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 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 all desired files into a risk-based threat-aware state. Policies can be set by file type (extension) and/or by location (folder). It protects files on the local PC, network file shares, and external media.

In normal operations, users work as they always do with no impact to their user experience. During Shields Up mode, users will be required to use multi-factor authentication to access protected files.

- Always on - requires authentication to access protected files
- Dynamic - requires authentication during a "Shields Up" condition

"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

Shields Up Mode

There are multiple ways to activate Shields Up mode:

- 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 be configured to automatically implement Shields Up based on defined triggers, such as a malware detection on an endpoint or a network intrusion
- Shields Up mode can be automated by policy when AV is disabled (by an adversary or by the user) or if the AV database is out of date
- A trigger when there is suspicious activity on ports such as 3389 (common for RDP) indicating a threat actor is attempting lateral movement.
- An alert from a Cigent Secure SSD self-encrypting drive (optional)
- 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, PC Matic