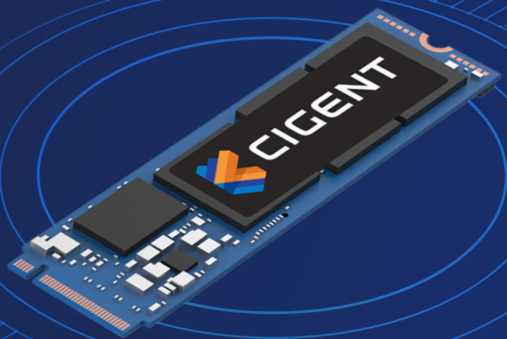
CIGENT SECURE SSD+™ ANTI-RANSOMWARE



Data Sheet

PROUDLY FUNDED BY

iqt IN-Q-TEL

The Challenge

Ransomware, extortion, and data theft continue to be executed by cyber criminals. Endpoint Detection and Response (EDR) products rely on “detecting and responding” after an attack is already in progress. To finally put an end to these threats, security controls must be closer to the data (in the storage itself) where they can prevent attacks from accessing files, even it circumvents EDR protections.

Our Solution

Cigent Secure SSD+ Anti-Ransomware is the solution to this challenge. It is the only storage device that comes with built-in ransomware detection and response. With this device installed on a Windows 8 or above laptop or desktop PC, the PC becomes a powerful artificial intelligence system that continuously monitors and prevents ransomware attacks.

How it works

Secure SSD+ has a dedicated AI microprocessor with machine learning that constantly monitors the data activity on your PCs. When ransomware is detected, Cigent has multiple methods to automatically protect your data, including:

- Cigent Data Defense software responds with “Shields Up” requiring MFA to access protected files
- Cigent Data Defense Secure Vaults automatically lock from within the storage device, preventing any unauthorized access, such as malware or even trusted Windows processes (e.g. RDP or PowerShell)
- The drive can optionally be put into read-only mode to protect data from being modified, wiped, or encrypted by ransomware

Additionally, the Cigent software notifies the Cigent Data Defense console a ransomware attack is underway. The console can then alerts security personnel, SIEMs, and SOARs to automatically engage “Shields Up” on the rest of the Cigent Protected PCs in your organization even if they don’t have a Secure SSD+.

Included Software

Each Secure SSD+ purchase includes a license to Cigent’s Data Defense Windows software, available for download

Management Console

With Cigent's Data Defense SaaS subscription, enterprises can fully manage their storage devices, receive security team alerts, integrate with SIEMs and SOARs, and benefit from FIPS 140-2 validated file encryption, among other features.

Additional Capabilities

Invisible Data

Adversaries cannot steal what they cannot see: unreadable storage partition protected by non-recoverable key

Storage firmware renders data unreadable at the sector level, preventing all physical and remote attacks. Drive can be configured with pre-boot authentication (PBA), rendering the O/S partition invisible.

Non-Recoverable Keys

A novel approach to the creation and storage of keys that prevents all known key recovery techniques

Cryptographically derived from a user-supplied password. Never stored in their final form. Use the maximum length allowed by the drive.

MFA for File Access

Zero-day ransomware, malware, and software service bypass prevention

Consistently defeats zero-day ransomware and data theft for in-use data. Files can be configured to always require MFA or as risk-based, only requiring MFA when threats detected.

Automated Threat Response

Makes data invisible if Cigent software is disabled

Protects against adversaries who disable endpoint security software. Makes in-use data invisible if attackers disable Cigent software.

Verified Data Erasure

Ensures every block has truly been wiped

Allows for drives to be safely repurposed or retired.
Saves budget and provides for a greener option.
Provides emergency data destruction confidence.

Immutable Insider Detection

Secure data access logs capture all insider threat activity

Only solution that tracks data theft when insiders boot off a USB stick. Prevents insiders or external attackers from "covering their tracks." May be used for incident response, non-repudiation, and litigation.

A Few Important Notes

1. *Secure SSD+ needs to be installed as the primary O/S drive*
2. *Ransomware detection is based on Windows O/S (Linux coming soon)*
3. *A small percentage of files may be encrypted by the ransomware before the drive countermeasures responds*
4. *The mature ML algorithms have been proven and provide protection even against newest ransomware*
5. *Detection sensitivity can be dynamically tuned to users normal activity to reduce false positives*
6. *Secure SSD+ comes in a M.2 2280 double-sided form factor and may not be compatible with some ultra thin laptops*

CIGENT®
Data Security that Works.™