DRAGONSOFT

Strengthen Cybersecurity Compliance
Achieve Holistic Protection

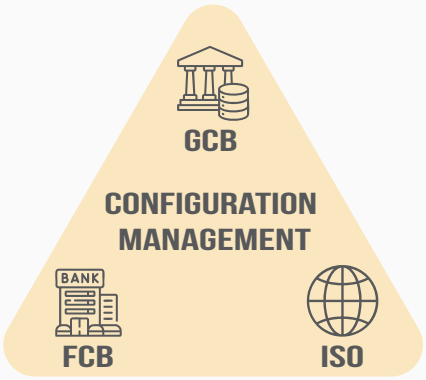
– Domestically Developed Product Catalog –

中華龍網
DragonSoft

CONFIGURATION COMPLIANCE PLATFORM

Ours platform helps organizations maintain secure, standardized, and auditable system configurations across endpoints, including personal computers and server infrastructure. Configuration management encompasses parameters such as password policy enforcement, Remote Desktop Protocol (RDP) access control, and other system-level configurations. It ensures alignment with internal policies and external regulatory requirements.

- ▶ INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
- ▶ GOVERNMENT CONFIGURATION BASELINE
- ▶ FINANCE CONFIGURATION BASELINE



KEY FEATURES

▼ CUSTOMIZABLE COMPLIANCE TEMPLATES

The system offers flexible template customization features, allowing users to configure baseline settings based on specific needs, enabling users to adjust detection thresholds and evaluation criteria. Personalized compliance templates enhance visibility and improve the efficiency of monitoring and auditing processes.

▼ ACCESS CONTROL

The system supports role-based access control (RBAC), allowing organizations to assign different permissions and responsibilities across user roles. Management can define roles and assign corresponding access levels. This ensures operational segregation and accountability, while also enhancing system security and audit integrity.

▼ API INTEGRATION

Supports Web API functionality, enabling seamless integration with third-party applications and systems to achieve automation and system interoperability.

▼ MULTI-OS SUPPORT

Supports a variety of operating systems, including Windows, Windows Server, Linux, AIX, and SUSE. Seamless integration with Jamf is also available, enabling a dedicated GCB compliance solution for macOS environments.

Windows Linux AIX AIX macOS

SEMI E187 ASSESSMENT TOOL

Our product is designed in full alignment with the SEMI E187 standard and specifically addresses the cybersecurity needs of semiconductor environments. It is intended for stakeholders such as equipment manufacturers, system integrators, and service providers that supply products or services to semiconductor fabrication plants, helping ensure that manufacturing equipment is secure by design and remains protected throughout its operational and maintenance lifecycle.

WITH JUST A SINGLE DONGLE,
ENABLES FULL INSPECTION AND SECURES THE SEMICONDUCTOR SUPPLY CHAIN

PRODUCT APPLICATION ARCHITECTURE

SEMI E187
ASSESSMENT TOOL

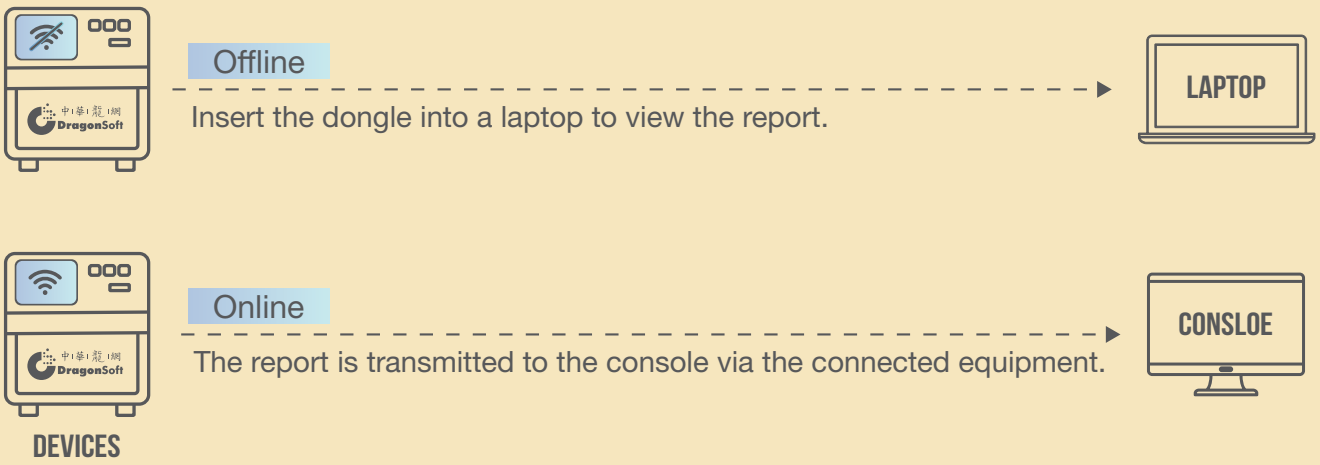
ZTA
DONGLE

- Available in Traditional Chinese, English, and Japanese
- Supports online updates for antivirus and vulnerability databases
- Zero Trust compliant Dongle with built in encrypted storage
- Continuous monitoring with comprehensive log retention
- Provides clear scan reports and detailed information
- Customizable scanning and verification for specific files upon request

PRODUCT FEATURES

- STEP 1 Use the dongle to scan the device
- STEP 2 The scan report is saved on the dongle.
- STEP 3 View the report on a laptop or from the console.

Based on the network status,
users can either check the report locally on a laptop or remotely through the console.



THREAT AND VULNERABILITY MANAGEMENT

In modern cybersecurity defense, vulnerabilities and exploits are among the most commonly targeted entry points for attackers. These may stem from operating systems, applications, third-party components, or misconfigured system settings. If discovered but not promptly patched, they can be exploited to launch ransomware, gain remote access, or exfiltrate sensitive data.

▶ VULNERABILITY ALERT AND NOTIFICATION SYSTEM

The system automatically scans and inventories software on internal devices across enterprises and government agencies. It quickly identifies known vulnerabilities, helping security teams monitor system status and reduce risk. It also supports compliance by facilitating patching, updates, and risk assessments in line with cybersecurity regulations.

Asset Inventory

Vulnerability detection & patch

System Integration & Data Upload

▶ DRAGONSOFT VULNERABILITY MANAGEMENT

With a fully Chinese interface and reports, it improves communication and understanding across departments. The system integrates two key functions "Security Scanning" and "Vulnerability Risk" Management to analyze risks across multiple operating systems and provide a clear view of internal cybersecurity conditions.

中華龍網 DragonSoft

DragonSoft were established in 2003 with a dedicated project team and security experts, committed to the research and development of information security software. Our mission is to provide comprehensive and cost-effective information security solutions.

Website Facebook Line

DRAGONSOFT

+886-2962-0065
www.dragonsoft.com
service@dragonsoft.com