

Build a Zero-Trust SaaS Security Posture

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



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.



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.

The screenshot displays the Adaptive Shield console interface. On the left is a navigation sidebar with options like Dashboard, Landscape, Security Checks, Compliance, Inventory, Users, Devices, Activity Monitor, Over Time, Alerts, Audit Log, Integrations, and Settings. The main area is titled 'Devices' and shows a list of devices under 'All Devices'. A detailed view for the device 'TEST-ORI-WIN-1' is open on the right, showing its posture and vulnerability data.

DEVICE NAME	USER	PLATFORM	OS	MANAGED	COMPLIANT
Gilads-MacBook-Pro...	[redacted]	Apple	MacOS 11	✓	✓
Mesch iPhone	[redacted]	Apple	IOS 14	✓	✓
stage-bins-test-win	[redacted]	Windows	Windows 10	N/A	N/A
Ori's MacBook Pro	[redacted]	Apple	MacOS 11	✓	✓
TEST-ORI-WIN-1	[redacted]	Windows	Windows 10	✓	✓
Ori's MacBook Pro	[redacted]	Apple	MacOS 11	✓	✓

TEST-ORI-WIN-1 Details:

- Compliant: ✓
- Encrypted: ✓
- Managed: ✓
- Reported By: [redacted]
- Platform: Windows
- OS: Windows 10
- Ownership: Personal
- Last Seen: Oct 18, 08:47 am
- MAC Address: 08002769a03c

Posture

- CrowdStrike:
 - 58% Zero Trust Total Score
 - 51% Zero Trust OS Score
 - 62% Zero Trust Sensor Score
- Vulnerabilities:
 - 2 Critical Vulnerabilities
 - 114 High Vulnerabilities
 - 40 Medium Vulnerabilities
- Tenable: [redacted]

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 estate caused by misconfigurations and misappropriated privileges. When connected with CrowdStrike's endpoint protection capabilities, your team gains continuous and comprehensive visibility and control over users and devices connected to SaaS apps in your environment.

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 a cleaner cyber hygiene.



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 insecure 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, you can monitor the 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 enrollments at the user level. Enable "soft" enforcement enhancements, through policies and organizational best practices rather than blocking a user, while having each device mapped to a specific user.

Key Capabilities



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.



Device Zero Trust Score and User Risk Assessment

Emphasize high risk users based on CrowdStrike's ZTA scoring of their device posture and their privileged access to the organization's SaaS applications.



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.



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

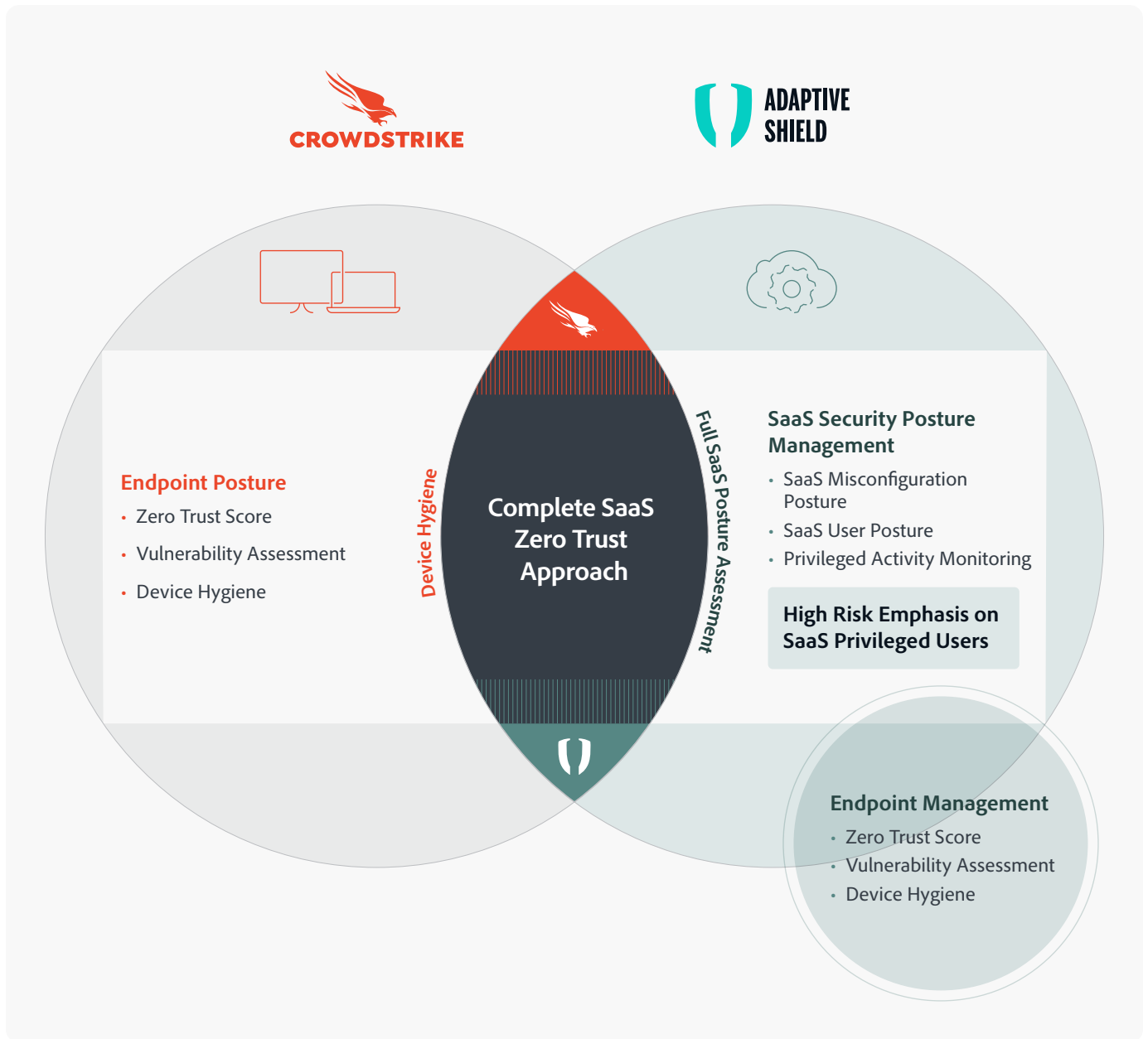
Check the compliance status of the user's device and monitor the user's SaaS app access, including monitoring the compliance to global standards.






Device Operating System Monitoring

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

Technical Solution



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

 <p>Endpoint Management the device's state of compliance and the device owner.</p>	 <p>Device security posture and vulnerability assessment (overall device hygiene score).</p>	 <p>The Adaptive Shield platform SaaS Security Posture and privileged SaaS roles of the device owners.</p>
--	--	--



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