SOLUTION BRIEF

Fortinet and Cigent Endpoint Security Solution

Extend FortiEDR Detection and Response Protections to the File Level of Windows 10 Endpoints

Executive Summary

Cigent's Dynamic Data Defense Engine for Windows 10 (D3E) ingests threat intelligence and security events from FortiEDR, and when the threat level is elevated, dynamically locks access to sensitive files and disk partitions with a step-up authentication.

There is a gaping hole in endpoint cybersecurity. When an endpoint is compromised by malware, hacker ingenuity, stolen credentials, or device theft/loss, there is no way to protect sensitive personal and corporate data. Full disk encryption protects data at rest but is not effective when the user is logged in.

Cigent and Fortinet recently established a technology partnership to prevent the financial and reputational loss due to advanced cyberattacks by helping organizations secure their sensitive files, even in the event of a breach.

Joint Solution Description

The Cigent D3E integration with FortiEDR provides a highly effective automated response mechanism to threats detected on Windows 10 endpoints. The D3E cloud-based management console ingests security events from the FortiEDR console and triggers

an ActiveLock on the local device through the D3E Windows client. ActiveLock protects individual files by requiring a step-up authentication until the threat is cleared. This integration ensures sensitive files are protected during periods of elevated risk.

The functionality of the joint solution is summarized in the illustration below.

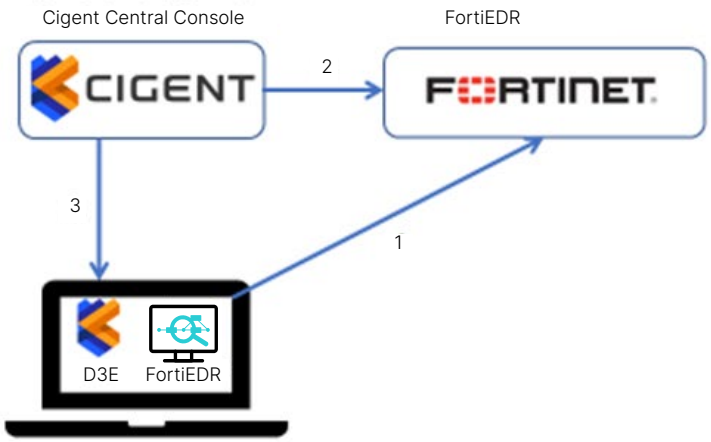

Figure 1: Joint solution components.

Joint Solution Benefits

- Fortinet FortiEDR
- Cigent D3E

Joint Solution Benefits

The FortiEDR-Cigent D3E solution offers the following joint benefits:

- Allows FortiEDR to automatically and rapidly lock files in an elevated threat environment without disrupting user productivity
- Supports file locking across groups of users while a threat is under investigation
- Extends FortiEDR threat response to the encryption layer of self- encrypting drives
- Locks sensitive files/disk partitions in the event the FortiEDR host endpoint is disabled
- Centrally manages integration with FortiEDR console and group policy for designation of protected files and response options
- Increased protection from ransomware, malware, and insider threats

FORTINET FABRIC-READY

Cigent D3E Business

Cigent's Dynamic Data Defense Engine (D3E) brings cybersecurity best practices to the file and encryption layer of Windows 10 devices with threat-aware two-factor authentication, deception, artificial intelligence, and integration with leading AV/EDR/cloud-based security solutions. D3E is designed to prevent loss of critical data, even in the event of a successful ransomware attack or breach.

FortiEDR Overview

Advanced attacks can take just minutes, if not seconds, to compromise the endpoints. First-generation endpoint detection and response (EDR) tools simply cannot keep pace. They require manual triage and responses that are not only too slow for fast-moving threats but also generate a huge volume of indicators that burden already overstretched security teams. Further, legacy EDR tools drive up the cost of security operations and can slow processes, negatively impacting business.

FortiEDR delivers advanced, real-time threat protection for endpoints both pre- and post-infection. It proactively reduces the attack surface, prevents malware infection, detects and defuses potential threats in real time, and can automate response and remediation procedures with customizable playbooks. FortiEDR helps organizations stop breaches in real time automatically and efficiently, without overwhelming security teams with a slew of false alarms or disrupting business operations.

Use Cases

1. The FortiEDR agent detects a threat and notifies FortiEDR.
2. Cigent Console polls FortiEDR for threats to managed devices.
3. Cigent Console engages ActiveLock on D3E endpoint to protect files until the threat is resolved or investigated.

About Cigent

Cigent Technology, Inc. is focused on providing network and endpoint cyber security solutions that protect your data from the inside out. Our software and next gen firmware based endpoint detection and response solutions are designed to thwart modern day cyber attacks, preventing critical data in the event of a breach.

August 27, 2021 12:50 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 2:sb-FA-fortinet-and-cigent-endpoint-security-solution:sb-FA-fortinet-and-cigent-endpoint-security-solution-2021

701126-0-0-EN