

Eliminate Insider Threats

Solution Brief

The Xceedium GateKeeper enables organizations to control and audit internal users accessing critical infrastructure devices and resources.

An internal user can be:

- A local or remote employee including IT and database administrators
- Outsiders working as guests physically within the infrastructure
- Remote contractors and vendors who require access to the infrastructure to perform their jobs

"86% of insider attacks were either by previous or current full-time employees in a technical position within the organization."

- CERT/FBI

The Xceedium GateKeeper delivers unparalleled insider threat protection from users accessing servers (Linux, UNIX, Windows) and network devices (routers, switches, firewalls). The GateKeeper provides a complete solution for insider threat protection for all components within the critical infrastructure - servers, network devices and other components.

Key Features and Benefits

Zero Footprint Access Methodology

- Users gain no footprint (IP Address) on the network
- Protects against unmanaged endpoints propagating viruses or malware
- No ability to copy files or print locally

Centralized Enforcement of Granular Policy

- Authentication Policy (integration with authentication systems)
- Access Controls (user authorization policy)
- Compartmentalization (restricts visibility to authorization resources)
- Containment (patented Leapfrog prevention)
- Remediation (corrective action capabilities)

Monitoring

- All activities and automatically alerting for violations

Recording and Tracking

- All user events and activities to provide a comprehensive audit trail

Viewing of Centralized Reports

- All user events, attempted violations, and session activities

Leading Industry Standard Certifications

The Xceedium Commitment to Quality

Listed below are the formal testing certificates and validations that Xceedium has earned. Additionally, Xceedium also has been system tested extensively in the federal government under individual agency DISCAP and DIACAP standards.

- **Common Criteria EAL2 (ISO 15408)**
Date Awarded: October 2006
- **Common Criteria EAL3 (ISO 15408)**
Date Awarded: April 2007
- **Common Criteria EAL4**
Product is officially in validation with NIAP
- **FIPS 140-2 Level 2**
Date Awarded: August 2007
- **Citrix Ready Certification**
Date Awarded: January 2008
- **MYSQL Technology Partner**
Date Awarded: January 2009
- **Cisco Technology Developer Program**
(In Process)
- **RSA Secured Technology Partner**
Date Awarded: November 2008

The Insight and Control You Need to Eliminate Insider Threats

A variety of insider threats can put your organization at substantial risk. Employees are only one dimension; internal users come in all shapes and sizes from IT administrators to vendors and the list goes on. Controlling these users can be a daunting task. Where do you start? You need an insider threat solution that controls insiders while providing a detailed audit trail. Xceedium's GateKeeper empowers you to seamlessly control the insider based on your dynamic security policy and therefore eliminate the threat they pose to your organization. GateKeeper is the only solution that lets you control, contain, compartmentalize and audit your users in real time to safeguard your critical infrastructure while enabling business to continue as usual.

How to Eliminate Insider Threats Depends on Your Network Infrastructure

How you use the GateKeeper to eliminate the insider threat from users who need to access key infrastructure resources depends on your network infrastructure.

Deployment Models

- **Physically and/or logically segmented networks**

A physically or logically segmented network, in which users and key infrastructure resources reside on different segments, provides a single entry point where the GateKeeper sits and all user traffic is directed through it. Your network topology remains unaltered as the GateKeeper enforces your policy and tracks and logs all user activity for future audit.

- **Flat networks**

A flat network, in which users and key infrastructure resources reside on the same segment, requires you to create Access Control Lists (ACL) to direct users through the GateKeeper. Your network topology may or may not be altered based on your ACL implementation. GateKeeper enforces your policy and tracks and logs all user activity for future audit.

- **Outsiders and guests physically on site**

An outsider or guest who is visiting your site and needs to access key infrastructure resources can be logically isolated using your existing 'guest network.' All outsiders and guests are directed through the GateKeeper, which resides at the boundary of the guest network, providing a single entry point to key infrastructure resources. GateKeeper enforces your policy and tracks and logs all user activity for future audit.

Example Network Topology

