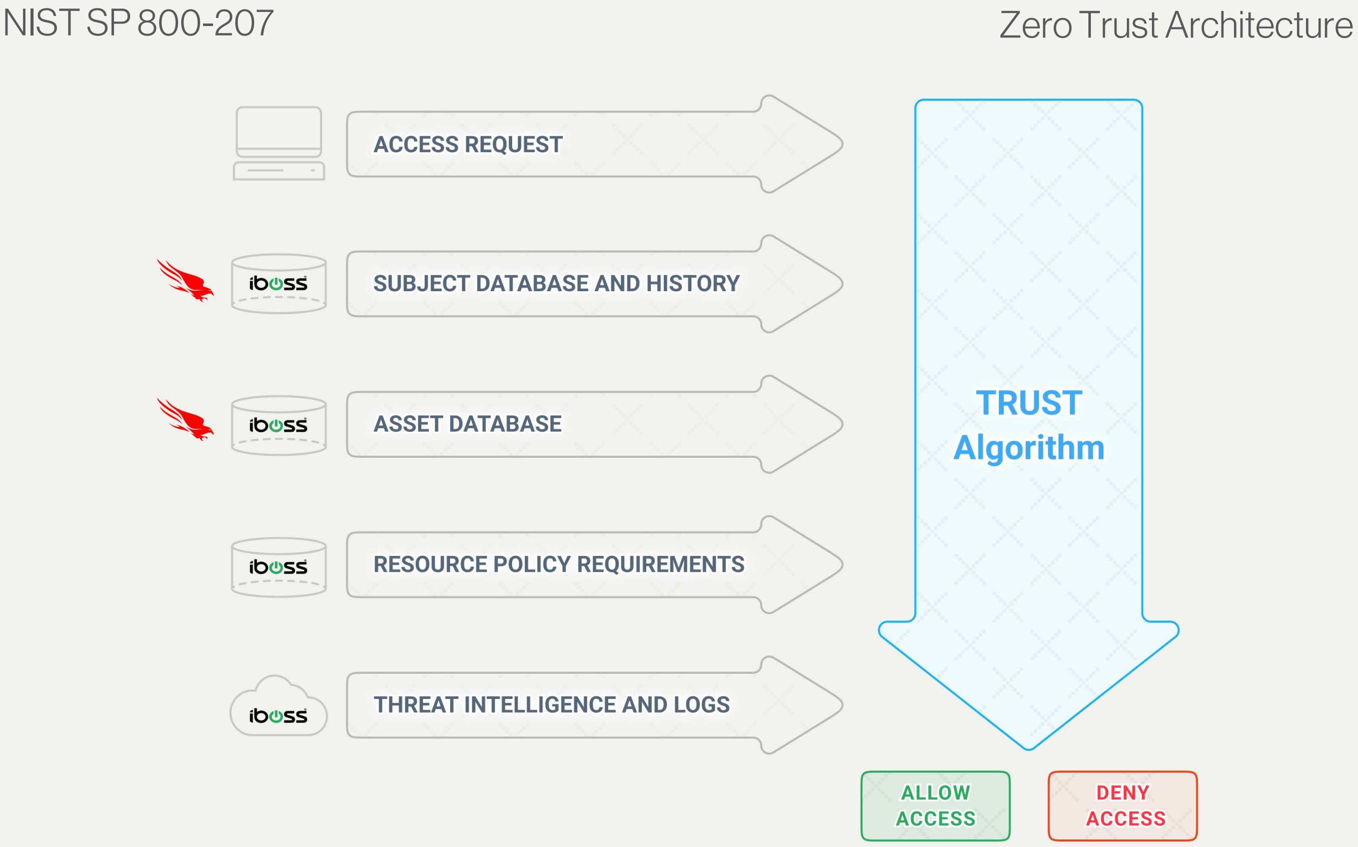
✓ **Adaptive Access, Security & Logging**

The iboss Zero Trust SSE provides continuous adaptive access with a full security stack for access that includes CASB, malware defense, Data Loss Prevention and logging.

TECHNICAL SOLUTION:

The iboss Zero Trust SSE connects with the CrowdStrike Falcon platform to deliver a seamless integration for user, asset, and resource protection. The iboss Zero Trust SSE connects to the Falcon platform using APIs to allow information to be exchanged related to the Falcon ZTA risk scores and CrowdStrike CrowdScore incident levels.

The iboss Zero Trust SSE directly aligns with the NIST 800-207 Zero Trust Architecture which allows it to ingest signals from external sources, such as CrowdStrike, and take action based on the inputs received

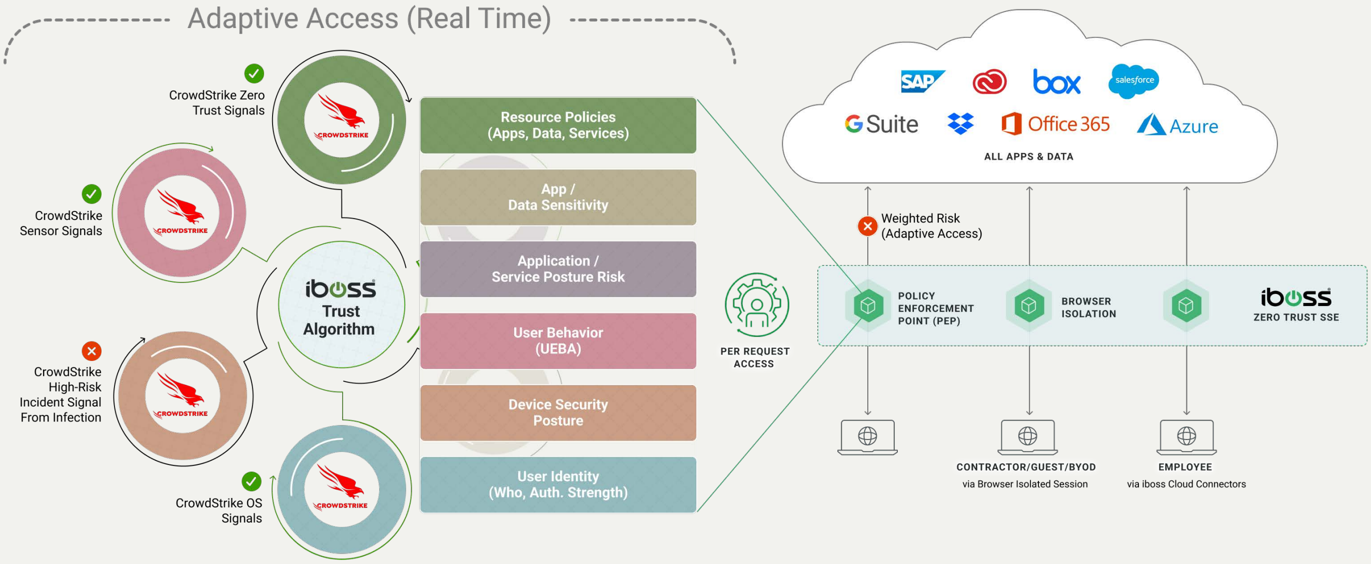


Trust Algorithm Input

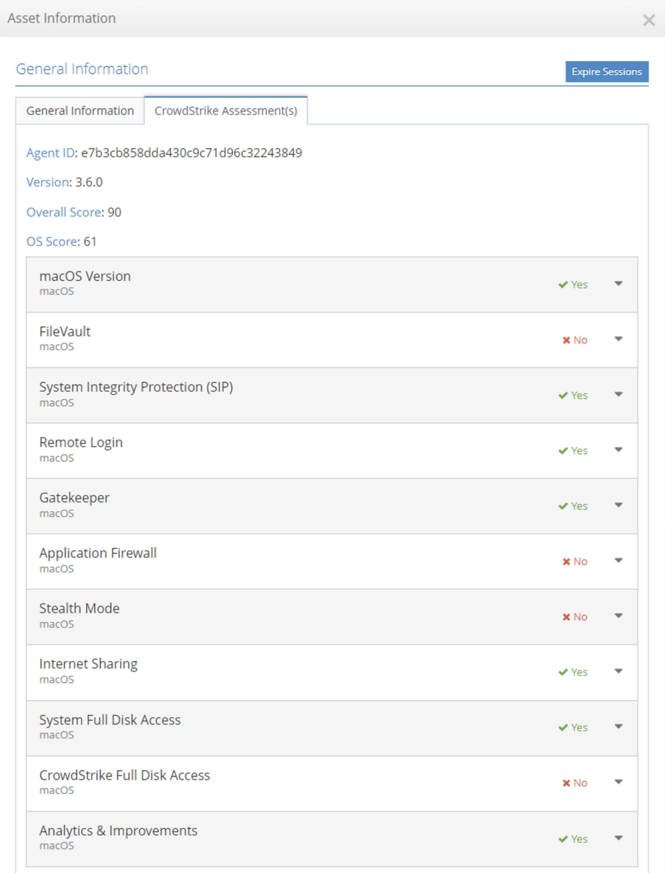
This is accomplished using iboss's continuous adaptive access Trust Algorithm that matches that of the NIST 800-207 that can leverage signals generated from iboss in addition to those from other sources, such as CrowdStrike. These inputs are interpreted for each and every request to protected resources and an action is taken such as blocking or isolating access to the sensitive application or data. This results in real-time protection by ensuring that infected or non-compliant devices cannot access applications, data or services as the iboss Zero Trust SSE automatically handles adaptively changing access decisions

Continuous Adaptive Access: CrowdStrike Integration

Integrates CrowdStrike Signals to Cut Access to Sensitive Resources Automatically


Adaptive Access (Real Time)
CrowdStrike Zero Trust Signals
CrowdStrike Sensor Signals
CrowdStrike High-Risk Incident Signal From Infection
CrowdStrike OS Signals
iboss Trust Algorithm
Resource Policies (Apps, Data, Services)
App / Data Sensitivity
Application / Service Posture Risk
User Behavior (UEBA)
Device Security Posture
User Identity (Who, Auth. Strength)
PER REQUEST ACCESS
SAP
box
salesforce
G Suite
Office 365
Azure
ALL APPS & DATA
Weighted Risk (Adaptive Access)
POLICY ENFORCEMENT POINT (PEP)
BROWSER ISOLATION
iboss ZERO TRUST SSE
CONTRACTOR/GUEST/BYOD
via Browser Isolated Session
EMPLOYEE
via iboss Cloud Connectors

The iboss Zero Trust SSE provides an asset, user, and resource database to track all sensitive resources within the organization. Asset information within the iboss Zero Trust SSE is enriched with Falcon ZTA signals and device posture checks.



Agent ID: e7b3cb858dda430c9c71d96c32243849

Version: 3.6.0

Overall Score: 90

OS Score: 61

macOS Version
macOS
✓ Yes

FileVault
macOS
✗ No

System Integrity Protection (SIP)
macOS
✓ Yes

Remote Login
macOS
✓ Yes

Gatekeeper
macOS
✓ Yes

Application Firewall
macOS
✗ No

Stealth Mode
macOS
✗ No

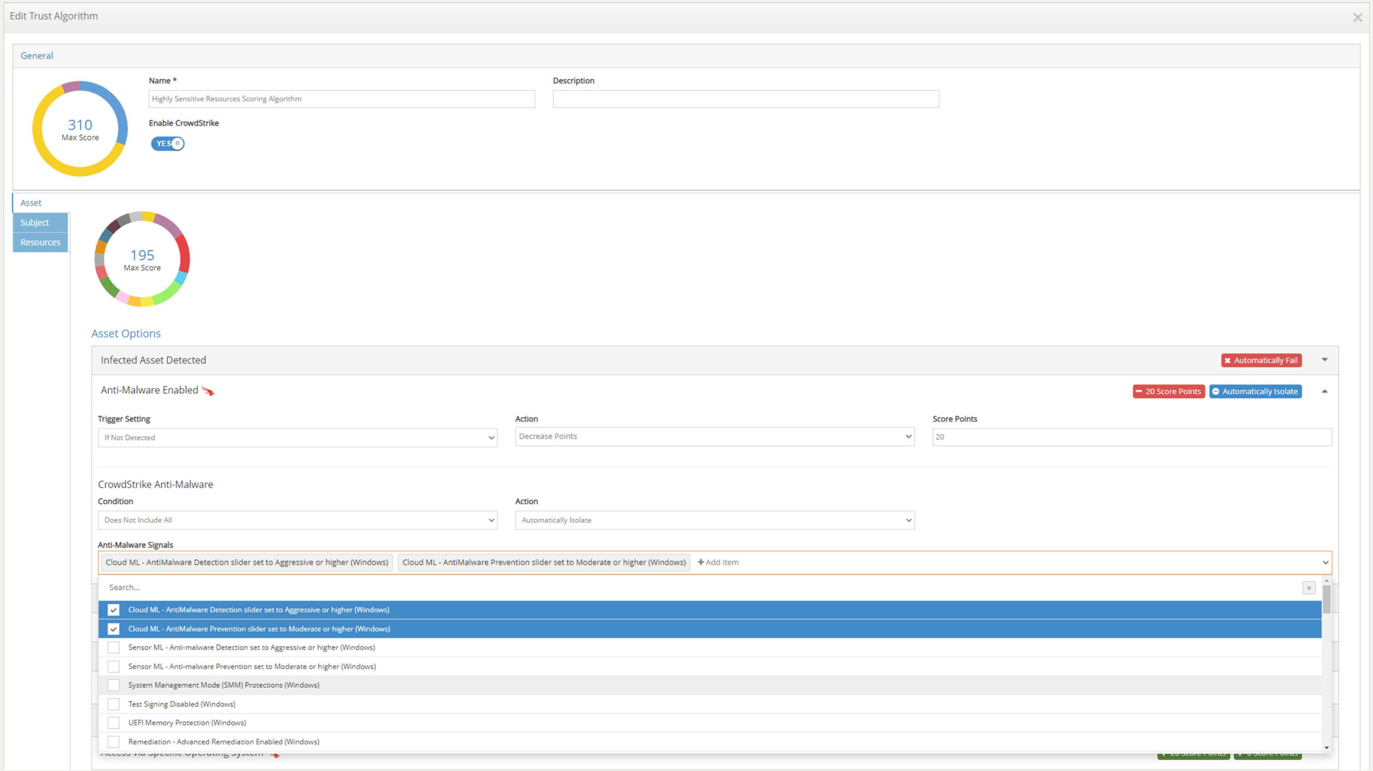
Internet Sharing
macOS
✓ Yes

System Full Disk Access
macOS
✓ Yes

CrowdStrike Full Disk Access
macOS
✗ No

Analytics & Improvements
macOS
✓ Yes

Falcon ZTA signals have been tied to the iboss Zero Trust SSE continuous adaptive access Trust Algorithms, which can take actions, such as cutting off or isolating access, based on CrowdStrike Falcon assessments.



Name *: Highly Sensitive Resources Scoring Algorithm

Description:

Enable CrowdStrike: YES

Infected Asset Detected — Automatically Fail

Anti-Malware Enabled — 20 Score Points — Automatically Isolate

Trigger Setting	Action	Score Points
If Not Detected	Decrease Points	20

CrowdStrike Anti-Malware

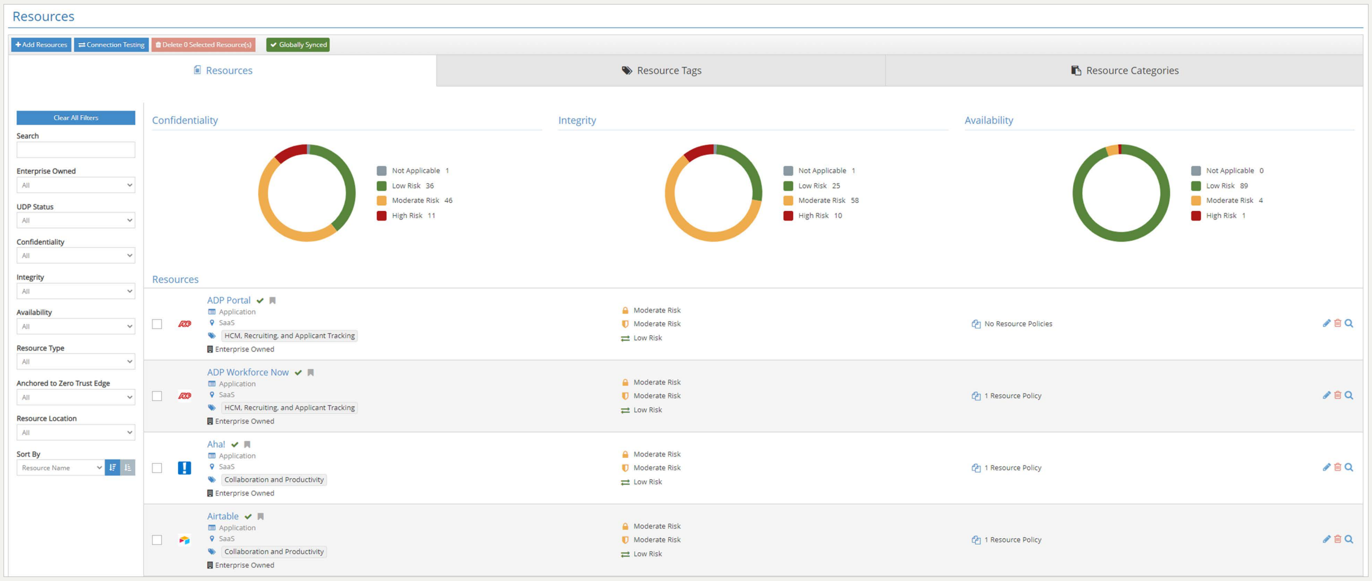
Condition	Action
Does Not Include All	Automatically Isolate

Anti-Malware Signals: Cloud ML - AntiMalware Detection slider set to Aggressive or higher (Windows); Cloud ML - AntiMalware Prevention slider set to Moderate or higher (Windows); + Add Item

Search...

- ☑ Cloud ML - AntiMalware Detection slider set to Aggressive or higher (Windows)
- ☑ Cloud ML - AntiMalware Prevention slider set to Moderate or higher (Windows)
- □ Sensor ML - Anti-malware Detection set to Aggressive or higher (Windows)
- □ Sensor ML - Anti-malware Prevention set to Moderate or higher (Windows)
- □ System Management Mode (SMM) Protections (Windows)
- □ Test Signing Disabled (Windows)
- □ UEFI Memory Protection (Windows)
- □ Remediation - Advanced Remediation Enabled (Windows)

When CrowdStrike Falcon identifies an incident, the iboss Zero Trust SSE can automatically cut off access to sensitive resources by leveraging the resources database, which contains all enterprise-owned resources.



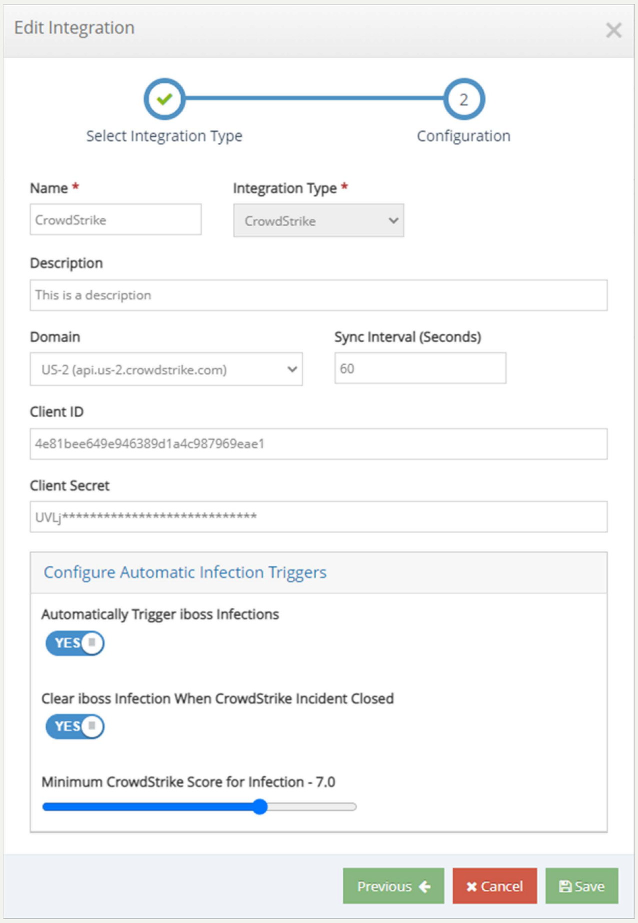
Filter	Value
Enterprise Owned	All
UDP Status	All
Confidentiality	All
Integrity	All
Availability	All
Resource Type	All
Anchored to Zero Trust Edge	All
Resource Location	All

	Confidentiality	Integrity	Availability
Not Applicable	1	1	0
Low Risk	36	25	89
Moderate Risk	46	58	4
High Risk	11	10	1

Resources

Resource	Risk	Policies
ADP Portal ✓ Application SaaS HCM, Recruiting, and Applicant Tracking Enterprise Owned	Moderate Risk Moderate Risk Low Risk	No Resource Policies
ADP Workforce Now ✓ Application SaaS HCM, Recruiting, and Applicant Tracking Enterprise Owned	Moderate Risk Moderate Risk Low Risk	1 Resource Policy
Aha! ✓ Application SaaS Collaboration and Productivity Enterprise Owned	Moderate Risk Moderate Risk Low Risk	1 Resource Policy
Airtable ✓ Application SaaS Collaboration and Productivity Enterprise Owned	Moderate Risk Moderate Risk Low Risk	1 Resource Policy

A CrowdStrike Falcon incident that reaches a high-risk CrowdScore level will automatically open iboss incidents, which tie back to the Falcon platform. These incidents will automatically cut off access to enterprise-owned sensitive resources without human intervention, reducing the exposure to damage from ransomware and attackers. The incident CrowdScore level can be configured to trigger an automatic action by iboss.


Edit Integration

Name *
CrowdStrike

Integration Type *
CrowdStrike

Description
This is a description

Domain
US-2 (api.us-2.crowdstrike.com)

Sync Interval (Seconds)
60

Client ID
4e81bee649e946389d1a4c987969eae1

Client Secret
UVLj****************************

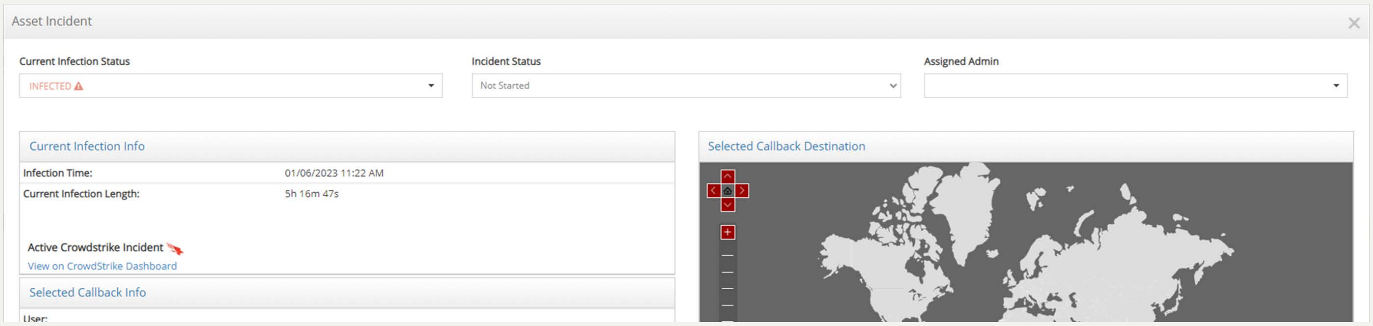
Configure Automatic Infection Triggers

Automatically Trigger iboss Infections
YES

Clear iboss Infection When CrowdStrike Incident Closed
YES

Minimum CrowdStrike Score for Infection - 7.0

Once the CrowdScore level is reached, an active incident will be created in iboss, immediately cutting off access to sensitive resources.


Asset Incident

Current Infection Status
INFECTED ⚠

Incident Status
Not Started

Assigned Admin

Current Infection Info

Infection Time:	01/06/2023 11:22 AM
Current Infection Length:	5h 16m 47s

Active Crowdstrike Incident
View on CrowdStrike Dashboard

Selected Callback Info

User:

Selected Callback Destination

When an incident is closed within the Falcon platform, the associated iboss Zero Trust SSE incident is also closed, automatically restoring access to resources.

KEY SOLUTION CAPABILITIES:

1. Cut off access to sensitive resources when the CrowdScore indicates a high-risk incident without human intervention by allowing the iboss Zero Trust SSE to close the loop and take action automatically.

2. Cut off or isolate access to sensitive resources when a policy leveraging the Falcon ZTA risk score is not met. The iboss Zero Trust SSE leverages its continuous adaptive access Trust Algorithm to take Falcon ZTA signals to add an additional pane of glass in front of those resources using iboss Browser Isolation.

ABOUT IBOSS

iboss is a cloud security company that enables organizations to reduce cyber risk by delivering a Zero Trust Security Service Edge platform designed to protect resources and users in the modern distributed world. Applications, data, and services have moved to the cloud and are located everywhere, while users needing access to those resources are working from anywhere. The iboss platform replaces legacy VPN, Proxies, and VDI with a consolidated service that improves security, increases the end-user experience, consolidates technology, and substantially reduces costs. Built on a containerized cloud architecture, iboss delivers security capabilities such as SWG, malware defense, Browser Isolation, CASB, and Data Loss Prevention to protect all resources via the cloud instantaneously and at scale. The iboss platform includes ZTNA to replace legacy VPN, Security Service Edge to replace legacy Proxies, and Browser Isolation to replace legacy VDI. This shifts the focus from protecting buildings to protecting people and resources wherever they are located. Leveraging a purpose-built cloud architecture backed by 230+ issued and pending patents and more than 100 points of presence globally, iboss processes over 150 billion transactions daily, blocking 4 billion threats per day. More than 4,000 global enterprises trust the iboss platform to support their modern workforces, including a large number of Fortune 50 companies. iboss was named one of the Top 25 Cybersecurity Companies by The Software Report, one of the 25 highest-rated Private Cloud Computing Companies to work for by Battery Ventures, and CRN's top 20 Coolest Cloud Security Companies of 2022.

To learn more, visit **www.iboss.com**

KEY BENEFITS

- Automatically cut off access to sensitive enterprise resources when a device becomes infected or an incident risk is high based on the CrowdStrike CrowdScore incident rating
- Automatically cut off or isolate access when the Falcon ZTA risk score indicates high risk
- Automatically cut off or isolate access if a device does not have critical Falcon settings enabled
- Get log events for every access to sensitive resources to detect data exfiltration attempts
- Apply CASB, malware defense, compliance policies, and DLP to every transaction to complement Falcon's on-device protections

ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: **https://www.crowdstrike.com/**

Follow us: **Blog** | **Twitter** | **LinkedIn** | **Facebook** | **Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**

To learn more about this integration:

https://www.iboss.com
sales@iboss.com
877-742-6832

www.crowdstrike.com