ADAPTIVE SHIELD

CROWDSTRIKE

Data Sheet

ADAPTIVE SHIELD: SAAS SECURITY POSTURE MANAGEMENT

Build a Zero Trust SaaS security posture and gain control over SaaS applications, users and devices

CHALLENGES

The threat landscape for software-as-a-service (SaaS) security is vast, as businesses rely on many SaaS applications that have hundreds or thousands of configurations to monitor and remediate. Though SaaS providers build in security features, it is a company's IT and security teams' responsibility to continuously fix any potential configuration weaknesses. Organizations are also responsible for protecting endpoints by detecting and remediating threats related to user permissions and privileges in SaaS applications.

SOLUTION

Adaptive Shield, a 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 teams 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 Falcon Zero Trust Assessment (ZTA) scoring within 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.

These endpoint management integrations enable Adaptive Shield to associate a device to its specific owner (i.e., SaaS user). Adaptive Shield's engine then consolidates between CrowdStrike's "device" and "endpoint management" entities to provide Device-SaaS user metrics.

Elusive threats can still take hold within devices, even if the user is authenticated, the network is encrypted and SaaS applications are secured. With the CrowdStrike Falcon® platform and Adaptive Shield, security teams are empowered with rich endpoint telemetry correlated with SaaS application insights, allowing them to quickly and accurately detect and respond to threats.

KEY BENEFITS

Enhanced visibility: Unify native security controls and see rich endpoint telemetry alongside CrowdStrike Falcon Zero Trust Assessment scores in a single view within Adaptive Shield's platform

Continuous monitoring: Continuously monitor your SaaS applications to quickly and accurately detect any misconfigurations

Timely notifications: Send detailed alerts at the first sign of a glitch, proactively notifying security teams in real time when there's a severe misconfiguration to stop minor incidents from becoming major problems

BUSINESS VALUE

Use Case/Challenge	Solution	Benefits
Implementing a complete end-to-end Zero Trust strategy	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, comprehensive visibility and control over users and devices connected to SaaS applications in your environment.	Gain context and visibility to easily see and manage the vulnerabilities and risks that stem from SaaS applications, your users and their associated devices, for a cleaner cyber hygiene.
Monitoring high-risk devices that serve as a critical threat vector in your SaaS environment	Continuously monitor users that have privileged access and insecure devices through CrowdStrike's rich telemetry and the Adaptive Shield interface.	Easily gain rich and timely insights by monitoring the devices with privileged access to your SaaS environment, reducing the company's overall risk of a compromise.
Associating between the device and its owner on a user level	Through the Adaptive Shield and CrowdStrike Falcon 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.	Gain visibility of CrowdStrike Falcon 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 mapping each device to a specific user.

TECHNICAL SOLUTION

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

- **Endpoint management:** the device's state of compliance and the device owner
- **The device:** security posture and vulnerability assessment (overall device hygiene score)
- **The Adaptive Shield platform:** SaaS security posture and privileged SaaS roles of the device owners
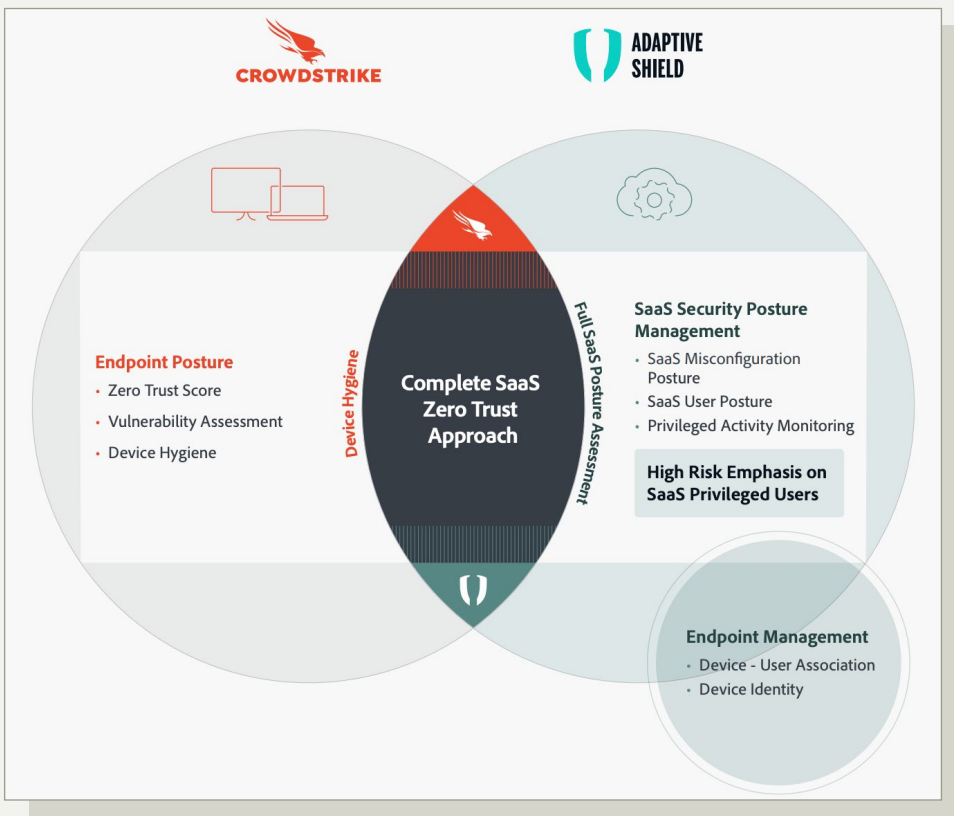
**ADAPTIVE SHIELD: SAAS SECURITY
POSTURE MANAGEMENT**

KEY CAPABILITIES

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

- **Device ZTA score and user risk assessment:** Emphasize high-risk users based on CrowdStrike Falcon's ZTA scoring of their device posture and their privileged access to your 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 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.

Adaptive Shield is a trusted **CrowdStrike Store Partner**, providing a secure application, leveraging rich data from the CrowdStrike Security Cloud and extending the Falcon platform's capabilities with Adaptive Shield's security posture management platform. Visit the CrowdStrike Store for a **free trial**.

ABOUT ADAPTIVE SHIELD

Adaptive Shield, a 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. For more information, visit **www.adaptive-shield.com** or follow Adaptive Shield on **LinkedIn**.

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (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 ulnerabilities. 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.**