DIB
CyberDome™

CYBER INTERCEPTOR™

Cyber Interceptor™ is designed to help small and medium-sized defense contractors protect against modern cyber threats, without the resources, time, or complex security infrastructure required by larger organizations.

Many operate without SIEM platforms, dedicated SOC teams, or fully managed security providers, and where tools exist, they are often difficult to maintain, integrate, or operate effectively.

This risk is increasing in the current geopolitical environment, including heightened cyber activity associated with Iranian state-affiliated groups following Operation Epic Fury.

Cyber Interceptor™ reduces the need for complex SIEM and SOC-driven security architectures by automating threat interception directly at the network edge.

LIMITATIONS OF ENDPOINT-BASED APPROACHES

Endpoint Detection and Response (EDR) tools are effective for workstations, but often present challenges in defense environments, particularly for legacy systems and sensitive servers where agents may not be appropriate.

Cyber Interceptor™ is engineered to help small companies or small IT organizations strengthen security through automation - without a big security stack.

Background – DCISE^3 solution – being used in DOD to protect defense suppliers

CELERIUM.com

HOW CYBER INTERCEPTOR™ WORKS: COMMUNITY AND INDIVIDUAL DEFENSE

CYBER INTERCEPTOR™ COMBINES TWO COMPLEMENTARY LAYERS OF DEFENSE:

1. COMMUNITY DEFENSE (DEFENSE INDUSTRIAL BASE LEVEL)

Cyber Interceptor™ operates within the DIB CyberDome, where threat activity is observed and analyzed across participating organizations.

This enables the system to:

- Identify emerging threats across the Defense Industrial Base
- Collect thousands of new threat indicators each month
- Incorporate threat indicators associated with active geopolitical campaigns, including recent Iranian cyber operations following Operation Epic Fury.
- In these campaigns, adversaries have shifted toward coordinated and disruptive attacks targeting U.S. and allied organizations.

2. INDIVIDUAL DEFENSE (ORGANIZATION-SPECIFIC PROTECTION)

Each organization receives personalized, adaptive protection based on its environment.

These continuously updated threat indicators, including those associated with Iranian cyber activity, are applied directly to organization-specific enforcement policies, enabling threats to be blocked before they reach contractor systems.

THREAT-BASED DEFENSE

- Firewall activity is analyzed using continuously updated threat intelligence
- Custom enforcement policies (blocklists) are created for each organization

CONTINUOUS RE-OPTIMIZATION

- Defensive controls are automatically updated, typically every 15 minutes
- Policies adapt to:
  - New threat indicators
  - Changing infrastructure
  - Evolving attack patterns

CONFIGURABLE PROTECTION LEVELS

Organizations can define their level of defense:

- Protection against only highly malicious threats
- Broader protection across multiple threat categories

HYBRID AND MULTI-ENVIRONMENT SUPPORT

Cyber Interceptor™ supports hybrid environments across:

- Leading on-prem firewall platforms (Cisco, Palo Alto, Fortinet, Sophos, Check Point)
- Cloud-native firewalls (AWS, Azure)

This enables consistent enforcement across distributed infrastructure.

View full list of **supported firewall platforms here.**

OPERATIONAL CAPABILITIES

- Real-time visibility into blocked threats
- Rapid allowlisting and exception management
- Custom whitelist and policy control
- Event notifications and alerting
- Fully automated operation with continuous updates

RAPID DEPLOYMENT

Cyber Interceptor™ is engineered for fast implementation in resource-constrained environments:

- No hardware or appliances required
- No endpoint agents or software installation
- Non-intrusive operation (no packet inspection)
- Firewall configuration completed in 30–60 minutes
- Secure communication with decision engine in AWS Government Cloud
- Blocking activity visible within minutes

DIB CyberDome™

A new model for protecting the Defense Industrial Base, built from real operational experience and designed for how it actually operates.

CELERIUM.com