

# RetiShield™ Series

## Global multi-platform access control for optimum risk management



### New challenges in security: Access Controls

Importance of information systems security is nowadays taken into consideration in most industries.

Despite common threats are being continuously re-evaluated; countermeasures are often only deployed at the border network (IDS/IPS, proxy, firewalls...) or at the workstation level (antivirus, user accounts, files privileges...).

While protection become stronger, the complexity of the management at both network and workstation level is increasing. It becomes more and more difficult to enforce and globally manage security policies on multiple systems.

Since protection against external threats has become stronger, most of financial loss now comes from information theft and unauthorized access to data (est. to US\$ 21 millions in 2006) mainly due to internal hacking, malwares and improper or wrongly applied security policies caused by disparate resources, security management and users turnover.

To avoid the hassle of managing a patchworked security, resources and in order to fully control undetected access to information from authorized systems, users or malwares: a new layer of access control is required.

RetiShield™ brings you the ultimate security countermeasure to mitigate risk, enforce global access security policies and prevent information disclosure and loss.

### RetiShield™: the ultimate solution for a global and granular access control management

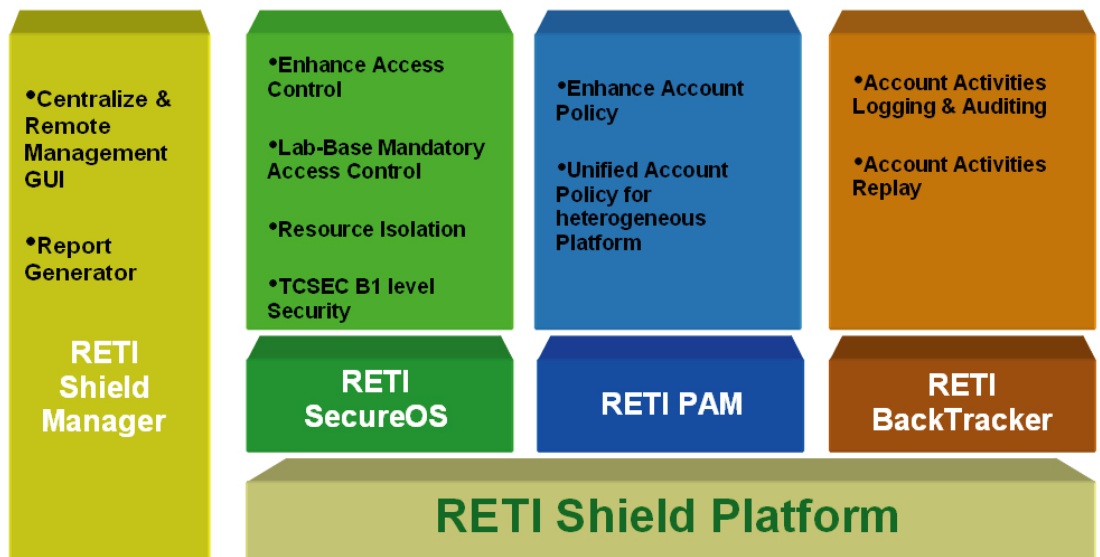
With more than 8 years of experience in information security, RETI is introducing RetiShield™: a software solution that a strong access control in order to achieve B1 protection on multiple operating systems.



### About RetiCorp

Founded in 2005 by a team of network experts from the U.S. and Taiwan, RetiCorp is positioned to provide the best security practices, not only to protect networks against viruses and attacks but also to prevent unauthorized access and information leaks. The innovative USM (Unified Security Management) technology has been embedded into a series of network security products and solutions - RetiEdge, RetiConnect, RetiVista, RetiSensor, and RetiIdentity. The USM product family works collaboratively to form an information-safe zone to secure your business against emerging threats and achieve the goal of Total Security.

Based on Mandatory Access Control a label based protection system, agent oriented design enforce effective security on multiple platforms.  
 RetiShield also offer additional authentication modules as well as centralized management, real time reporting and playback interface.



## Mandatory access control Management solution and B1 protection

The limitation of current discretionary access control is obvious: Super users always have the right to avoid security policy; Compromise a system, get "root" access and control the system.

The goal of Mandatory Access Control (MAC) is to deny users full control over the access to resources they created. The system security policies (set by the security officer) will determinate the access rights on a system where a user may never grant less restrictive access to their resources than the one specified by the administrator. This way information owners may not grant access to un-authorized users.

In the end, a "minimum level of access security" is guaranteed, often called "B1 protection".

B1 protection level is defined in the orange book and refers to **mandatory protection** implementation according to TCSEC evaluation criteria.

Requirements for B1 protection must include an informal statement of the security model, data sensitivity labels, implementation of a mandatory access control over selected subjects and objects and security label exportation.

The effective access is then defined by the authorization for a subject to access an object based on security labels and not based on file access privileges like standard discretionary access controls.

RetiShield™ agents implement a modified Bell-LaPadula model based protection. Using MAC and a need to know concept for a user to access an object, where subject with a lower sensitivity level than an object cannot READ its information. Similarly, subject with higher level of sensitivity cannot WRITE on an object with lower sensitivity level.

## RetiShield Benefits, global risk mitigation

- Annihilate compromised systems impact: The multi-level and independent security guarantees that you **STAY PROTECTED** even if your system has been compromised
- Protects business logic and maintains productivity while managing costs of security policies deployment
- Ensure the degree of confidence in satisfaction of security needs in your risk management process

### With RetiShield™, you can:

Implement separation of duties: ensures that the enforcement of organizational security policy does not rely on voluntary user compliance

- Avoids misconfigurations: users may not grant less restrictive access to their resources than the administrator has specified
- Avoid malicious user access: an Authorized system user cannot access any resource based on his system privileges. Only administrator policies taken into consideration

### Prevent malwares impacts

- Vulnerable programs cannot cause harm to the system when compromised as Mandatory Access Control adds a layer of protection even when a system is compromised
- Viruses cannot compromise systems as they are not allowed to access system files
- Spyswares, worms, viruses or any malware can not install themselves onto the system: Registry detailed access control to prevent the impact of any threat

### Deploy a full protection for better cost management

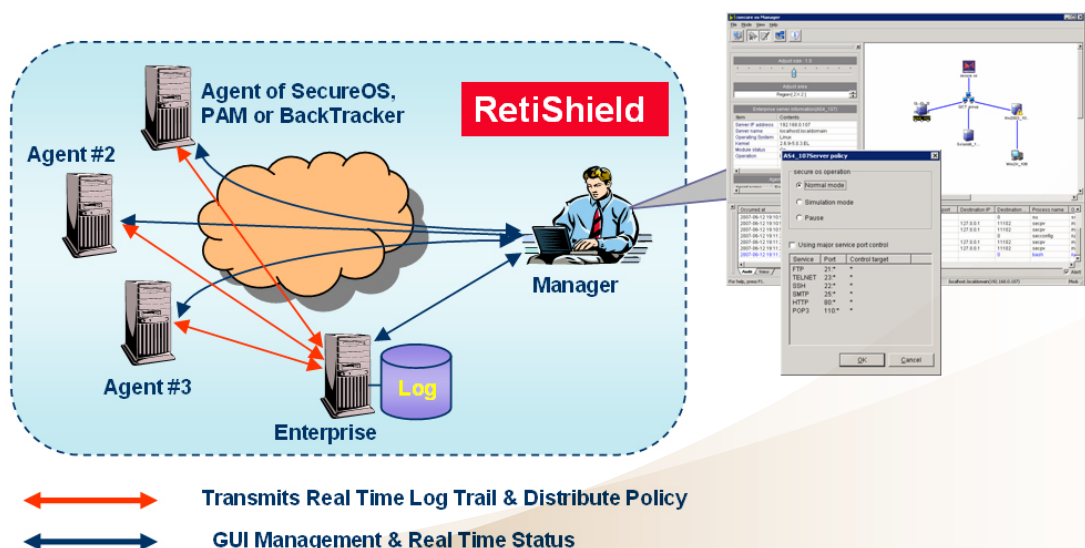
- RetiShield supports multiple platforms including virtual systems
- Protects applications, resources, data, system, processes and accounts
- Avoid redundant server administration through a comprehensive security management. Increase productivity and minimize downtimes

### Easily achieve regulatory compliance

- Individual accountability
- Audit log protection
- Regulatory compliance is achieved with a consistency of strong security policies deployed across multiple resources and a complete audit trail proving the compliance

### Globally manage, configure and audit your security measures

- Allows global management and policies distribution for an easy to implement granular access control
- Real time reporting and command (input/output) playback for a detailed monitoring



## Features:

---

### B1 protection

**Mandatory Access Control** with reference monitor brings B1 level protection to your infrastructure

### Central management

Clustered agent architecture and privileges inheritance for a convenient and simpler policy distribution and management

### Resources isolations

Isolates system resources with security labels and mediates access between the different regions

### Strong Authentication

Supports double authentication for system administrator and security administrator. **PAM** (Pluggable Authentication Modules) is also supported for stronger users account policies enforcement

### Full resources management

Per system User accounts, Registry, Files, Processes, Shares, Services... bringing a security reinforced privilege policy

### Hacker proof

**Label based Protection** to prevent hacker's illegal access if a system is com-promised

### Intrusion Detect & Prevention

Behavioral based intrusion detection to enforce detection of illegal access attempts to the systems

### Integrated firewall

Inside/Outside Discriminated Defense provide a firewall protection to control connection from and to the station

### GUI

Integrated Security Management maps giving a global view of your infrastructure

### Auditing

Real-time Auditing, command replay, logs and statistics report

### Robustness and security

Robustness of the system ensured by ELA3+ certification and fully encrypted communications and storage

### Very High Performances

Less than 3% degradation after RetiShield is loaded onto your system

### Certifications

Label-based Access Control System for Governmental Institutions

- CC EAL 3+ for SUN Solaris
- CC EAL 3+ for IBM AIX
- CC EAL 3+ for HP-UX
- CC EAL 3+ for Linux
- CC EAL 3+ for Windows