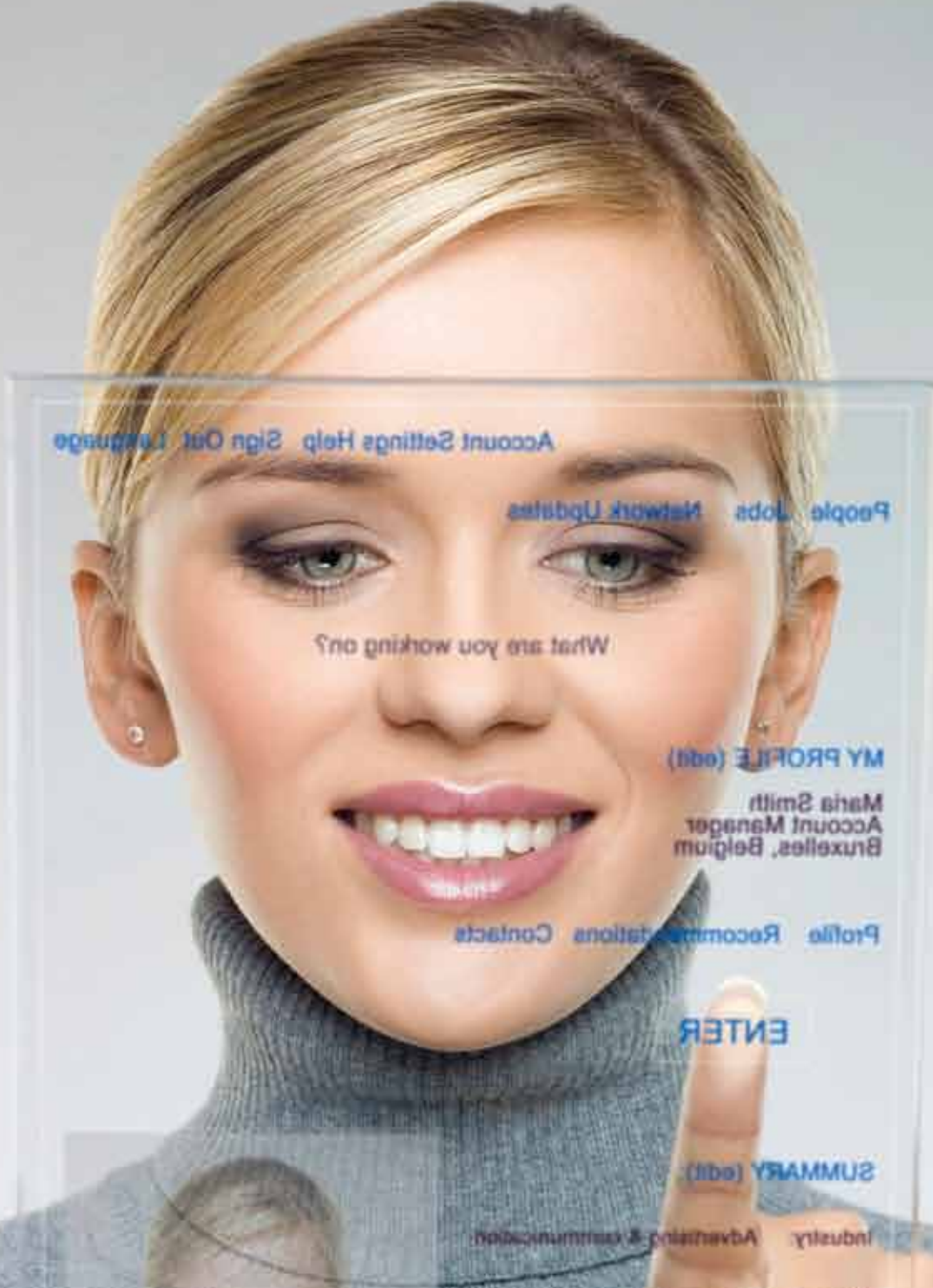


Enterprise Communications Security:

Closing a Serious Security Risk to Business Operations & Continuity



Communications Security By Design



Cybercriminals' New Target: Enterprise Communications

As more corporate data is transferred through corporate networks, cybercriminals are intensifying their attacks. New security threats are being developed as quickly as IT departments are adopting new technology, and corporate communications are coming under fire as never before. In just one year, from 2009 to 2010, attacks from hackers targeting enterprise unified communications (UC) servers increased by 50 percent. What's more, a full 25 percent of all hacking attacks in the open Internet are against voice and UC.

It's no longer enough to think of security as a series of discrete elements in your IT infrastructure. Security must lie at the core of your operations and be an integrated part of your IT and voice networks.

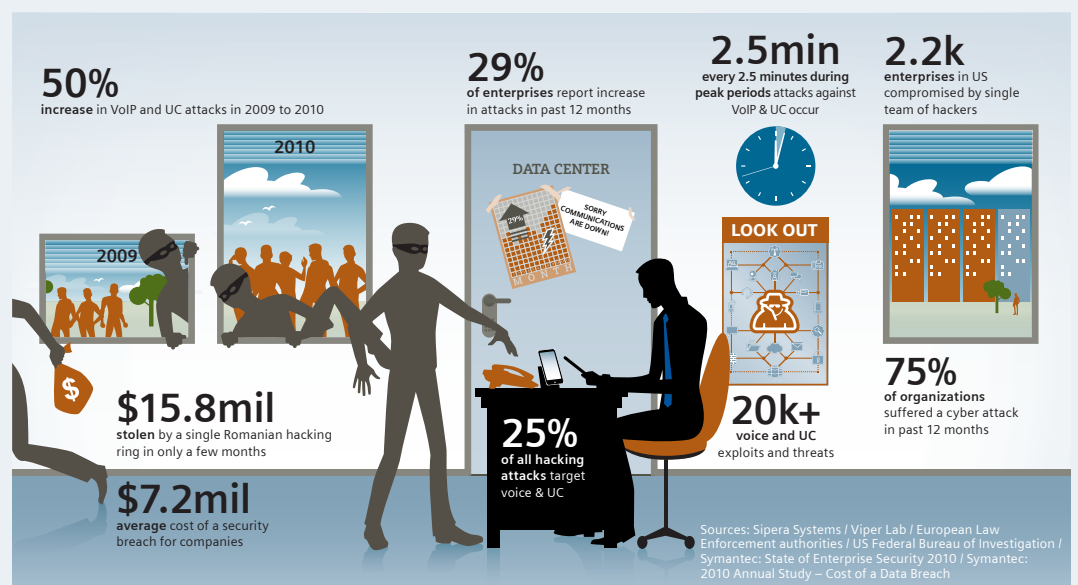
Megatrends Driving Secure Communications Issues

In today's dynamic corporate environment, end users are at the center of a series of megatrends driving the future of IT. Employees

are increasingly demanding the freedom to work anytime and anywhere on any device of their choosing. In addition to this mobility and flexibility, they want an increasingly large feature set, including social collaboration tools and easy-to-use interfaces.

Adding to the challenge, IT has its own set of priorities for supporting the network and communications infrastructure. At the top of the list is security, obviously. But a secure system is useless unless it operates with the highest possible degree of reliability. And given the need to quickly integrate new technologies and respond to new threats, flexibility is also vital for an organization to maintain its competitive edge.

Combined with today's multivendor environments, shortage of staff and a lack of internal expertise, these IT challenges highlight key issues faced by both IT and the end users as they attempt to establish secure communications. An experienced technology partner can help a business navigate the risks, and recommend products that offer advanced security features. Security services and solutions must support a multilayer approach to security.



Cybercriminals: Is your Enterprise Communications system their new target?



CASE STUDY

Enterprise Communications Security: A Growing Imperative

An outdated security infrastructure prompted a global financial services firm to seek help in developing and implementing a state-of-the-art security infrastructure across its 20 sites worldwide. Drawing on the products of one of its qualified third-party partners, Siemens Enterprise Communications delivered a new firewall, anti-virus and intrusion protection systems along with a centralized management interface. The tailored, updated infrastructure provides the security the firm needs, plus high availability and lower total cost of ownership.



Communications Security Designed and Engineered from the Start

At Siemens Enterprise Communications, we believe that *security must be built in, not bolted on*. In the past, applications were developed in silos, with a modular approach that led to integration problems when applied across systems. But today's enterprises need information to flow seamlessly across a variety of systems and applications to increase productivity. Because that raises fears of a system-wide security breach, Siemens Enterprise Communications incorporates fundamental security principles throughout the lifecycle of every product, solution and service, complying with internationally recognized standards.

Siemens Enterprise Communications' product, service and solution development and deployment are based upon our security philosophy: Our security focus begins at the moment a product, service or solution is conceptualized and continues through to implementation by our customers, and beyond. Each of our offerings integrates a robust set of security technologies, processes and features to ensure compliance with our clients' internal requirements. During the design phase of each of our solutions, we perform a comprehensive theoretical threat and risk analysis to assess real-world issues such as password management, as well as penetration tests during the testing phase to uncover and correct vulnerabilities.

In addition to extensive testing during product development, we ensure that our staff members are well versed in fundamental security procedures. We provide them with regular training on general security requirements. They also learn secure coding principles to guide their software development efforts.

Our highly organized security procedures also include the development and deployment of security checklists and hardening guidelines for effective, secure software implementation. To prepare for and mitigate emerging threats, we create Incident Response and Vulnerability Management plans.

Our Lifecycle Security Philosophy

Our security philosophy encompasses the entire lifecycle of products, solutions and services. From the moment we begin to develop a new application, appliance or service, we carefully consider and integrate established internal security standards, as well as internationally accepted standards and certifications, including ISO 2700x, BS 25999, IT Service Management (ITIL) and the National Institute for Standards & Technology (NIST) among others. Our integrated, comprehensive security approach means our clients can rest easy knowing that their communications are as secure as possible.

Global, Proven Communications Security Experience



Siemens Enterprise Communications has long been a global leader in corporate communications, providing solutions for organizations around the world. From small businesses needing a basic voice solution to connect employees in a single office to multinational enterprises with tens of thousands of employees needing a complete UC suite, we have helped businesses around the world secure and improve their communications infrastructure. Nobody knows communications security better.

- **Voice over IP (VoIP) and UC:** For more than five years, we have been at the forefront of VoIP and UC protection, securing clients against an increasing number of threats, including Denial of Service attacks, spam and fraud.
- **Identity and privacy:** With hackers increasingly seeking to compromise data and identity in all forms of communication, we have been including advanced security features in our products, services and solutions. Comprehensive identity and access management, authentication, authorization and encryption technologies ensure a higher level of security and prevent theft of data and identities.
- **Threat mitigation and data security:** While the struggles to secure corporate data have recently been making waves throughout the corporate world, we have more than 15 years of experience in providing IT security solutions, professional and managed security services.

Providing Real-Time Communications Security: Unique in the Market

To establish the best security possible, and ensure that we are up to date with current

events in the world of security, we partner with leading security companies, including Cisco, McAfee, Trend Micro, Check Point, Fortinet, Atos, Imprivata, TippingPoint and IronPort.

Siemens Enterprise Communications provides the most comprehensive set of products, solutions and services in the enterprise communications field. Together with Enterasys, Siemens Enterprise Communications is the only vendor providing a holistic approach to secure real-time communication by offering all of these features:

- **Multilayer UC security** defense comprising firewall, session border controllers, anti-virus, encryption and IP network services.
- **Identity management and privacy solutions** including provisioning, single sign-on, certificate management, electronic signatures and public key infrastructure.
- **Secure network solutions** from Enterasys automating network security configuration.
- **Security technology** integrated into communications solutions, built on an open platform to facilitate integration with a variety of technologies.
- **Combining UC and secure operations on a live network** to ensure availability and protection from threats in real time.

Confidence in the Cloud

As cloud computing becomes more and more popular, Siemens Enterprise Communications has been committed to expanding its expertise to support this rapidly growing deployment option. Our team of experienced professionals





Government Communications Security: A Fundamental Imperative

Following are examples of the standardizations, recommendations and rules for security released by governmental organizations that are guidance for Siemens Enterprise Communications:

- European Network and Information Security Agency (ENISA), the European Union's leading body chartered with securing information and networks across its member states;
- National Institute of Standards and Technology (NIST), the U.S. government's leading agency for cyber security, along with establishing industrial standards;
- Communications-Electronics Security Group (CESG), the United Kingdom's national authority for information security;
- Bundesamt für Sicherheit in der Informationstechnik (BSI), the agency in charge of managing computer and communication security for the German government.



has applied our fundamental security principles to our own cloud network, keeping in mind the primary goals of cloud operation. Our cloud support focuses on maintaining high availability, survivability in case of attack, proper governance of identity and maintaining data privacy.

As part of our commitment to security we maintain three Centers of Competence and a global network of security experts, who focus on combating current threats and providing state-of-the-art security services to our clients.

Open Standards for Compatibility

Today's data center often is a conglomeration of vendor technologies and varying platforms, and bringing in any new technology can cause compatibility issues for IT. To prevent downtime and improve efficiency, Siemens Enterprise Communications embraces open standards in our technology, allowing you to integrate multiple solutions from different vendors. We are a provider that extends this open philosophy to approved third-party security solutions, giving customers greater flexibility in configuring and maintaining their communications infrastructure.

What our customers have to say...

"Siemens Enterprise Communications has understood how to realize our demand for 'highest quality, security and targeted innovation' with a comprehensive security concept tailored to our needs."
— Dirk Fußwinkel/SportCast GmbH, Germany

"It has been integrated, without modifying the existing applications, a fingerprint-based SSO that allows access through only one authentication during the log-on."
— Jose Antonio Borreguero/UCI, Spain

"The open architecture and integration of Siemens Enterprise Communications and Enterasys' systems required minimal effort from our team. Their professional services experts succeeded in implementing an overarching management system in just one week, saving us a huge amount of work while at the same time making communication more secure."
— T. Giese/ESMT, Germany

Complete Communications Security Solutions

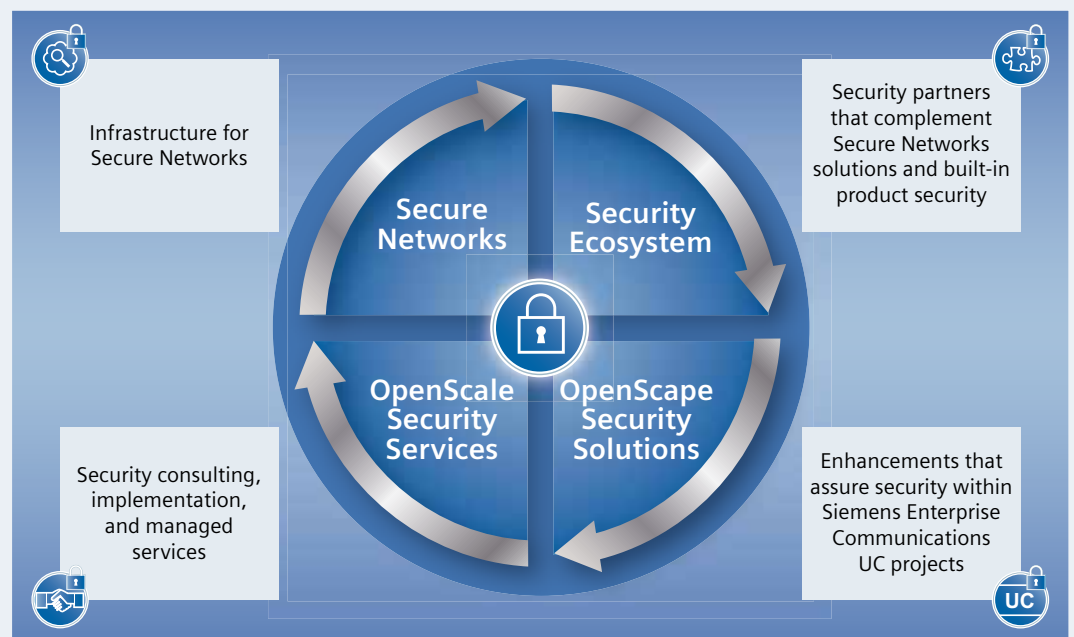
End-to-End Security Solutions Based on Open Standards

Budgetary and staffing issues prevent IT staff from having the time to integrate a large number of proprietary devices and applications to keep communications running smoothly. With so many vendors selling specialized products, a competent end-to-end solution can greatly improve efficiency in the data center. To help, the open platform of our individual solutions allows organizations to seamlessly incorporate our solutions into their multivendor infrastructure.

Siemens Enterprise Communications offers a complete set of solutions, products and services designed from the ground up with security in mind to keep your corporate communications running smoothly. With integrated security features at the foundational level of each product, peace of mind is a standard feature in everything we create.

Our wide range of advanced security offerings include the following to protect your communications infrastructure at every level.

- **Secure Networks:** Through our Enterasys solutions portfolio, we provide secure network infrastructure elements as well as advanced security applications, ensuring the confidentiality, integrity and availability of all your business-critical resources within the network.
- **Security Ecosystem:** We utilize expertise from the independent security solutions market to continually improve our standalone security solutions, improving protection for your IT infrastructure.
- **OpenScale Security Solutions:** Beyond the basics, our UC and VoIP products and solutions provide additional customer value, adding an extra layer of system-specific protection to your corporate communications.
- **OpenScale Security Services:** To keep everything running smoothly, we offer ongoing support ranging from individual tasks to complete outsourcing of security management.



Siemens Enterprise Communications offers everything you need for a secure and reliable VoIP and UC infrastructure.



CASE STUDY

Healthcare: Fulfilling Legal Requirements

Secure and highly available communications across a multisite healthcare provider is critical to its meeting strict privacy regulations. Siemens Enterprise Communications combined Enterasys and third-party products to develop, engineer and implement a complete security solution that included separation of laboratory, clinical and administrative facilities. The healthcare provider can now meet its legal and regulatory requirements with complete confidence.



Siemens Enterprise Communications is uniquely positioned to provide solutions ranging from social deployments, to on-premises infrastructure, to cloud systems. And with our extensive portfolio allowing organizations to automate security-related tasks such as certificate deployment, our solutions provide reduced cost of ownership and improved IT productivity.

Network Security—Secure Networks by Enterasys



Enterasys Security Information and Event Manager (SIEM): To simplify the complex area of technology management, Siemens Enterprise Communications is the only UC vendor to offer the Enterasys Security Information and Event Management solution. This versatile, open management system allows you to easily monitor and secure your communications system, improving the overall security of your corporate data and reducing the TCO of your communications infrastructure.

Enterasys Network Access Control (NAC): This innovative network access control solution allows administrators to give users the proper level of access to corporate information. With no need to install new switching hardware, and no endpoint software installation required, this

standards-based solution provides unparalleled control over authentication based on variables including user identity, time and location, and device type.

Enterasys Intrusion Prevention System (IPS): Detecting and neutralizing security threats in real time is vital for protecting corporate resources, and the Enterasys IPS provides a comprehensive set of security features that identify, isolate and eliminate in-line intrusions. Its advanced, multi-threaded architecture allows it to scale to meet the needs of even large enterprise networks.

Enterasys Network Management Suite (NMS): An efficient network is key in today's business operations, and the NMS gives administrators granular control over the entire network, down to individual users and applications. It allows IT to bypass time-consuming configuration tasks and manage the network through role-based access controls.

Security Ecosystem—Expertise in IT Security

Siemens Enterprise Communications has a broad expertise in the various fields of IT security. And to further supplement the security needs of our customers we work with a variety of leading security providers, with a variety of best-of-breed third-party security products and solutions.



CASE STUDY

Large Enterprise: Secure Communication & Data Infrastructure

A market steel producer in Latin America needed a comprehensive, highly secure and cost-effective communications solution to support its corporate growth while improving service quality and securing its data and networks. The company engaged Siemens Enterprise Communications to serve all its corporate communications and data needs via OpenScale Managed Services, which provides all hardware, software and services with multi-layered security. This outsourced approach helps the company save costs, ensure communications and data security, and stay focused on its core business of making steel.

Identity Management, User Provisioning:

We streamline the provisioning process, allowing administrators to add, update and remove users from a single source. We also provide additional identity management solutions including self-service tools and automated, rule-based access management.

Content Security: Our comprehensive content security offerings include anti-spam and URL filtering software, proactively protecting corporate resources from spyware. We provide security for email and Web environments, as well as anti-virus protection and solutions to prevent data loss.

Authentication and Authorization, PKI, Strong Authentication: As an integral part of a complete security system, validating user identity is vital. Our authentication solutions include certificate infrastructures, one-time password tokens, access control and single-sign-on solutions.

Perimeter Security, Unified Threat Management, Network Access Control:

Boosting the outer defenses of your network is one of the most important steps you can take in your security plan. We provide comprehensive security through firewalls and IPSec VPN, network intrusion detection and prevention, SSL VPN, encryption including load balancing and SSL offloading, and Session Border Controller.

OpenScale Security Solutions—VoIP and UC Security Portfolio

OpenScale Identity Lifecycle Assistant:

This solution can bridge IT and unified communications systems, maintaining up-to-date user information across the IT infrastructure. This versatile tool is easily integrated into a variety of applications, including SAP HR, Microsoft Windows Active Directory and other identity management systems.

OpenScale SignOn: Centralized single sign-on password management simplifies user access and reduces security risks. OpenScale SignOn gives administrators a centralized tool for securing access to corporate resources. It improves productivity by allowing users to more quickly access their accounts and prevents the need to require ever more complex passwords.

OpenScale Location and Identity Assurance:

With the complexity of today's enterprises, keeping user information up to date is a challenge. The OpenScale Location and Identity Assurance solution serves as a real-time database of asset information, allowing you to securely automate asset management, location services, IP phone monitoring and network provisioning.

OpenScale UC Firewall: One of the most fundamental security measures, a firewall helps keep your UC system safe from IP-based

attacks and unauthorized access from untrusted networks. Secure your communication and data infrastructure according to your security policy.

IP Network Services for UC: Our IP network services allow IT to more efficiently use resources, providing a cost-effective strategy that lowers the cost of operation and provides higher reliability.

Anti-virus for UC Servers: It's just as important to protect your UC environment as it is to keep other systems safe. Our anti-virus solution secures your entire UC infrastructure, keeping it safe from viruses and malware, all the while keeping licensing costs, as well as capital and operating expenses, at a minimum.

Certificate Services for UC: Efficient encryption for your UC system keeps operating costs low for maintaining certificates. Through our Certificate Services, you can enjoy the benefits of fully secure authentication and encryption throughout your systems.

OpenScale Session Border Controller: Designed specifically for use with OpenScale Voice, OpenScale Session Border Controller may be used independently or in conjunction with UC Firewall. It provides a single point of administration and allows you to connect multiple locations, securing VoIP and UC security at the enterprise network border.

OpenScale Security Services

In order to ensure complete protection of your communications infrastructure, our OpenScale Services provide protection throughout the lifecycle of the system: from the evaluation, the design and the implementation phase through the operation and the continuous improvement of the system, we offer comprehensive support to maximize your IT resources.

To further improve the TCO and efficiency of your communications system, we offer a series of OpenScale Security Services to enable you to keep your communications secure while focusing on your core business. From individual tasks to full outsourcing, we offer a full range of services including 24/7 availability, single point of contact for reporting, and multiple levels of SLAs to serve your needs across voice, UC and mobile network infrastructure.

Our OpenScale Security Services include:

- **OpenScale Professional Services:** Siemens Enterprise Communications provides end-to-end security within premise, hybrid, and private and public cloud deployments. Our security offerings can be tailored to combat threats and attacks across our solutions, network infrastructures, devices and clients—built-in from the ground up. They include ITIL-based, multi-vendor and globally available integration, implementation, operation and cloud services. The Security Professional



CASE STUDY

Small & Medium Business: Tailored Security Concept for TV Production

A sports TV producer required a secure, highly available IT infrastructure for its production processes and collaboration with partners. Siemens Enterprise Communications designed and implemented a new network and security infrastructure, virtualized its server landscape and developed Web applications to help it cooperate with partners. The solution combined Enterasys and third-party security products, plus OpenScale Security Solutions and OpenScale Security Services. The result? A redundant, secure, high-performance network and Web portal that has helped optimize processes and improve information flows across customers and partners.




Services Suites contain evaluation, design and integration services for all communication and security needs.

- **Professional Services Suite for Threat Mitigation and Data Security:** Offers assessments and readiness checks, design and integration, and training services.
- **Professional Services Suite for Identity and Privacy:** Offers services for design and integration, conceptual studies, and services for upgrade and migration as well as training and coaching services and certificate services.
- **Professional Services Suite for Virtualization Infrastructure:** Offers virtualization strategy analysis and consulting, virtualization assessments, design and integration services, and training services.
- **OpenScale Managed Services:** Delivers a complete range of multi-vendor, multi-technology managed services—from simplest tasks to complete outsourcing including operation of communication solutions in a secure manner and operation of security solutions.
 - **OpenScale Total Care:** Offers remote break/fix maintenance with flexible SLAs and options for on-site service, parts replacement and Moves, Adds and Changes (MAC) customizable for each site.
- **OpenScale Proactive Support:** Provides a proactive and cost-effective way to ensure the right resources are always available to handle the vital day-to-day activities to ensure a reliable and stable security infrastructure.
- **OpenScale Advanced Performance:** Offers complete visibility to performance parameters of your security infrastructure so you can respond to changes before they become problems.
- **OpenScale Patch Management:** Increases effectiveness of the patching process for voice infrastructure while cutting operational costs and reducing staff workloads.
- **OpenScale Security Device Management:** Offers out-task operation and monitoring of security infrastructure, while meeting compliance requirements and taking advantage of rare, skilled resources trained in both UC and security.
- **OpenScale Security Event Monitoring:** Offers real-time defense against threats and vulnerabilities within voice solution or network including comprehensive security status reporting.

OpenScale Security Services can be designed with your specific requirements in mind, to offer support where and when you need it. Features include 24-hour call desk services, a Web portal for user assistance and alarm monitoring for critical incidents. Our experts are ready to help.

Siemens Enterprise Communications: VoIP, unified communications and contact center solutions, networks infrastructure and security, private and public cloud deployments, devices and clients.



Siemens Enterprise Communications can provide end to end security within premise, hybrid, and private and public cloud deployments. Our security services offerings can be tailored to combat threats and attacks across our solutions, networks infrastructures, devices and clients—built in from the ground up.

Siemens Enterprise Communications solutions and services are open and comply with best practices.

Siemens Enterprise Communications is a global leader in communications security, with years of experience. Siemens Enterprise Communications is uniquely positioned to offer best-in-class, secure products, applications and services, allowing clients to focus on their core business.

Siemens Enterprise Communications is uniquely positioned to offer best-in-class, secure products, applications and services, allowing clients to focus on their core business.

Siemens Enterprise Communications

Keeping corporate information safe has never been more critical—or challenging—than in today’s global economy. As security threats become more pervasive and damages continue to mount, businesses need to respond with robust security solutions implemented throughout their network.

Security Is Part of Everything We Do

Siemens Enterprise Communications security solutions and services are based on an open architecture that complies with the most rigorous government standards. We can provide end-to-end security within premise, private and public cloud deployments or any hybrid of these. Our security offerings can be tailored to combat threats and attacks across our solutions, network infrastructures, devices and clients. Security is built-in from the start, not an afterthought.

At Siemens Enterprise Communications we are committed to establishing fundamental security practices in everything we do, from individual employee training to the global launch of complete communications infrastructure solutions. As a global leader in communications security, our years of experience uniquely position us to offer best-in-class, secure products, solutions and services, allowing our clients to focus on their core businesses.

We can secure all your enterprise communications with:

Proven security expertise

Our OpenSmart Security Best Practices are based on proven experience, exceeding governing body standards and security features designed into our products, services and solutions.

Comprehensive security portfolio

Siemens Enterprise Communications offers the industry’s most comprehensive Unified Communications security portfolio including products, services and solutions.

Best-of-breed security solutions

We employ a multi-vendor Security Ecosystem to deliver best-of-breed security solutions.

Global, multi-vendor security service

Our OpenScale Security Services include integration, implementation, operation and cloud services that are ITIL-based, multi-vendor and available globally.

Secure Cloud Services

OpenScape Cloud Services offer end-to-end security and physically secure and geographically redundant support centers.



Siemens Enterprise Communications:

Siemens Enterprise Communications is a premier provider of end-to-end enterprise communications solutions that use open, standards-based architectures to unify communications and business applications for a seamless collaboration experience. This award-winning "Open Communications" approach enables organizations to improve productivity and reduce costs through easy-to-deploy solutions that work within existing IT environments, delivering operational efficiencies. It is the foundation for the company's OpenPath commitment that enables customers to mitigate risk and cost-effectively adopt unified communications. This promise is underwritten through our OpenScale service portfolio, which includes intern anaged and outsource capability. Siemens Enterprise Communications is owned by a joint venture of The Gores Group and Siemens AG. The joint venture also encompasses Enterasys Networks, which provides network infrastructure and security systems, delivering a perfect basis for joint communications solutions.

The information provided in this brochure contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice. OpenScape, OpenStage and HiPath are registered trademarks of Siemens Enterprise Communications GmbH & Co. KG. All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

© 2011 Siemens Enterprise Communications GmbH & Co. KG.

Status (07/2011)

Siemens Enterprise Communications GmbH & Co. KG is a Trademark Licensee of Siemens AG.