

Xceedium GateKeeper

Data Sheet

Xceedium, Inc., the leading provider of access control and audit solutions, provides commercial and government organizations with a comprehensive access control, monitoring and audit solution to protect against insider and external threats.

Xceedium's solutions address the fundamental shift in corporate computing when it comes to assigning and managing trust. Regulatory and public pressure to incorporate accountability and transparency into all facets of IT operations has resulted in new requirements around access and audit. In this new 'Zero Trust' computing model, users, both insiders and outsiders -- such as consultants, vendors, IT administrators, outsourced employees and partners -- play an important role in the success of organizations and require access to critical network infrastructure.

Ensuring these users are provided the appropriate privileges is crucial in protecting the organization and its information assets. Xceedium GateKeeper is flexible enough to enable users to do what they need to get their job done, but tight enough to ensure unauthorized access doesn't occur under any circumstances.

It provides unmatched enforcement, monitoring and auditing of user activity across the entire infrastructure, allowing organizations to easily define access privileges based on policy. Purpose built with the needs of highly complex, geographically dispersed and heterogeneous technology infrastructures in mind, Xceedium GateKeeper is the only automated, end-to-end solution that can provide organizations with both the agility and control required to successfully meet these new zero trust requirements.

Solutions:

Third Party Access Control

Xceedium GateKeeper allows organizations to balance the need for accessibility against the requirements for security, manageability, control and audit. The Xceedium GateKeeper meets these requirements by ensuring that third parties are controlled and contained to authorized areas and a complete audit trail for accountability is established.

Automated Compliance Reporting

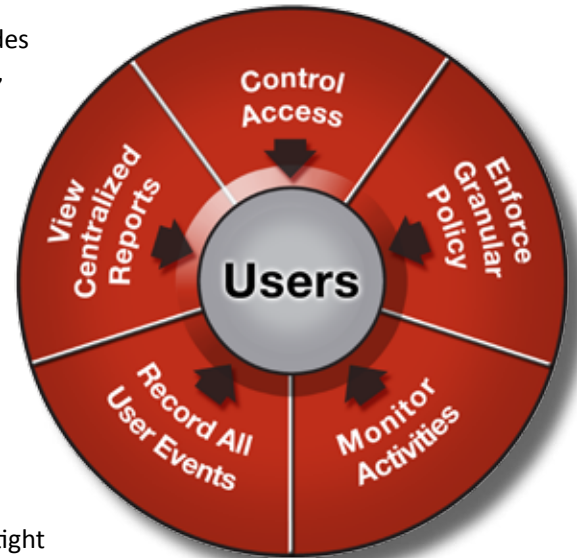
Xceedium GateKeeper centralizes and streamlines all activities required to provide real-time accountability for access across the enterprise, providing the necessary proof for compliance. This includes granting access, compartmentalizing, containing, monitoring, tracking and reporting. Centralized reporting and custom and out-of-the box reports allow organizations to easily meet compliance mandates such as PCI DSS, SOX, HIPAA and FISMA.

Reducing the Risk of Outsourcing

Xceedium GateKeeper significantly reduces the risk of outsourcing with its patent-pending LeapFrog Prevention technology which contains users to authorized areas and proactively detects and thwarts violations to ensure automatic enforcement of policy.

Secure Remote Management

Xceedium GateKeeper allows an organizations devices to be accessible from a single, centralized management portal, providing for zero-touch administration and zero-footprint access, regardless of geography. With the GateKeeper, IT data centers and equipment rooms remain locked, on-site administrators are rarely required and administrative travel is basically eliminated. This results in faster response time, significant cost savings and enhanced physical security.



Feature	Description	Benefit
Access Control		
Restrictive Access Methodology	Zero-footprint access methodology using reverse port tunneling to provide secure access to any well-defined TCP/UDP port using integrated applets or third party clients.	Reduces risk by employing a deny all permit by exception (DAPE) security model while preventing endpoints from gaining a footprint on the network. It also ensures accountability by delivering visibility to the user's source IP address.
Centralized Authorization Policy Management	Provides a single location to manage authorization policy for any users accessing infrastructure resources.	Increases security by centralizing policy management and enforcement for user activity across the infrastructure. It also increases efficiency by centralizing authorization policy management.
Enforce Granular Policy		
LeapFrog Prevention	Uses a white/black list approach to contain users to authorized servers or network devices using socket and command filtering technology.	Enforces controls for users when they are inside the critical infrastructure enabling organizations to easily meet compliance and security requirements.
Integrated Java Access Applets	Uses integrated applets like RDP, VNC, SSH and Telnet, with Reverse Port Tunneling access methodology to provide compartmentalization at the port level. This also includes support for mainframes (TN3270 and TN5250).	Enhances security and provides strong controls while protecting the entire IT infrastructure by compartmentalizing and segmenting users according to their roles and responsibilities.
Monitor Activities		
User Activity Monitoring	Real time monitoring and alerting for attempted policy violations.	Provides visibility into user activity and proactively alerts so automated corrective actions can be taken.
Automated Remediation	Fully customizable and automated remediation based on the number of attempted violations.	Automation of policy enforcement using pre-defined corrective action capabilities.
Record All User Activities		
Universal CLI Session Recording	Full session recording for Telnet, SSH and Serial Command Line activities and also allows for fully searchable playback of the recorded sessions. This also includes support for mainframes (TN3270 and TN5250).	Validates controls by establishing a complete audit trail and ensures full accountability for user activities.
Windows Graphical Session Recording	Full recording for all RDP sessions with a searchable DVR-style playback viewer.	Validates controls by establishing a complete audit trail and ensures full accountability for user activities.
View Centralized Reports		
Custom Reporting	Custom and ad hoc reporting module for real-time reporting of log data.	Customized targeted compliance reports which can be automatically generated to meet audit and regulatory requirements.

System Components

Chassis	1U IPC Chassis
Power Supply	250W Power Supply Unit (PSU) (220W at 50+°C)
System Board	Single Board Computer (SBC) Intel 945G Chipset w/ Socket 775
CPU	Intel Core2 Duo 2.13GHz
Memory	4 GB DDR2
Primary Storage	16 GB SATA Solid-State Drive (SSD)
Secondary Storage (backup)	16 GB SATA Solid-State Drive (SSD)
Display	16x2 LCD Display

Standard Interfaces

Network	Six Gigabit Ethernet Ports
LCD Inputs	Four buttons
Serial	One RJ-45 Serial Port

Physical Specifications

Height	1.7" (4.40 cm) or 44 mm
Width	17" (43.18 cm) or 432 mm
Depth	14" (35.56 cm) or 356 mm
Unit Weight	14 lbs. (6.3 kg)
Shipping Weight	20.5 lbs. (10.6 kg)
Enclosure	Fits standard 19 rack