

KEY BENEFITS

- Standardization on Office Communications Server 2007 by blocking access to unauthorized real-time communications networks
- Built-in support for both Microsoft Office Live Communications Server 2005 and Office Communications Server 2007 allows for flexible migration
- Identity management with policy control at global, group and individual employee levels
- Guaranteed TrueCompliance™ to meet corporate policies and government regulations
- Interoperability with existing anti-virus solutions
- Zero-day blocking of IM-based worm and virus attacks
- Anti-SpIM controls protect bandwidth and close security holes
- Archival of file transfers over Office Communications Server 2007 into WORM storage
- Advanced content filtering and keyword blocking to prevent loss of confidential information
- Targeted remediation and inoculation of spyware-infected endpoints without deploying client software
- Automatic protection against threats identified by FaceTime Security Labs
- Granular controls for multiple UC modalities
- Support for VMWare deployment enhances scalability and redundancy

The Reality of Real-time Communications

Instant messaging (IM) and other real-time communications protocols are a fact of life in today's enterprise, as evidenced by the rapid adoption of unified communications (UC) platforms such as Microsoft Office Communications Server; industry analysts expect enterprise IM to reach 100% adoption by 2010.

Beyond the world of IM and P2P channels, more than 200 social networking sites are now available to anyone with a browser, several of which have evolved into full-blown development platforms – Facebook alone supports almost 20,000 applications. From the enterprise side, it's become common practice for human resources to review candidates' social networking activities as part of the hiring process, and for knowledge workers, social networks have become an always-on focus group for testing and reviewing new ideas.

Despite widespread access to enterprise-ready communications networks such as Office Communications Server 2007 and regardless of corporate policy, users continue to communicate through public IM networks such as Yahoo, Google Talk, and MSN and through social networks. Unfortunately, these real-time communications channels are increasingly becoming the threat vector of choice for malware attacks; add client-side code vulnerabilities and the potential for intellectual property loss, compliance breach and identity theft, and it is clear that these channels are a major risk factor for existing security, policies and infrastructures.

Additional security requirements arise when the edge of the corporate network effectively moves out into the broader community as employees become increasingly mobile. And as the line between corporate networks and social networks blurs, social networks and their applications – many of which involve real-time communications – become an issue for enterprise IT.

Specific challenges

Enterprises are faced with a number of key discrete challenges in managing the use of IM in a unified communications environment:

- Collaborative environments, including social networks, are increasingly targeted by malware, with blended threats (viruses, worms, spyware, and more) hopping from public to enterprise network — federation with public IM networks and partners only adds to the risk.
- Not only are more attacks entering the network over real-time channels than email, but the attacks themselves are becoming more damaging. Crimeware, rootkits, exploits, and other malware are designed to bypass traditional security measures, and the real-time channel only makes that task easier.
- Just as malware is moving to real-time communications to bypass existing security measures, spam is moving beyond the email inbox into the IM stream, further increasing the risk of accidental malware introduction as well as increasing traffic.
- Compliance regulations, including e-Discovery, largely apply to real-time conversations and chat threads just as they do to email records.
- Communications that can't be seen can't be monitored. Unverified identities such as “buddy names” prevent appropriate corporate policies from being applied to public IM communications, and the port-hopping behavior exhibited by these applications renders simple blocking controls unusable
- Proprietary information can be transferred outside the company networks using unmonitored IM channels

KEY BENEFITS

- FaceTime Enterprise Edition for OCS provides organizations with the tools to standardize their Instant Messaging (IM) infrastructure on the Office Communications Server 2007 unified communications (UC) platform while ensuring compliance and securing their environment against malware traveling over external real-time communications channels.
- Single solution to secure, manage and control the use of instant messaging, social network applications, web conferencing, VoIP, and other Office Communications Server 2007 tools
- Leverage existing investment in Office Communications Server 2007 and anti-virus to apply the same high level of security and compliance across all real-time communications channels
- Prevent spyware with targeted remediation and inoculation of infected endpoints
- Minimize IT administration costs with flexible deployment and enhanced management capabilities, including support for VMWare deployments
- Mature, proven solution backed by world class research and used by leading corporations around the world

FaceTime Enterprise Edition brings together the benefits of IMAuditor and Unified Security Gateway to deliver the first fully-integrated solution to unified security, management and compliance for Office Communications Server 2007.

Security

- Blocks SpIM using a combination of allow/block lists, rich content filtering mechanism and patent-pending challenge/response
- Prevents zero-day worm and virus attacks from using OCS communications channels
- Continuous protection against greynet threats identified by FaceTime Security Labs
- Scans file transfers using existing anti-virus tools
- Delivers targeted remediation of spyware-infected endpoints without client software deployment
- Sets granular level user policies for the transfer of files over IM
- Blocks unauthorized real-time communications applications, including Facebook applications

Compliance

- 100% auditing across major public and enterprise IM, web conferencing and professional and social networks
- Consolidated transcript export reporting for faster e-Discovery process handling
- File transfer archival support to WORM storage
- TrueCompliance™ blocks attempts to circumvent established compliance workflow
- Automatic display of customizable legal disclaimers to all parties involved in the IM conversation informing them that OCS is a corporate not a personal messaging system
- Blocks messages depending on severity of breach, with real-time alerts
- Prevents data tampering by assuring exported conversations match recorded conversations at the level of time-stamped messages
- Stores messages in binary and text format in the order they appear for content accuracy
- Enforce ethical rules in real-time by configuring "Chinese Wall" policies to restrict intergroup contact and using "Hair Pinning" to restrict inter-organization contact
- Establishes compliance workflow with custom search queries for tracking and managing review of conversational content

Management and Control

- Hierarchical view of enterprise to provide rich policy management at global, group and individual employee levels
- Import employees from nested directory groups for greater flexibility in use of corporate directory groups
- Fine grained control of OCS client capabilities including the ability to manage file transfer, collaboration (e.g., audio/video conferencing, VoIP, games), and other client privileges at the company, group, and user levels
- Granular permissions to control audio and video across all real-time communications applications
- Provides visibility and insight into real-time communications throughout the distributed enterprise
- Controls IM capabilities at global, group, and individual employee levels
- Unique support for AOL Identity Services (including Triton) and MSN Connect allows businesses to own corporate domain name use in buddy names and match buddy names to company directories
- Real-time enforcement of policy changes
- Unified real-time usage reports, inter-group reports and graphical monitoring of statistics
- Secure, intuitive Web-based access to configuration functions by authorized personnel

Ease of Deployment and Operations

- Flexible OS and DB platform-neutral deployment architecture in the LAN
- Co-exists with standard IT infrastructure, such as firewalls, load balancers, email systems, and proxy servers
- Support for VMWare deployment enhances options for architecture scalability and redundancy
- Load-balances among redundant/standby directory, database and corporate proxy servers
- Plug-and-play deployment at network perimeter with purpose-built hardened configuration
- Automated protocol and threat protection updates

Enterprise-grade Solution

- Ease and flexibility of enterprise deployment means minimal IT administration
- Cost-effective support of global scaling for complex distributed data centers
- Support for multiple languages
- High level of fault-tolerance provides support for normal operations in the unlikely event of a critical infrastructure resource failure
- Maximize IT and compliance productivity with intuitive Web-based administration and reporting



Software Requirements

- Microsoft Windows 2000 Server or Windows 2003 Server
- Microsoft SQL Server 2000

Hardware Requirements

- Pentium 4 2 GHz CPU or higher recommended
- 1 GB of RAM
- 30 GB Available Hard Disk Space