

Zscaler & CrowdStrike Webinar

10. März 2021

Zscaler & CrowdStrike Webinar

Modernizing Security for a Cloud and Mobile World

From Endpoint to Cloud to App

10. March 2021

1 / ©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION

AVANTEC
Competence. Security. Trust.



Thanh Trieu
Practice Build Consultant at Zscaler

Zscaler integration CrowdStrike Platform



Posture Driven
Conditional Access

ZPA + FALCON INTEGRATION

Zero-trust access rules validate and inspect device posture and ensure compliance status before allowing access to internal apps



Advanced Threat
Protection and Response

ZIA + FALCON INTEGRATION

Automatic correlation of detected threat with endpoint device information;
Fast console pivot for faster investigation and response

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION

Securing your cloud transformation

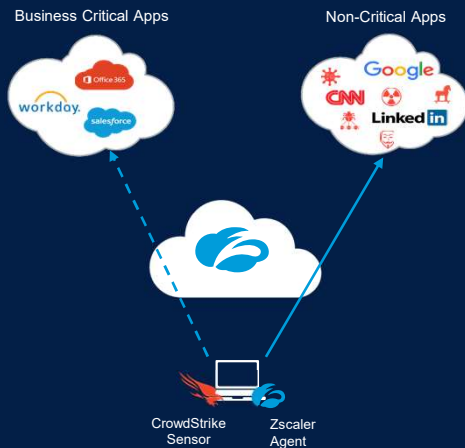


AVANTEC
Competence. Security. Trust.

Zscaler & CrowdStrike Webinar

10. März 2021

Integration #1: Posture Driven Conditional Access



Device Posture-driven Conditional Access

Z-APP agent inspects the presence of a running CrowdStrike sensor (i.e. agent)

Access blocked for non-compliant, unmanaged or rogue devices

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION

Securing your cloud transformation



Enable Device Posture



Dashboard Enrolled Devices

Settings

- Zscaler App Store
- Zscaler App Notifications
- Audit Logs
- Forwarding Profile
- Trusted Networks
- Zscaler App Support
- Zscaler Service Entitlement
- User Agent
- Zscaler App IdP
- Device Posture**

MANAGE DEVICE POSTURES

+ Add Device Posture Profile

#	Profile Name
1	Carbon_Black_Posture_Check
2	CrowdStrike_Posture_Check
3	thumbprint CB

Add Device Posture

DEFINE POLICY AND SCOPE

Name test1

PLATFORM

Windows macOS Android iOS

DEVICE POSTURE CONFIGURATION

Posture Type Certificate Trust

- Domain Joined
- Detect Carbon Black v. 2.1.2+
- Detect CrowdStrike v. 2.1.2+
- Detect SentinelOne v. 2.1.2+

Save Cancel

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION

Securing your cloud transformation

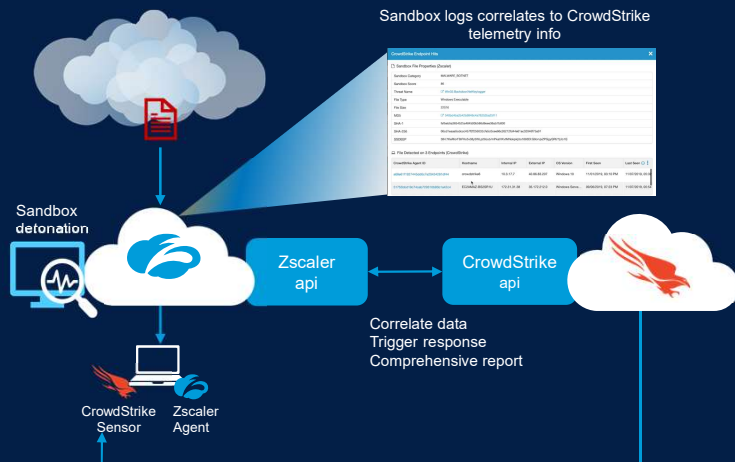


AVANTEC
Competence. Security. Trust.

Zscaler & CrowdStrike Webinar

10. März 2021

Integration #2: Advanced Threat Prevention



©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION

Securing your cloud transformation / zscaler

Enhanced Visibility and Seamless Pivot

Insights Logs

N...	Event Time	User	Policy Action	MD5
1	Wednesday, February 19, 2020 10:58:0...	tsullivan@crowdstri...	Malware block: malicious ...	32dde274e5e8c...
2	Wednesday, February 19, 2020 11:08:5...	tsullivan@crowdstri...	Malware block: malicious ...	32dde274e5e8c...
3	Wednesday, February 19, 2020 11:11:2...	tsullivan@crowdstri...	Sandbox block inbound r...	4e2c0b9df709a9...

File Detected on 1 Endpoint (CrowdStrike)

CrowdStrike Agent ID: 454ae5077de04600701737df945d...

Host Name: W10CLIENT03

Internal IP: 10.10.10.84

OS Version: Windows 10

File Status: Detected

Last Seen: 02/19/2020, 12:04 PM

Endpoint Status: Normal

Contain

Auto-populated

Agent ID: 454ae5077de04600701737df945d...

One click from ZIA to bring up CrowdStrike console

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION

Securing your cloud transformation / zscaler

AVANTEC
Competence. Security. Trust.

Zscaler & CrowdStrike Webinar

10. März 2021

Zscaler + CrowdStrike Working Together

Endpoint To Application Protection



Reduced TCO



Simple to deploy and manage cloud native security services that scale with demand

End-to-end Protection



Comprehensive visibility and remediation from the device to the app

Quicker Remediation



Faster detection, investigation and response to threats

©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION

Securing your cloud transformation



Thank you

8 / ©2019 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION

Securing your cloud transformation



AVANTEC
Competence. Security. Trust.