

# Integrated Security Management for Unified Communications Applications

Track, analyze, and control the security posture of all real-time applications utilizing the converged unified communications network

VoIP and other unified communications (UC) implementations have opened new doors for cybercriminals to exploit, which has hampered UC adoption. The new attack vectors associated with UC real-time applications (VoIP, IP video, collaboration, and instant messaging) are now a major concern for the security manager along with other threat vectors such as email and web. The Sipera UC-Sec appliance is integrated with McAfee<sup>®</sup> ePolicy Orchestrator<sup>®</sup> (McAfee ePO<sup>™</sup>) software to provide more comprehensive enterprise security. The Sipera UC-Sec appliance ensures that the VoIP/UC infrastructure and endpoints (mobile or fixed) are protected and visible to the security manager for the first time with McAfee ePO software.

## McAfee Compatible Solution

Sipera UC-Sec V4.0.4 and McAfee ePO software 4.5 and 4.6

Sipera's UC-Sec appliance provides complete application-layer security architecture in one device:

- *Real-time encryption and privacy*—Providing stateful, real-time end-to-end encryption
- *UC recording and logging support*—Securely forking media for efficient call and UC traffic recording and logging by a centralized third-party recording system
- *Policy enforcement*—Ensuring that communications policies related to mandated requirements are enforced
- *Access control*—Managing and enforcing the authentication of users, including enabling two-factor authentication for VoIP and UC
- *Threat mitigation*—Detecting and halting intruders and eavesdroppers who seek to steal consumer information and credit card data

UC holds great promise for enterprises of all types to adopt new modes of communication and interaction with customers, suppliers, partners, and an extended array of remote and distributed employees. Through VoIP, IP video, instant messaging, collaboration, and other tools, enterprises can improve agility and efficiency, reduce travel costs, boost business continuity, and gain competitive advantages.

Motivated by the prospect of lucrative payoffs, cybercriminals are staging a variety of attacks, exploiting network vulnerabilities, and taking advantage of unsuspecting enterprises. According to the Communications Fraud Control Association, toll and premium services fraud totaled nearly \$20 billion in 2009. Chief causes were unsecured VoIP PBX and UC implementations. In a massive recent international toll fraud case, the U.S. Federal Bureau of Investigation reported that an estimated \$55 million worth of minutes were stolen from U.S. enterprises by a single fraud ring that resold the minutes in European countries. Sipera UC-Sec and McAfee ePO software manage and check that your VOIP/UC implementations are secure and compliant, providing peace of mind for your security manager and helping to improve cost effectiveness.

## Holistic View of the Risks Inside and Outside of the Firewall

Mobility is a key benefit of UC, extending the office experience beyond the firewall, but communications must be secure, encrypted, threat-free, and easy to manage. UC extends the office environment to remote workers using VoIP-phones, softphones, smartphones, and tablets. The real-time nature of the communication itself has typically prevented security devices from performing full application layer inspection of voice traffic, yet the Sipera UC Sec enables full application layer inspection and security threat reporting to the McAfee ePO platform, allowing the security manager to have a complete view of these communications.

The Sipera UC-Sec appliance addresses a wide range of security challenges associated with launching and managing UC implementations and teleworking programs. The UC-Sec appliance offers comprehensive VoIP/UC security by providing policy enforcement, threat protection, access control, and privacy for VoIP/UC. When integrated with the McAfee ePO platform, a holistic view of threats, both inside and outside of the firewall, is available efficiently, rapidly, and centrally.

## Solution Brief Integrated Security Management for Unified Communications Applications

*“When we set out to deploy VoIP as part of our communications transformation, we planned from the outset that we would never compromise the security and privacy of the many different types of data and communications traversing our network. We selected Siperas UC-Sec appliance so we can deploy highly effective, targeted security that ensures confidentiality.”*

—Cindy Phillips,  
Director, Northern  
Illinois University

UC also can have significant impacts on your ability to comply with critical privacy requirements, regulatory mandates, industry best practices, and fiduciary responsibilities around information security. The Siperas UC-Sec appliance provides many critical compliance features that help solve many of these regulatory mandates. For example, the industry council that issues payment card privacy rules recently unveiled new guidance that indicates VoIP and other unified communications are in scope for the Payment Card Industry Data Security Standard (PCI DSS) rules. With UC-Sec, security managers can quickly and easily establish the needed encryption, logging, archiving, and intrusion prevention functions to ensure compliance with PCI DSS.

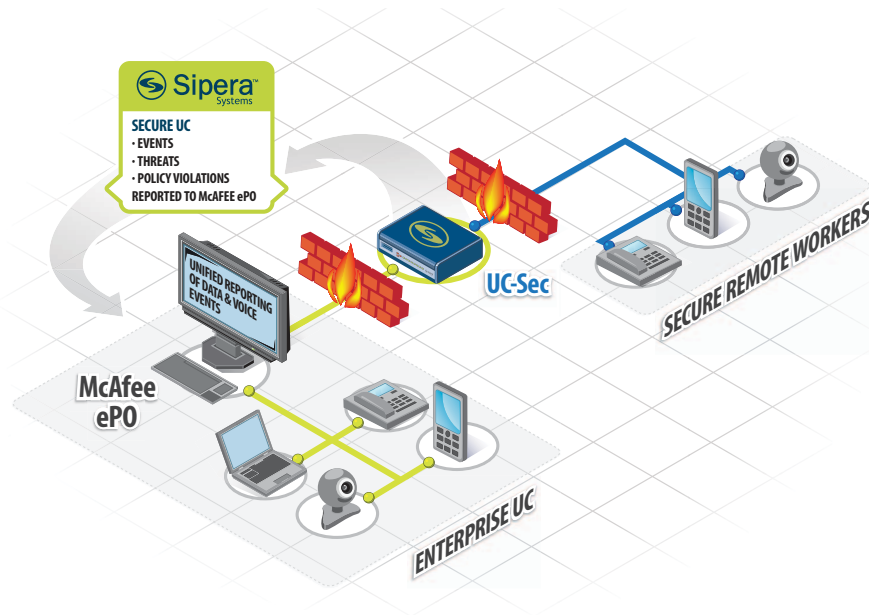
### True UC Security Requires Real-Time, Multilayer Security to Achieve UC Benefits

The Siperas UC-Sec platform offers security solutions for virtually every enterprise. The UC-Sec appliance offers plug-and-play security, enabling mission-critical unified communications. Backed by the VIPER Lab team’s leading UC security experts, UC-Sec is equipped with the most up-to-date vulnerability information to ensure enterprises are protected from UC related attacks. The UC-Sec appliance is designed to securely enable many deployments, including; IP PBX and VLANs, Mobile Client Security (UC SliC), SIP trunks, Secure Border Access for I/CLECs, and remote workers.

The McAfee ePO platform seamlessly ties all endpoint security devices, including UC-Sec, into a single console for management ease of use and compliance peace of mind. Siperas recognizes McAfee as the industry leader in threat mitigation, and this integration enables enterprises using McAfee ePO software to securely unleash the benefits of UC and improve operational costs.

### About Siperas

Siperas offers groundbreaking solutions securing voice, video, messaging, collaboration, and other real-time communications in converged IP networks, boosting compliance with information security requirements and simplifying the adoption of UC. Siperas’s innovative Borderless UC architecture delivers secure and private enterprise-class communications to any device over any network in any location. Backed by the industry-leading research of the VIPER Lab, Siperas’s award-winning UC-Sec appliance provides comprehensive threat protection, policy enforcement, access control, and encryption in a single, flexible, plug-and-play device. The UC-Sec is pre-integrated with all market-leading UC vendor solutions and is the world’s first UC security device to be Common Criteria certified, meeting the stringent international standard for IT security.



### About McAfee ePolicy Orchestrator Software

McAfee ePolicy Orchestrator software is the industry-leading security and compliance management platform. With its single agent and single-console architecture, McAfee ePolicy Orchestrator software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.



McAfee  
2821 Mission College Boulevard  
Santa Clara, CA 95054  
888 847 8766  
www.mcafee.com

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided “AS IS” without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.

McAfee, the McAfee logo, McAfee ePolicy Orchestrator, and McAfee ePO are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2011 McAfee, Inc. 25904brf\_sipera\_0411\_ETMG