CIGENT
Data Security that Works.™

CIGENT DATA DEFENSE™ SECURE VAULT

Solution Brief

PROUDLY FUNDED BY

iqt IN-Q-TEL™

The Challenge

Data has become the most valuable organizational asset. Strong data security controls are implemented in the data center, however sensitive data is also on user endpoint systems where it is more vulnerable and difficult to protect, especially from advanced threats already inside the network. EDR technologies are consistently circumvented, and Windows-based drive encryption automatically unlocks at login. When adversaries gain access to endpoints, there are virtually no safeguards to protect their data from theft and ransomware.

Our Solution

Cigent Secure Vault solution uses a combination of Cigent software and hardware (TCG Opal 2.0 compliant drives) to add a digital “vault” where sensitive files are stored and protected. Like a physical vault, this digital equivalent ensures that only authorized users with the “combination” (multi-factor authentication) can unlock the vault and access its contents.

How it works

Part of the Cigent Data Defense software platform, Secure Vault provides an additional layer of security by creating a drive partition that is invisible to users and the operating system until it is unlocked with MFA by an authenticated user.

Contents of the Secure Vault partition are automatically encrypted using fast and secure AES-256 hardware-based encryption. The partition is not accessible while the Secure Vault is “locked.” Even when using advanced drive utilities or booting with an alternate operating systems (e.g. using a bootable USB drive), the partition with the Secure Vault remains invisible when locked. Locked data cannot be stolen or ransomed. It is even protected from drive cloning utilities, wiping software, and other malware. Malware and bad actors simply can’t attack what they can’t see.

Secure Vault Protection Modes

Cigent Data Defense has two operating modes for protecting data in a Secure Vault: Always-on and Dynamic. In both modes, when the user is not working with the protected content, the user can instantly lock the Secure Vault to prevent any authorized access.

Dynamic Mode – When unlocked, the Secure Vault contents are fully accessible to the user with no further actions required. As an added measure of protection, MFA for file access can be implemented by file type or folder to prevent unauthorized access to files. When a threat is detected, Secure Vaults are automatically locked and access to all files within the Secure Vault requires MFA for individual file access. This “Shields Up” condition is temporary and is used to enforce additional security until the threat status is removed.

Always-on Mode – When a Secure Vault is set to Always-on mode, the Secure Vault will always enforce MFA-based access to all Secure Vault content. This mode is ideal for extremely sensitive content.

Authentication Options

Secure Vault requires the end user to use multi-factor authentication (MFA) to unlock the Vault. Cigent Data Defense supports multiple options for MFA and can leverage the tools you already have. MFA options include the following:

- PIN - PIN requirements are managed by the administrator.
- Authenticator Apps – Including Google Authenticator, Microsoft Authenticator, Duo Security by Cisco, and others.
- Windows Hello – Microsoft facial recognition and fingerprint-based authentication integrated into the Windows operating system.
- Personal Identity Verification (PIV) devices such as a YubiKey.
- Common Access Cards (CAC) smartcards.

Centralizaled Management

When purchased as a subscription, Cigent Data Defense includes a cloud-based or on-premises administrative console to manage Data Defense endpoint clients. From within the management console, administrators can set authentication policies such as authentication methods and requirements. Secure Vaults can also be remotely locked from the administrative console.

Command Line Interface (CLI)

Secure Vaults can also be managed using the Cigent CLI utility. The utility can be used to create up to eight Secure Vaults and adds support for Linux operating systems. The command line utility is ideal for headless environments or for usage in automated processes (such as backing up to a dedicated, hidden partition).

Automated Threat Response

Secure Vaults can also be configured by policy to automatically lock and go into a “Shields Up” condition when a threat is detected. Threats include disabling Cigent Data Defense or endpoint anti-virus, out-of-date AV signatures, threat detection by a SIEM, or an integrated security solution including SentinelOne, VMware Carbon Black, Cisco Secure Endpoint, CyberARK, Sophos, PC Matic, and Dell Trusted Device.

Additional Features with Cigent Ready Drives*

Service Monitoring

Cigent Data Defense maintains an active “heartbeat” between the Cigent Data Defense service and the drive firmware. In the event the service is disabled (by an attacker or insider), the Cigent Secure Vaults lock at the storage layer, instantly making its content inaccessible to threat actors.

True Erase™

Ensures that data can be truly erased from drives so that they can be reused or disposed of. Includes, cryptographic erase (CE), block level erase, and erasure verification.

Immutable Insider Threat Data Access Logs

Enables administrators to view data access logs maintained on the drive itself, preventing bad actors from “covering their tracks.”

* Requires a Cigent Secure SSD® or “Cigent Ready” drive from Cigent partners such as Digistor, Seagate, Kanguru, and Envoy Data

CIGENT®
Data Security that Works.™

Inquiries

Phone: 669-400-8127
Toll Free: 1-844-256-1825
www.cigent.com

Email:
General Inquiries - info@cigent.com
Sales Inquiries - sales@cigent.com
Partner Inquiries - partners@cigent.com

Locations

Headquarters
2211 Widman Way, Suite 150
Fort Myers, Florida 33901

R&D
402 Amherst St, Suite 402
Nashua, New Hampshire 03063

©2023 Cigent Technology Inc. All rights reserved.

Cigent and Cigent Secure SSD are registered trademarks of Cigent. Cigent Data Defense, True Erase, and Data Security that Works are trademarks of Cigent Technology Inc. In the United States and other jurisdictions.