

# Your world is changing...

## ...should your security be built-in?

Siemens Enterprise Communications

2011

# 1. Executive summary

## Your world is changing...

Today we're witnessing a major shift in social and technology trends that are set to make a big impact on your business communications landscape.

The forces of consumerization, social communication and mobility are colliding with advances in security and all kinds of flexible deployment models in a way that will change forever how businesses access information, collaborate, and build customer relationships.

We call this revolution the Communications Tipping Point. And it's driving organizations to embrace a new era of cloud communications.

## Cloud is compelling

The benefits of the cloud are clear. Just for starters, cloud offers lower upfront costs, a reduced need for technical expertise, and overall business simplification. Plus businesses can rapidly scale up and down, create virtual organizations without geographic boundaries or physical data centers, and deliver all the communication and collaboration services their users want.

But by liberating their communications from the wired world, enterprises large and small reap other rewards such as new and powerful advanced communications capabilities.

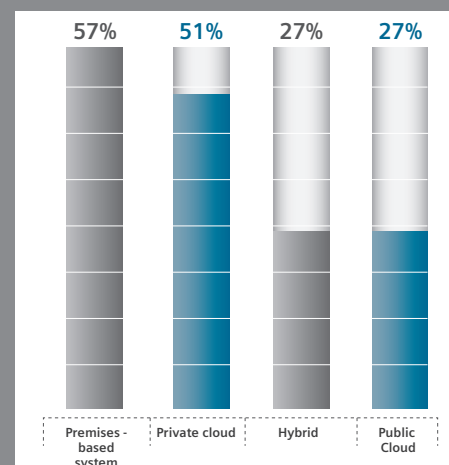
Ultimately, that means their employees can connect to their chosen communications application – whether it's voice, web conferencing, or instant messaging - from almost any device on any network, anywhere. Plus, web collaboration across and beyond the enterprise becomes a cinch.

Quite simply, the cloud gives organizations improved communications efficiency, accessibility and control, alongside truly impressive flexibility, scalability and mobility.

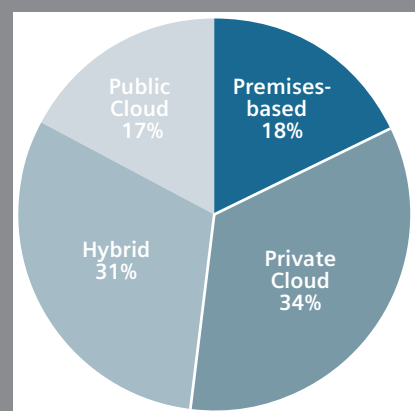
## A new perspective

Indeed CIOs believe the Communications Tipping Point to be so influential that in just two years time Private Cloud and Hybrid operating models will have eclipsed premises-only solutions as the dominant models.

Today premises-based models dominate<sup>1</sup>



In two years cloud and hybrid models will dominate<sup>1</sup>



But in this brave new hyper-connected world, there's a new challenge to consider; security. And the very first step in addressing this challenge is asking, and then answering the question, is your security built in, or bolted on?

1. Loudhouse Research, September, 2011.

## 2. A shifting security landscape

### Open to attack?

As we've seen, from the phenomenon of social media that's taken us by storm to the seamless mobility and flexible deployment options that give everyone choice in how, when and where we communicate, the Communications Tipping Point is triggering a seismic shift in the way organizations operate today.

And for the enterprise, that means taking stock of the potential security challenges this raises.

Because alongside all the good stuff – seamless mobility, social collaboration, and smart devices that give you instant access to any application or data source - the open nature of our connected world means your enterprise is at risk of compromise.

As the No Jitter Blog for Connected Enterprises so succinctly puts it; "The unpleasant truth is that the greater the number of communications data flows – voice, IM, text, email, video – the more potential entry points for an attacker. And with a growing percentage of that traffic relying on wireless device and network facilities, exposure increases even more."

The explosive year-on-year growth in unstructured data (79%), mobility (63%) and Web 2.0 usage (52%) between 2009 and 2010 alone is testament to the rising threat levels. And the reality is that these trends are only set to escalate.

### What's the risk?

In today's highly connected world, cyber-breach has moved from the realms of science fiction to an everyday reality. This year alone, 29% of enterprises reported an increase in attacks while 79% of organizations confirm they've suffered a cyber attack in the past 12 months.

---

### What's the cost?

**\$7.2 million represents the average company cost of a security breach**

**In 2010 a Romanian hacking team stole \$15.8 million in just a few months**

**2,200 US enterprises in the US were compromised by a single team of hackers**

---

With hackers becoming ever more sophisticated and daring, a closer look reveals how the connected enterprise is becoming more vulnerable.

As we've seen, the increase in seamless mobility multiplies the number of potential entry points to the enterprise. Which means data stored on the corporate network is at risk because it's more accessible than ever, thanks to cross network hand-offs, the multiplicity of access points, and the number of external collaboration participants (mobile and home works, partners, suppliers and customers) operating within the enterprise ecosystem.

The growing use of employee-owned 'smart' devices for work-based activities now represents a serious security headache for CIOs. As well as making it challenging to maintain a centralized security policy, the escalation of attacks on smartphone operating systems plus downloads from apps stores by workers all represent potential unseen entry channels for viruses and malware.

The reality is that the use of mobile phones, laptops, Web 2.0 applications, video and other social media at home, at work and on the road, creates an ever more complex environment to safeguard.

## Security myths and realities

The enterprise security battle ground has changed, and these days it's no longer just about protecting data. Because as voice and unified communications move 'outside' the firewall, they're also vulnerable to cyber attack.

---

### A growing threat

- 50% increase in VoIP and UC attacks in 2009-2010
- 25% of all hacking attacks target voice and UC
- Attacks on VoIP and UC occur every 2.5 minutes in peak periods

---

As VoIP and UC systems peer with external networks and direct voice-to-voice services, organizations open a new potential vector of attack on underlying network elements. And that puts your enterprise at risk.

Through eavesdropping, hackers can obtain names, passwords and phone numbers, giving them control over voicemail, call plans, call forwarding and billing information, or access to business data. And just like computers, VoIP softphones are vulnerable to worms, viruses and malware, while denial-of-service attacks can degrade voice services, halt call processing, or provide cover for attackers to redirect or hijack calls.

Assessing risk potential across the entire business is a critical first step. But getting a grip on what's vulnerable – and why – can be a daunting task. And that's because the security landscape is ever changing.

Thanks to the effects of the economy, geo-politics, cyber war and cyber terrorism, in today's world any organization is a potential target. The primary external threats and risks – toll fraud, eavesdropping, phishing, vishing (ID attacks on VoIP traffic), and SPIT - are usually financially motivated. But that's before you take internal sabotage risk factors into account.

For organizations this means stepping back and reassessing what security really means. Because assuring the confidentiality, integrity and availability of your enterprise now means security must be built-in – not bolted on.

### The web conferencing risk profile

Web conferencing extends collaboration to anyone with an Internet connection – allowing participants to chat, share concepts, share screens, transfer files, and access virtual whiteboards. But substituting Web conferencing sessions for in-person meetings can pose a risk of content seeping beyond an enterprise's four walls.

- If a Web conferencing server is infiltrated the streams of communication are at risk of exposure to others who have access to this hub environment.
- If end-user systems (operating system or Web browser) or the client software facilitating Web conferencing on participant devices are compromised by spyware or remotely controlled botnet programs, there's a risk sensitive information can be harvested.
- Unauthorized participants may receive content not intended for them, while other participants may not have accounted for the risk their surroundings may have on content exposure.
- Non-presenting participants can contribute to the risk of exposing content by volunteering content through in-session instant messaging and audio conferencing.
- Any omission of popular collaboration modes – such as cloud-based file sharing services – within an enterprise-grade secure Web collaboration tool can indirectly contribute to a company's overall content exposure risk.

# 3. Building security from the ground up

New attacks, aided by the use of cloud computing, mobility, social media and inadequate IT security concepts mean enterprises need to embrace new and highly integrated IT security strategies.

The key areas of emphasis for security – authentication, identity and auditing – haven't changed. But when it comes to your enterprise communications – and ultimately your data – it pays to expect that security is built into your voice and unified communications from the ground up, regardless of whether your cloud deployment is private, public or hybrid.

## So, should I trust the cloud?

That depends on if you use our OpenScope Secure Cloud Services.

If you do, there is absolutely no problem. Because OpenScope Secure Cloud is a fully secure, robust enterprise-class communications infrastructure with disaster recovery built-in as standard.

And every aspect of security is taken care of, from in-built technical resilience through to the application of best practices and standards that assure the integrity of your communications and data from the device, to the network, to the data center – and everywhere in between.

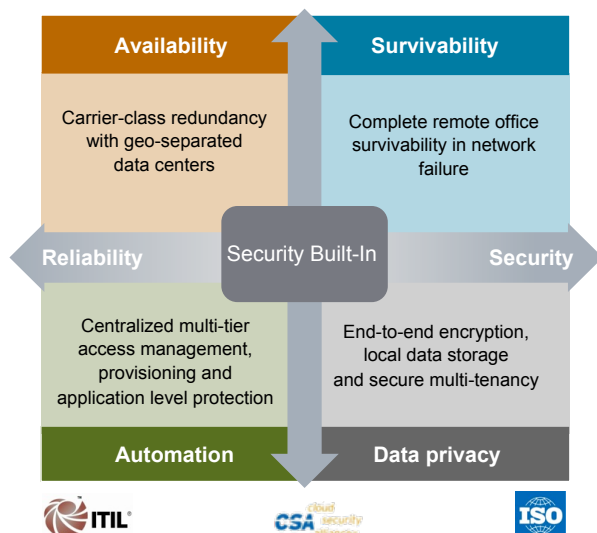
Our services are hosted in world-class redundant and geographically separated data centers that are independently certified at the highest industry standard (Tier 4 TIA-942). What's more, the OpenScope Secure Cloud Services network is permanent monitored, managed and controlled 24x7.

We also employ a host of security controls such as firewalls and Session Border Controllers to protect against virtual attack, while voice-signaling and payload encryption prevents eavesdropping dropping on live phone calls. And we routinely 'penetration test' all our services to ensure you are completely protected.

## Built-in – not bolted on

At Siemens Enterprise Communications we take security seriously. It's why we've built end-to-end security and reliability into our cloud network and our voice and data products, solutions and services, and why we've left no aspect to chance.

As IT security experts you'll find we cover all the bases, from identity management and user provisioning to securing content, and authentication and network access controls that prevent unauthorized access from untrusted networks. And at every stage of the game, from initial coding to the vigorous penetration testing we undertake during development, all our services are designed with security in mind.



## Security myths and realities

Our built-in end-to-end security approach covers all the bases. From protecting end-user access points to the encrypted storage and transmission of data, our best of breed security solutions deliver the peace of mind you need in a constantly evolving threat landscape.

What's more, our world-class Professional and Managed Services teams are on hand to ensure that whatever your deployment model, your enterprise cloud communications are implemented and maintained in a manner that ensures they are always available, and always secure.

## The Siemens Enterprise Communications approach

Working together with Enterasys, a Siemens Enterprise Communications Company, we have the most comprehensive security portfolio available in the industry today. So when it comes to keeping your network, UC and VoIP communications secure, we've got it covered.

But that's not all. When it comes to the tricky issue of making sure only the right people gain access to your communications infrastructure, our services deliver built-in access controls so you can extend your UC applications to any end-point in any location and over any network – and enable enterprise offices, distributed call centers, mobile UC on smartphones, and collaboration environments with partners.

# 4. Don't just take our word for it

Built on the award-winning OpenScape UC Suite and OpenScape Voice, our cloud services deliver an extensive portfolio of unified communications and collaboration capabilities to enterprises via the cloud, backed-up by the most advanced security and resiliency techniques available in the industry today.

With over a decade of experience in VoIP and UC we've implemented many hundreds of identity and security solutions, while our automated networks were the first to integrate security into switching and management. And to deliver on our 'open' cloud vision we've invested in the technical expertise it takes to integrate multiple technologies from a variety of vendors.

And by offering a comprehensive portfolio of wired and wireless network infrastructure and security solutions from Enterasys, we can help organizations to drive down IT costs while improving business productivity and efficiency through a unique combination of automation, visibility and control capabilities.

Our proven expertise in high security areas like public sector and defense means customers around the globe rely on us for their voice and data services and solutions.



EUROPEAN  
COMMISSION



We continually strive to assure compliance with standardizations, recommendations and rules for security released by governmental organizations; from the European Network and Information Security Agency (ENISA), and the National Institute of Standards and Technology (NIST), through to the UK government's national authority for information security (CESG) and the German Bundesamt für Sicherheit in der Informationstechnik (BSI).

## Security know-how

Our long standing pedigree in security innovation and leadership means you can depend on us for the professional expertise you need to protect your enterprise environment.

By tapping into our Centers of Competence - Identity & Access Management and Security & Networks - and our Security Network Operations Center you'll gain the essential know-how to evaluate your security capabilities, mitigate threat, and ensure you achieve the confidential real-time communication you need.

---

## Proven security expertise

### ■ VoIP security

Over a decade experience in VoIP and UC

### ■ Identity and privacy

Several hundred implemented identity and privacy security solutions

### ■ Threat mitigation and data security

15+ years experience in threat mitigation and data security solutions

### ■ Automated networks

Enterasys first to integrate security in switching and management

### ■ High security areas

Proven expertise in high security areas (Public/Military Sector)

### ■ Open approach

Experience and technical expertise needed to integrate multiple technologies from a variety of vendors

### ■ Comprehensive security solutions

Based upon world's leading security vendors and standards-based communications solutions

---

# 5. Next steps

At Siemens Enterprise Communications we recognize no two businesses are alike. Which is why we're the only vendor to provide the complete range of Voice, UCC and Contact Center solutions across premise, private cloud, hybrid and public cloud services based on our open, next-generation software-based architecture. Uniquely, this enables us to make a totally objective recommendation on what's right for your business.

When it comes to protecting your enterprise communications, we understand the potential vulnerabilities and challenges you face. And that includes securing the IT infrastructure for edge-to-core protection right, through to the assurance of flexible security solutions and services that deliver state-of-the-art security capabilities and compliance features.

## **The Siemens Enterprise Communications security advantage:**

**1. Proven security expertise:** our OpenSmart Security Best Practices are based on proven experience, and exceed governing body standards.

**2. Comprehensive security portfolio:** we offer the industry's most comprehensive Unified Communications security portfolio that includes products, services and solutions.

**3. Best-of-breed security solutions:** we employ a multi-vendor Security Ecosystem to deliver best-of-breed security solutions.

**4. Global, multi-vendor security service:** our OpenScale Security Services include integration, implementation, operation and cloud services which are ITIL-based, multi-vendor and available globally.

**5. Secure Cloud Services:** our OpenScape Cloud Services offer end-to-end security and physically secure and geographically redundant support centers.

---

**Find out more about our built-in Security Portfolio.**

**[www.siemens-enterprise.com/security](http://www.siemens-enterprise.com/security)**

---

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 international, managed 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.

© Siemens Enterprise Communications GmbH & Co. KG 2011.

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

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.