

Secure Remote IT Operations with Xceedium GateKeeper

Highlights

Xceedium

Vendor name: Xceedium, Inc

Product name: Xceedium GateKeeper

Product function: Secure Remote IT Operations

Vendor contact information:

Website: www.xceedium.com

Address: 30 Montgomery Street, Jersey City, NJ 07302

Telephone: (201) 536-1000 x112 or (877) 636-5803 x112

Email: info@xceedium.com

Availability: Immediate

- Enterprises may open multiple internal and external access points (including modems, serial controllers, back doors, console access, in-band and out-of-band administration tools, open ports, IPSec or PPTP, and virtual access for blade and grid administration), many of which effectively bypass perimeter or centralized security controls. Enterprises must establish tight controls in many places, which are difficult to maintain, or shut down these alternative access points.
- Internal administrators are over-provisioned with highly sensitive 'root' access to multiple systems, with no separation of duties. This is increasingly becoming the main threat to IT security. Enterprises need to provide selective, temporary, specific, and secure access to administrative roles based on the granularity of their access need.
- Multiple access points and over-provisioning reduce control and audit capabilities, raise compliance risks (specifically for Sarbanes-Oxley, GLBA, and HIPAA regulations), and increase the complexity of security policy administration. Enterprises need to centralize access administration, provide audit, and control access by internal administrators, vendor support, and consultants.
- Unmediated physical access to systems and native consoles in equipment rooms is a high security risk. Direct, local management also increases costs, including the travel costs for administrators to manage geographically diverse networks, and/or the cost of local staff. Enterprises need to lock down equipment rooms, and provide secure remote management to reduce the time and resource costs, and the security risks, of local and direct operations.
- Separation and lack of integration between access methods for in-band, out-of-band, and power management is insecure, reduces audit and control, and lowers the productivity of system administrators who must switch consoles, sessions, or devices to administer blades and remote systems. Enterprises must integrate these access methods to reduce both costs and risk.

Executive Summary

While perimeter security protects against unwanted intruders, authorized IT administrators still require secure, remote access to many systems, across many offices and geographies. Traditional solutions like SSL/VPN, IPSec, modems, and direct physical access introduce unacceptable risks, high costs, complexity that is hard to maintain, and/or compliance problems around audit and control. Xceedium GateKeeper addresses these problems with an appliance-based solution for secure remote IT operations. Enterprise Management Associates (EMA) recommends organizations of all sizes and industries review this solution to resolve problems in providing internal administrators and external resources access to sensitive systems, devices, and applications.

Problems with Remote Operations

Many enterprises have implemented IT security measures to ensure that their perimeter is secure, such as firewalls, intrusion detection systems, and identity and access controls. However, there are still security exposures and risks in providing secured access for IT Operations, including system administrators, remote consultants, and vendor support. For example:

Xceedium GateKeeper – Securing Remote IT Operations

Xceedium GateKeeper is an appliance-based solution for secure remote IT operations. It effectively acts as a centralized management portal that provides secure access for remote administration, connecting authorized users through a secure channel to a wide variety of remote systems, consoles, devices and control points. Instead of connecting directly through virtual consoles, IPSec, SSL/VPN, modems, etc., GateKeeper provides a centralized and secure connection for all users – including administrators, operators, vendor support, consultants, and end-users.

This resolves many of the problems, costs, and risks associated with administrative access, such as:

- Providing a single access point removes the risk of legitimate and illegitimate back doors. All access by administrators to the Xceedium GateKeeper is secured by SSL over TCP, allowing the enterprise to close all access except one standard firewall port. Communications from GateKeeper to specific systems, however, remains highly flexible, supporting access methods including telnet, SSH, GUI, serial, KVM, and power. This reduces risk, and saves the significant costs of redesigning network security to accommodate network-wide secure protocols such as IPSec.
- Granular, timely, and functionally specific access control reduces the risk of over-provisioning. GateKeeper provides detailed control over administrator access, including role- and identity-based access control, scheduled access times, and granular restriction on access rights. This allows enterprises to provide temporary access as required, separate control activity, restrict visibility, and lock down excessive access.
- Centralized management capability reduces the risks and costs of physical access. The ability to access and control all remote consoles and devices from a single management portal provides zero-touch administration regardless of geography. Equipment rooms can stay locked, local administrators are rarely required, and administrative travel is greatly reduced, resulting in significant cost savings and reduced physical security risks.
- Central, restricted access through a single portal improves audit and control. GateKeeper provides secure, identity-based access with a single point of ingress, as well as flexible access notification and audit facilities.

This establishes simple standards for access control, provides central audit reporting with granularity of identities, activities, targets, times, and access methods.

Xceedium GateKeeper provides a synergistic companion to traditional enterprise monitoring systems, such as HP/OpenView, BMC Patrol, IBM/Tivoli, and CA-Unicenter. Remote monitoring connectivity alone does not provide all the access required for remote support. Individual tools for remote control are also not sufficient to accommodate the broad requirements of remote administrators. While system monitors provide the eyes into enterprise operations, GateKeeper effectively provides the hands, allowing administrators to not only monitor remote systems and devices, but also to directly and securely control them.

Differentiating Factors

Xceedium GateKeeper has a number of significant differentiating factors, by providing capabilities including:

- Integration of in-band, out-of-band, power, and regular access controls – individual tools such as KVM must be supplemented by additional tools to provide all the touch points and controls required for remote administration. This complexity adds to management costs and reduces security, audit, and control. GateKeeper unifies these multiple entry points, simplifies infrastructure management, more tightly restricts access, and improves audit and control.
- A single target for remote administration access – with GateKeeper, there is no need to open up multiple targets inside the network, expose modems and serial access points, or open multiple ports in the firewall. It is designed specifically with remote support in mind, to replace SSL/VPN with more functionality, and replace IPSec with easier administration.
- Native interfaces that are secure and accessible – GateKeeper supports access to systems and devices with many different native protocols and control methods (such as telnet, SSH, GUI, serial, KVM, and power). However, user access to GateKeeper is through a single secure protocol (SSL over TCP), which simplifies firewall management, and provides extensive compatibility for remote access.
- Multi-infrastructure administration and management from a single control point – GateKeeper provides a single point of control for multiple islands of IT

operations and infrastructure. This resolves the issues of control and audit surrounding a proliferation of tools, by providing comprehensive, platform-independent access to blade management systems, supporting infrastructure, and legacy devices.

- Secure cross-network and data center connectivity – GateKeeper’s Identity-based Concurrent Multi-network Connectivity (ICMC) allows IT administrators to connect securely to multiple networks and data centers using multiple concurrent sessions. Each session is secured by identity, exposing only authorized services and resources in each network. This removes the need to open up network connectivity (e.g. using IPSEC or SSL VPN) between otherwise separate networks and data centers, reducing the associated management costs and security risks.
- Secure server-to-server connectivity – GateKeeper’s Identity-based Secure Server-to-Server Connectivity (ISSC) allows servers and other automated systems to connect through the secure management portal, with the same level of identity-based access control and auditing as manual, human connection. This extends the cost savings, risk avoidance, and accessibility of GateKeeper beyond physical human interaction, to automatic, inter-process, and server-to-server communications.
- Ease of installation and management – Xceedium GateKeeper is an appliance-based solution, with the software installed, configured, and ready to go. This makes it much easier to install, implement, and manage than most comparable software solutions.

Xceedium GateKeeper Use Cases

Xceedium GateKeeper has been successfully deployed in internet and intranet installations at large government agencies as well as Fortune 1000 companies. Two use cases drawn from these customer implementations are as follows:

A large financial institution had several globally dispersed datacenters, managed by dispersed IT resources. They needed a single point of entry for administrative access, so they could enforce their security policies, and eliminate backdoor access via modems and T1s. Xceedium GateKeeper provided them with a single, secure front door so they can now enforce their policies enterprise-wide. They can strictly audit and control who has access, what access they have, when they have access, and what they are doing. This has helped with their compli-

ance reporting, especially around Sarbanes-Oxley and GLBA. Another requirement was to provide “touch-free maintenance.” Xceedium GateKeeper allowed them to connect remotely and securely to serial consoles for their routers, to KVM utilities over IP for SAN management, and to their power control devices. They were able to avoid the costs and risks of local administrators, and maintain compliance across a geographically distributed network

In a large defense organization, there was significant concern about the access and physical security of their widely distributed blade deployment. Administrators had keys not only to the blade frame, but also to the blades themselves, creating an unacceptable security risk. They required a solution that would allow administrators, and hardware and software vendors, to access these blade systems through a secure interface, without having physical access to the blade hardware, and without having access beyond their immediate requirements. Xceedium GateKeeper addressed this requirement by providing secure remote access, with granular and scheduled restrictions, to allow vendors to access the blade management tools without over-provisioning, and without having any physical access to the blade infrastructure. In addition, this organization had older devices that could only be accessed via telnet. However, any use of telnet from outside the organization, even over SSL, contravened their security procedures. Xceedium GateKeeper addressed this requirement with its ability to work with legacy protocols inside the firewall, while serving emulated sessions to end-users. The end-user applet still looks like telnet to the administrator, but GateKeeper encapsulates the traffic via SSH and SSL, and decrypts it inside the firewall to communicate natively with the legacy devices over telnet, fully satisfying the security requirements of this organization.

EMA’s Perspective

Xceedium GateKeeper is a smart and effective solution to a complex, significant, and widespread problem. Administrators generally have too much access, through over-provisioning, direct physical access, and backdoor access to systems. This access is often not properly controlled and audited, creating unacceptable security risks. It can also be expensive to maintain secure access, and to have multiple IT resources go on-site to support wide geographic networks. Xceedium GateKeeper provides an excellent complement to monitoring systems, blade management, and other remote access solutions, by integrating and securing remote IT operations.

Small and medium enterprises that outsource their IT or support services, or that have external contractors who connect to internal systems and applications, would benefit from using Xceedium GateKeeper to implement a secure, single point of access for these remote staff. Larger enterprises that need external vendor support or contractor access can similarly benefit by providing locked-down access that is still flexible to accommodate their business needs. Any enterprise that has IT systems in multiple geographic locations, especially where blades and legacy equipment are deployed, will benefit from centralizing access to these dispersed systems. The ability to tightly control and audit internal administrator access will reduce risk, and make compliance and reporting much easier.

About Xceedium

Xceedium Inc. is a privately held company headquartered in the USA in Jersey City, New Jersey. Founded in 2000, Xceedium now has over 50 customers including large financial, government, and Fortune 1000 companies. Their flagship product, Xceedium GateKeeper, is an appliance-based solution for secure remote IT operations. GateKeeper delivers a service-oriented framework for centralized, policy-based, secure access for IT operations management, and is compliant with Common Criteria and FIPS 140. For more information, visit www.xceedium.com.

Enterprise Management Associates

2585 Central Avenue, Suite 100

Boulder, CO 80301

Phone: 303.543.9500, Fax: 303.543.7687

www.enterprisemanagement.com

1096.041706