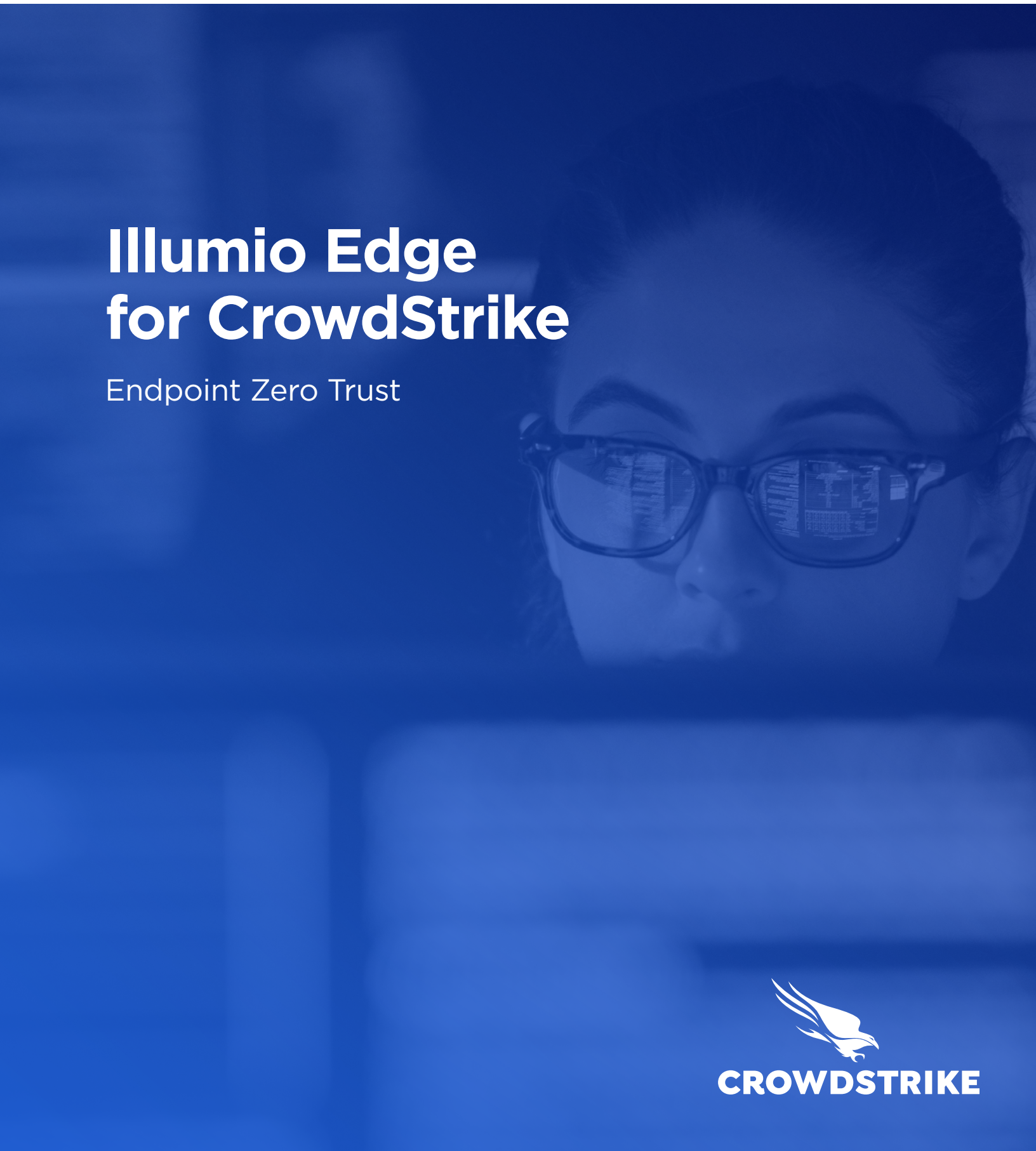
illumio

SOLUTION BRIEF

Illumio Edge for CrowdStrike

Endpoint Zero Trust



CROWDSTRIKE

Challenge

Ransomware and malware are designed to move laterally to target entire organizations, locking up whole networks in seconds. Alternatively, attackers themselves can take more time with precise attacks that move laterally as they "live off the land" and target crown jewels. Either way, an isolated incident on a single endpoint can turn into a large-scale attack, particularly if new ransomware has yet to be detected.

Solution

Stop ransomware propagation and attacker lateral movement in its tracks with the Illumio Edge module that makes every endpoint a Zero Trust endpoint.

This enables containment by default, complementing CrowdStrike state-of-the-art malware prevention, to ensure that in the case of never-before-seen-ransomware, the first endpoint infected is always the last endpoint infected.

By deploying whitelist, Zero Trust policy on the endpoint, peer-to-peer communications between endpoints are blocked, except for essential traffic. This vastly reduces the risk of ransomware and malware spreading laterally, peer to peer.

Key Capabilities

Cloud-delivered:

CrowdStrike and Illumio work together in the cloud, making deployment quick and easy.

Single, lightweight CrowdStrike agent:

Get even more capability from the CrowdStrike Falcon agent, with nothing new to deploy.

Off-network protection:

Protection follows the user whether at the office, at home, or on a public network.

Key Benefits

- Get complete endpoint protection with state-of-the-art CrowdStrike prevention and Illumio Zero Trust containment.
- Achieve risk-free Zero Trust by easily whitelisting legitimate services while preventing ransomware propagation and attacker lateral movement.
- Deliver Zero Trust capabilities, all from your CrowdStrike Falcon agent.

Complementary prevention and containment:

CrowdStrike NGAV prevention is designed to work hand in glove with Illumio endpoint Zero Trust.

Native host Windows firewalling:

Program the existing Windows firewall on every endpoint to use what is already in place.

Automated Zero Trust policy:

No need to tediously write manual Windows firewall rules or Group Policy Object (GPO) since Zero Trust policy and rule writing is automated.

Endpoint-to-endpoint traffic visibility:

See precisely what peer-to-peer traffic is happening between endpoints to investigate potential propagation of ransomware or refine policy based on business needs.

illumio

Technical Overview

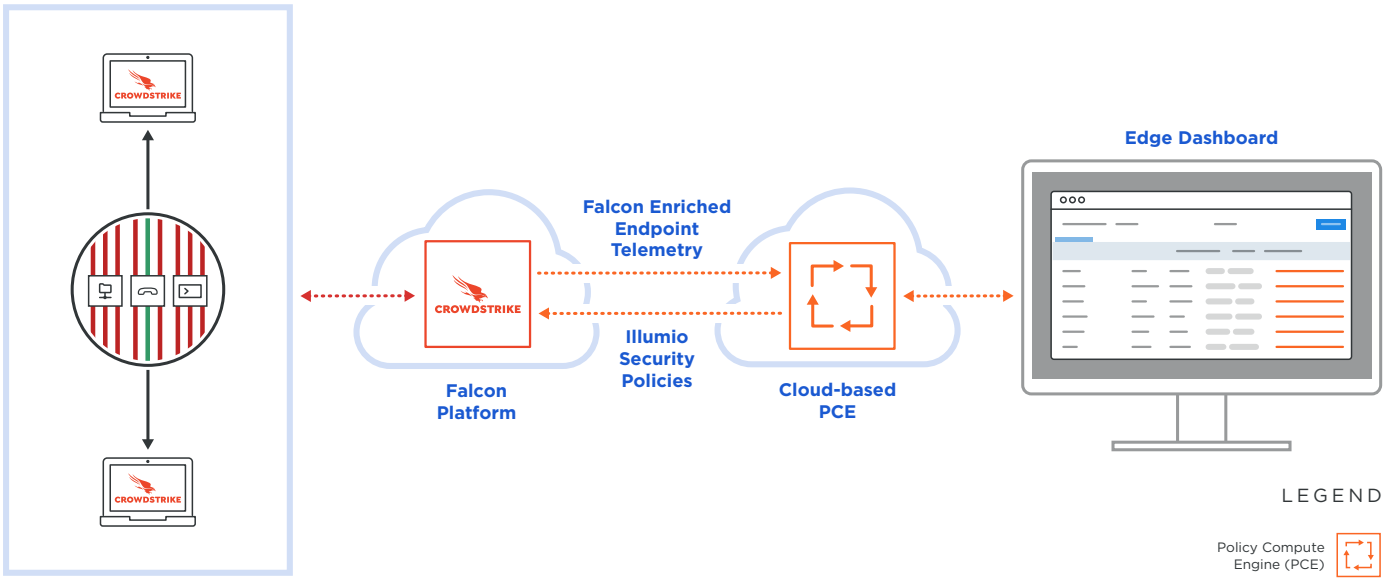
Illumio and CrowdStrike come together in the cloud through Falcon Connect, CrowdStrike's open and extensible collection of APIs. Illumio's cloud-based Policy Compute Engine consumes Falcon endpoint telemetry that is used to build intuitive, whitelist policies in Illumio Edge. Illumio Edge automates this process with a three-step workflow, eliminating the need to manually create individual host firewall policies. Once created, these polices are shared back with the CrowdStrike agent that programs the host firewall native to the operating system for enforcement.

The result is an effective whitelist approach that blocks all inbound communications to endpoints, except for permitted services, shown by the green line in the diagram below.

Requirements

1. Falcon Prevent NGAV or Falcon Insight EDR
2. Falcon Firewall Management module
3. Illumio Edge for CrowdStrike module

ILLUMIO EDGE CROWDSTRIKE INTEGRATION



illumio

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.

© 2020 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are marks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.

Illumio enables organizations to realize a future without high-profile breaches by providing visibility, segmentation, and control of all network communications across any endpoint, data center or cloud. Founded in 2013, the world's largest enterprises, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085, Tel (669) 800-5000, www.illumio.com. Copyright © 2020 Illumio, Inc. All rights reserved. This document is protected by U.S. and international copyright and intellectual property laws. Illumio's products and services are protected by one or more U.S. and international patents listed at https://www.illumio.com/patents. Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. To review a list of Illumio's trademarks, go to https://www.illumio.com/trademarks. Third-party trademarks mentioned in this document are the property of their respective owners.