CrowdStrike Store

illumio

CROWDSTRIKE

Data Sheet

ILLUMIO EDGE: ENDPOINT ZERO TRUST

Stopping ransomware propagation and attacker lateral movement

CHALLENGES

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" seeking valuable assets and access. Either way, an isolated incident on a single endpoint can turn into a large-scale attack, particularly if ransomware is new and has not previously been detected.

SOLUTION

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

This module enables containment by default, complementing CrowdStrike's state-of-the-art protection and detection technology, to ensure that for never-seen-before ransomware, the first endpoint infected is always the last endpoint infected.

By deploying allowlisted, 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.

KEY BENEFITS

Get complete endpoint protection with Illumio Edge containment, complementing the CrowdStrike Falcon® platform

Achieve risk-free Zero Trust by easily allowlisting legitimate services while preventing ransomware propagation and attacker lateral movement

Deliver Zero Trust capabilities, all from your CrowdStrike® Falcon agent

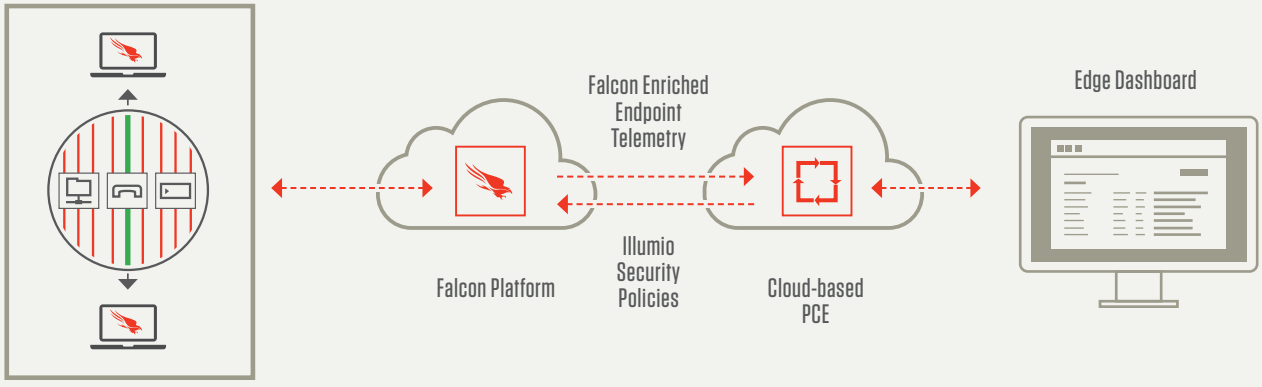
KEY SOLUTION CAPABILITIES

- **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 in the office, at home or on a public network.
- **Complementary prevention and containment:** CrowdStrike next-generation antivirus (NGAV) prevention is designed to work hand-in-glove with Illumio Edge 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 a 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 occurring between endpoints to investigate potential propagation of ransomware or refine policy based on business need.

TECHNICAL SOLUTION

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 (PCE) consumes CrowdStrike Falcon Data Replicator (FDR)-enriched endpoint telemetry that is used to build intuitive allowlist policies in Illumio Edge. Illumio Edge automates this process with a three-step workflow that eliminates the need to manually create individual host firewall policies. Once created, these policies are shared with the CrowdStrike Falcon agent, which uses the Falcon Firewall Management module to program the native Windows firewall for enforcement. The result is an effective allowlist approach that blocks all inbound communications to endpoints, except for services that should be permitted, as shown by the green line in the diagram below.

Illumio Edge Module and CrowdStrike Falcon Platform



REQUIREMENTS

1. Falcon Prevent™ NGAV or Falcon Insight™ endpoint detection and response (EDR)
2. Falcon Firewall Management module
3. Illumio Edge for CrowdStrike module

ABOUT ILLUMIO

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.

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 3 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.