CIGENT

CIGENT DATA DEFENSE™ SHIELDS UP™

Solution Brief

PROUDLY FUNDED BY

iqt IN-Q-TEL

The Challenge

Ransomware, extortion, and data theft continue to be executed by cyber criminals. EDR/XDR can be effective in identifying threats, but they do not provide an effective response measure to prevent data theft and ransomware encryption. To truly protect against these threats, the security controls must shield data itself and enforce Zero Trust principles to ensure only authorized access.

Our Solution

Cigent Data Defense™ Shields Up™ adds risk-based multi-factor authentication to ensure all protected files are shielded from access by cyber criminals and malware. The solution ensures that only authorized users and processes have access to protected files, safeguarding sensitive data from ransomware and theft.

How it Works

Data Defense software is configured by policy in the management console to put protected files and folders into a risk-based, threat-aware state. During normal operations, users work as they always do with no impact to their user experience. During a Shields Up condition, users will be required to use multi-factor authentication to access protected files. Data protection policy can be set by file type (extension), folder, and partition (Cigent Secure Vault). The protection can also extend beyond files on the local PC, to cover file shares, clouds (e.g. OneDrive), and external media.

Data Encryption

Cigent Data Defense protects data using strong FIPS 140-2 Level 1 validated, AES 256-bit encryption, the same encryption used by the US government to protect its classified information. The encryption is transparent to the user and can operate in software or take advantage of the hardware-based encryption modules in TCG Opal self-encrypting drives.

Shields Up Mode

During a Shields Up event, Data Defense locks all protected files and requires the end user to use multi-factor authentication (MFA) for access. Shields Up is activated by:

- Your security team can manually engage Shields Up from the Cigent Data Defense management console to a single PC, a group, or the entire organization
- Your SOAR can automatically implement Shields Up based on defined triggers, such as a malware detection on an endpoint or a network intrusion
- Automated by policy when AV is disabled (by an adversary or by the user) or if the AV database is out of date
- Triggered when there is suspicious activity on ports commonly attacked such as 3389 (RDP)
- When AV/ EDR detects an attack (either locally on the PC or from the EDR management console)
- By integrations with SentinelOne, Cisco Secure Endpoint, VMware Carbon Black, Sophos, CyberArk, Dell Trusted Device SafeBIOS, or PC Matic
- Ransomware detection by a Cigent Secure SSD+™ Anti-Ransomware drive (optional)

Authentication Options

Unlocking data during Shields Up requires the user to authenticate prior to accessing protected data. 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

The Cigent Data Defense subscription includes a cloud-based or on-premises administrative console to manage Data Defense endpoint clients. From within the management console, administrators can manage policy for endpoint clients as well as configure integrations with enterprise solutions such as EDRs, SIEMs, and Azure AD. Management features include:

- Create and manage user groups
- Reset a user's PIN
- Add a recovery key for encrypted files
- Enforce authentication policies such as authentication methods
- Define protected folders and file types
- Manage allow list for safe applications
- Set security sensitivity levels
- Pre-approved file access counts and session durations
- Enable notifications and alerts

Additional Features with Cigent Ready Drives*

Service Monitoring

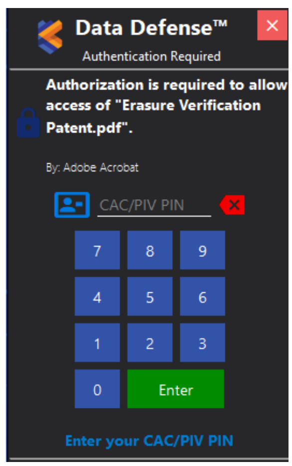
Cigent Data Defense maintains an active "heartbeat" between the Cigent Data Defense service and the drive firmware. In the event the service is disabled (by an attacker or insider), the Cigent Secure Vaults lock at the storage layer, instantly making its content inaccessible to threat actors.

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."



"Our SOC's capability to protect files with Cigent during a security incident is an essential layer of our cybersecurity offering, particularly given the complexity and proliferation of Zero Day and Supply Chain attacks on small and medium sized organizations."

Greg Scasny

CTO, Blueshift Cybersecurity

* 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