Build a Zero-Trust SaaS Security Posture

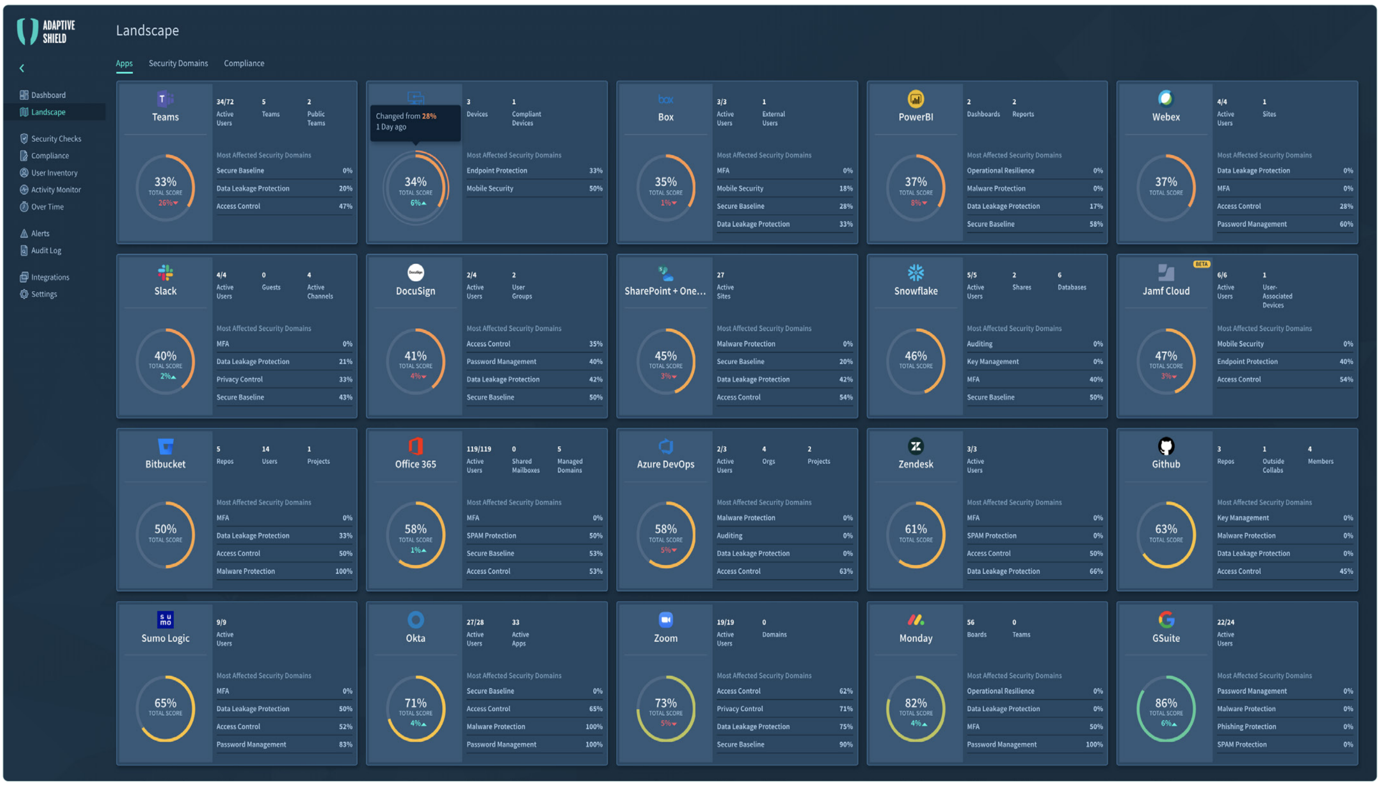
A Holistic Solution to Gain Control over Your SaaS Security, Users and Devices

CROWDSTRIKE + ADAPTIVE SHIELD

Introduction

The threat landscape for SaaS security is vast as businesses rely on a multitude of SaaS apps that have hundreds to thousands of configurations to monitor and remediate. While SaaS providers build in security features, it is the company's IT and security team's responsibility to continuously fix any potential configuration weaknesses. It is also critical that organizations protect endpoints to detect and remediate threats related to user permissions and privileges in SaaS apps.

Adaptive Shield, the market-leading SaaS Security Posture Management (SSPM) solution, has partnered with CrowdStrike, a leader in Endpoint Detection and Response (EDR), to create a solution that provides an enhanced SaaS Security assessment.



Landscape

Teams
34/72 Active Users · 5 Teams · 2 Public Teams
33% TOTAL SCORE 26%▼

Most Affected Security Domains	
Secure Baseline	0%
Data Leakage Protection	20%
Access Control	47%

Changed from 28%
1 Day ago
3 Devices · 1 Compliant Devices
34% TOTAL SCORE 6%▲

Most Affected Security Domains	
Endpoint Protection	33%
Mobile Security	50%

Box
3/3 Active Users · 1 External Users
35% TOTAL SCORE 1%▼

Most Affected Security Domains	
MFA	0%
Mobile Security	18%
Secure Baseline	28%
Data Leakage Protection	33%

PowerBI
2 Dashboards · 2 Reports
37% TOTAL SCORE 8%▼

Most Affected Security Domains	
Operational Resilience	0%
Malware Protection	0%
Data Leakage Protection	17%
Secure Baseline	58%

Webex
4/4 Active Users · 1 Sites
37% TOTAL SCORE

Most Affected Security Domains	
Data Leakage Protection	0%
MFA	0%
Access Control	28%
Password Management	60%

Slack
4/4 Active Users · 0 Guests · 4 Active Channels
40% TOTAL SCORE 2%▲

Most Affected Security Domains	
MFA	0%
Data Leakage Protection	21%
Privacy Control	33%
Secure Baseline	43%

DocuSign
2/4 Active Users · 2 User Groups
41% TOTAL SCORE 4%▼

Most Affected Security Domains	
Access Control	35%
Password Management	40%
Data Leakage Protection	42%
Secure Baseline	50%

SharePoint + One...
27 Active Sites
45% TOTAL SCORE 3%▼

Most Affected Security Domains	
Malware Protection	0%
Secure Baseline	20%
Data Leakage Protection	42%
Access Control	54%

Snowflake
5/5 Active Users · 2 Shares · 6 Databases
46% TOTAL SCORE

Most Affected Security Domains	
Auditing	0%
Key Management	0%
MFA	40%
Secure Baseline	50%

Jamf Cloud BETA
6/6 Active Users · 1 User-Associated Devices
47% TOTAL SCORE 3%▼

Most Affected Security Domains	
Mobile Security	0%
Endpoint Protection	40%
Access Control	54%

Bitbucket
5 Repos · 14 Users · 1 Projects
50% TOTAL SCORE

Most Affected Security Domains	
MFA	0%
Data Leakage Protection	33%
Access Control	50%
Malware Protection	100%

Office 365
119/119 Active Users · 0 Shared Mailboxes · 5 Managed Domains
58% TOTAL SCORE 1%▲

Most Affected Security Domains	
MFA	0%
SPAM Protection	50%
Secure Baseline	53%
Access Control	53%

Azure DevOps
2/3 Active Users · 4 Orgs · 2 Projects
58% TOTAL SCORE 5%▼

Most Affected Security Domains	
Malware Protection	0%
Auditing	0%
Data Leakage Protection	0%
Access Control	63%

Zendesk
3/3 Active Users
61% TOTAL SCORE

Most Affected Security Domains	
MFA	0%
SPAM Protection	0%
Access Control	50%
Data Leakage Protection	66%

Github
3 Repos · 1 Outside Collabs · 4 Members
63% TOTAL SCORE

Most Affected Security Domains	
Key Management	0%
Malware Protection	0%
Data Leakage Protection	0%
Access Control	45%

Sumo Logic
9/9 Active Users
65% TOTAL SCORE

Most Affected Security Domains	
MFA	0%
Data Leakage Protection	50%
Access Control	52%
Password Management	83%

Okta
27/28 Active Users · 33 Active Apps
71% TOTAL SCORE 4%▲

Most Affected Security Domains	
Secure Baseline	0%
Access Control	65%
Malware Protection	100%
Password Management	100%

Zoom
19/19 Active Users · 0 Domains
73% TOTAL SCORE 5%▼

Most Affected Security Domains	
Access Control	62%
Privacy Control	71%
Data Leakage Protection	75%
Secure Baseline	90%

Monday
56 Boards · 0 Teams
82% TOTAL SCORE 4%▲

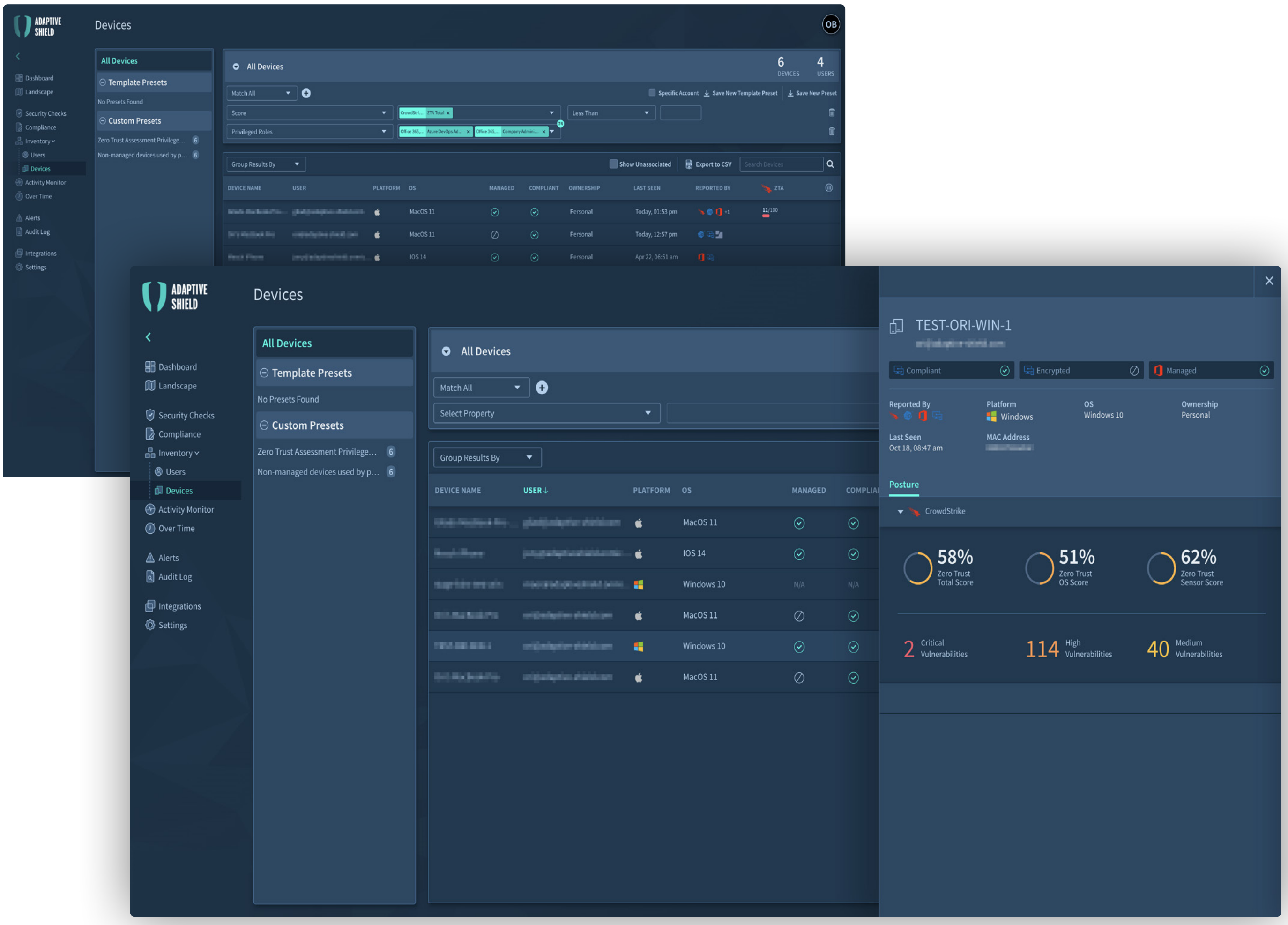
Most Affected Security Domains	
Operational Resilience	0%
Data Leakage Protection	0%
MFA	50%
Password Management	100%

GSuite
22/24 Active Users
86% TOTAL SCORE 6%▲

Most Affected Security Domains	
Password Management	0%
Malware Protection	0%
Phishing Protection	0%
SPAM Protection	0%

This partnership enables your team to implement a holistic Zero Trust approach in your SaaS security posture by analyzing the device posture. By correlating CrowdStrike's rich endpoint telemetry and Zero Trust Assessment scoring within the Adaptive Shield's SaaS security posture technology, your security team will gain unprecedented context and visibility to easily see and manage the risks that stem from SaaS users and their associated devices. This is achieved through Endpoint Management integrations, where Adaptive Shield gains the capability to associate a device to its specific owner (SaaS user). Adaptive Shield's engine consolidates between CrowdStrike's Device entity and the Endpoint Management entity, to provide the Device - SaaS user metrics.

Even if the user is authenticated, the network is encrypted, and the SaaS applications are secured — elusive threats can still take hold within devices. With CrowdStrike and Adaptive Shield, security teams are empowered with rich endpoint telemetry correlated with SaaS application insights, allowing them to detect and respond to threats with speed and accuracy.



DEVICE NAME	USER ↓	PLATFORM	OS	MANAGED	COMPLIA
[redacted]	[redacted]		MacOS 11	✓	✓
[redacted]	[redacted]		IOS 14	✓	✓
[redacted]	[redacted]		Windows 10	N/A	N/A
[redacted]	[redacted]		MacOS 11	⊘	✓
[redacted]	[redacted]		Windows 10	✓	✓
[redacted]	[redacted]		MacOS 11	⊘	✓

TEST-ORI-WIN-1
[redacted]

Compliant ✓ | Encrypted ⊘ | Managed ✓

Reported By

Platform
Windows

OS
Windows 10

Ownership
Personal

Last Seen
Oct 18, 08:47 am

MAC Address
[redacted]

Posture

CrowdStrike

58% Zero Trust Total Score

51% Zero Trust OS Score

62% Zero Trust Sensor Score

2 Critical Vulnerabilities

114 High Vulnerabilities

40 Medium Vulnerabilities

Use Cases

Implement a complete end-to-end Zero Trust Strategy

Solution Description

Adaptive Shield's SSPM solution provides visibility and remediation of potential risks in the SaaS stack caused by misconfigurations and misappropriated privileges. When connected with CrowdStrike's endpoint protection capabilities, your team sees each device's Zero Trust Assessment (ZTA) score together with the device configurations that are impacting the ZTA score.

Benefits

Gain context and visibility to easily see and manage the vulnerabilities and risks that stem from SaaS apps, your users, and their associated devices for cleaner cyber hygiene. For the first time, users can understand their ZTA score and the vulnerabilities they need to mitigate to improve device posture.

Monitor High-risk Devices that Serve as a Critical Threat Vector in your SaaS Environment

Solution Description

Continuously monitor users with privileged access that have unsecured devices through CrowdStrike's rich telemetry and the Adaptive Shield interface.

Benefits

Easily gain rich and timely insights by monitoring the devices with privileged access to your SaaS environment, reducing the overall company's risk of a compromise.

Associate Between the Device and its Owner on a User-level

Solution Description

Through the Adaptive Shield and CrowdStrike integration, Spotlight users can monitor vulnerabilities in their device posture in correlation with its owner, through a consolidation engine that fuses the data between the device and endpoint management system.

Benefits

Gain visibility of the CrowdStrike device coverage, compliance status, and policy enrollment at the user level. Take a deep dive into vulnerabilities for each device, including CVS issues, remediation plans, and context into each vulnerability.

Key Capabilities

SaaS Device-User-App Cross Referencing

Cross reference between the user's device and the SaaS apps to which they have access, including their privileged roles in these apps.

Device Zero Trust Score and User Risk Assessment

Emphasize high risk users based on CrowdStrike's ZTA scoring of their device posture, including context that allows users to understand why the device is failing.

Enhance Endpoint Security

Enable a "soft" policy and enrollment enforcement, by implementing best practices instead of access blocking, granted by the correlation between the device and its specific owner.

Deep Observability into Device-User-SaaS Risk

Easily run an in-depth query in the Adaptive Shield platform to cross reference any user, app usage and device posture.

Device Compliance Status

Check the compliance status of the user's device and monitor the user's SaaS app access, including monitoring the compliance to global standards.

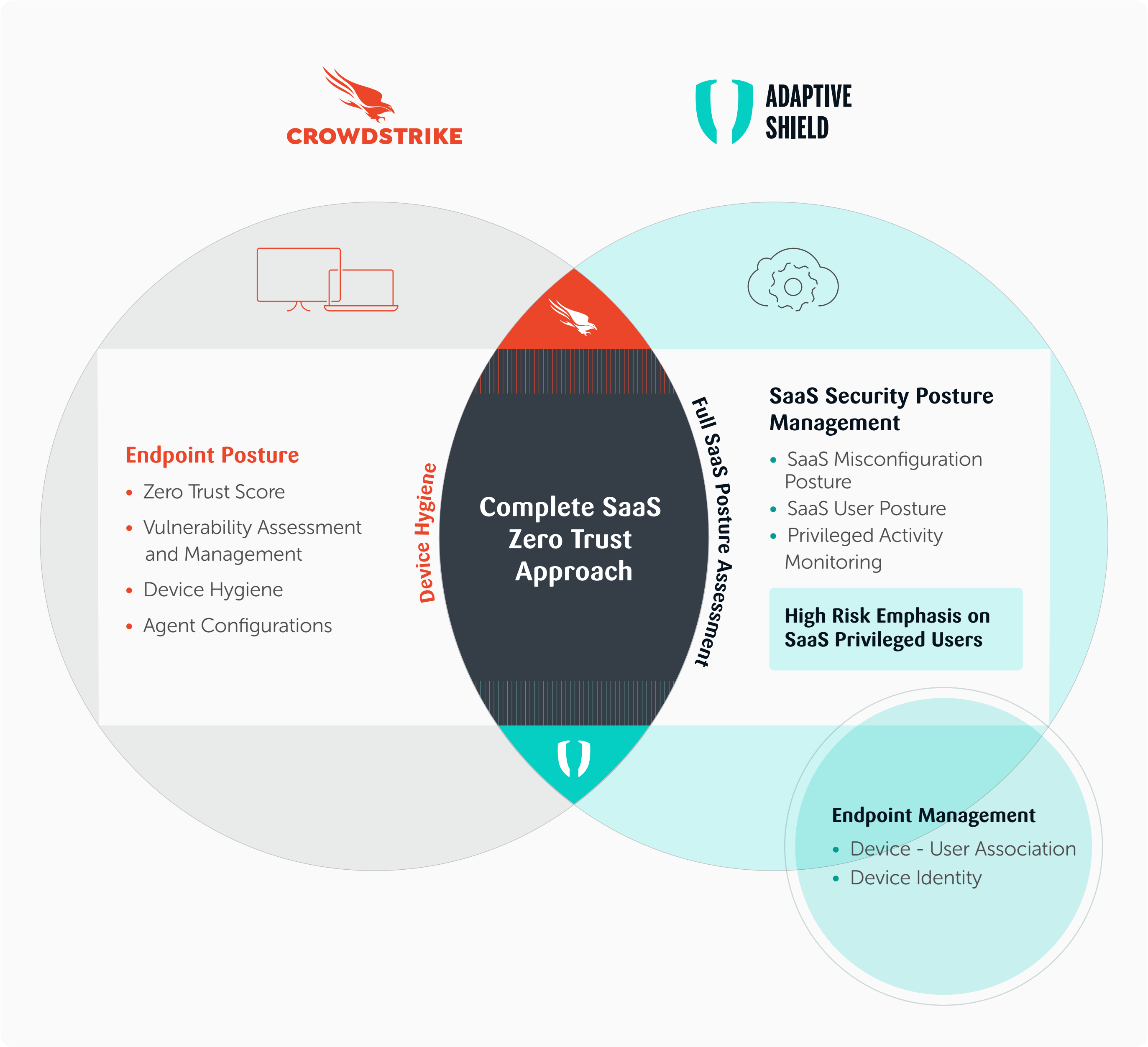
Device Operating System Monitoring

Check devices for up-to-date OS configurations and monitor the user's SaaS app access, including vulnerabilities.

Device Vulnerability Management

Gain insights into the device and the impact it has on the user, with a granular view of all the vulnerabilities of each device.

Technical Solution



CROWDSTRIKE

ADAPTIVE SHIELD

Endpoint Posture

- Zero Trust Score
- Vulnerability Assessment and Management
- Device Hygiene
- Agent Configurations

Device Hygiene

Complete SaaS Zero Trust Approach

Full SaaS Posture Assessment

SaaS Security Posture Management

- SaaS Misconfiguration Posture
- SaaS User Posture
- Privileged Activity Monitoring

High Risk Emphasis on SaaS Privileged Users

Endpoint Management

- Device - User Association
- Device Identity

The Consolidation Engine fuses the data of the device and the endpoint management system, aggregating data from:

SaaS Posture

SaaS Security Posture and privileged SaaS roles of the device owners.

Endpoint Management

The device's state of compliance and the device owner.

Device Posture

Security posture and vulnerability assessment (overall device hygiene score).

About Adaptive Shield

Adaptive Shield, the leading SaaS Security Posture Management (SSPM) company, enables security teams to locate and fix configuration weaknesses quickly in their SaaS environment, ensuring compliance with company and industry standards. Founded by Maor Bin and Jony Shlomoff, Adaptive Shield works with many Fortune 500 enterprises to help them gain control over their SaaS threat landscape.

Visit us at **www.adaptive-shield.com**

Follow us

About CrowdStrike

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security. With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform. There's only one thing to remember about CrowdStrike: We stop breaches.

Learn more **www.crowdstrike.com**

Follow us