Maximizing Security in Enterprise Unified Communications

This guide discusses the importance of security in enterprise communications, Unify’s unique approach to communications security, examples of Unify security solutions, and key insights for IT communications professionals.
Our identity management solution from Unify has significantly increased the data quality and security in our IT systems as well as greatly simplified administrative IT processes.

Volker Bertermann, IT-Service and Identity Management, Deutsche Rentenversicherung NOW IT GmbH
The Changing Workplace and the Impact to Enterprise Communications

We are in the midst of entering a new era where security is at the forefront of business survival.

**The Impact of the Cloud**
Digital disruption is well underway as the economics of on-demand computing capacity and the shifting of capital expense risk are driving more businesses to the cloud. On-demand applications and easy-to-deploy communications are driving adoption and usage, but with this opportunity comes new challenges in terms of security risks.

**The Impact of Cyber Threats**
Cyber threats are becoming more malicious as the modern security landscape continues to evolve beyond the borders of enterprise firewalls to a “connected anywhere” world of mobile devices. As more information is stored in the cloud and transmitted between mobile devices, cyber criminals have increased their efforts to compromise secured data for financial gain.
Security threats are growing by 20% per year. As a result, by 2020, “25% of global enterprises will engage the services of a ‘cyberware mercenary’ organization” to combat the threats. (source: Gartner Research)

Cybercrime costs are $345 billion per year.²

**The Impact of Mobility**

Mobile users are connecting to their confidential information directly through Virtual Private Networks (VPN), or indirectly via the Internet and across a multitude of networks (many non-secure networks: WLAN, 3G/4G, UMTS), and from a variety of devices. Applications and identities are being used inside and outside the boundaries of our secure workplace infrastructures. Private and professional boundaries have become blurred, placing confidentiality and privacy at risk.

“The challenge companies face is how to enable security ‘in a way that doesn’t freak employees out’ but still gives information technology departments enough control,” says Cheryl Tang, senior manager for enterprise mobility at Symantec. It’s a real concern. Up to 51% of employees said they would go around any policy that restricted their use of their own devices or use of cloud storage, according to a 2014 Fortinet security survey.

Internet security company Webroot found that only 42% of companies required employees to have a security app installed, and only 19% required mandated security supplied by the company.³

While no organization can ever be fully protected against security breaches, managing security risk is essential for any organization seeking to leverage technology for increasing growth and customer engagement.

**The Importance of Security in Enterprise Communications**

The world of unified communications means that today’s “voice” solutions include connections to voice calls and conferences, messages, files shared, screen-sharing, remote PC access, mobile devices, user-selected devices, business apps, your data centers and networks and much more. There are many components from many manufacturers involved and this can introduce security risks.

Security breaches and cyber attacks put your data and your customers’ data at risk, damages customer satisfaction, lowers productivity, and impacts your financial stability from downtime to recovery. The financial and reputational costs of a security breach can be extraordinary.

---

¹ Atos “Ready for anything – Business driven security for the digital era
² http://www.usatoday.com/story/tech/2014/08/26/byod-bring-your-own-device/14393635/
Whether they know it or not, many enterprise businesses are already exposed to network security threats. In a September 2014 Network World article entitled *Network Security Challenges in the Enterprise*, Jon Oltsik notes the following startling statistics as it relates to enterprise security:

- 39% of organizations’ IT initiatives are being adopted without the proper network security oversight or controls in place.
- 31% of organizations’ network security policies and controls are not cohesive as they must be implemented across many different security and networking technologies.
- 28% of organizations are challenged by too many overlapping security controls and processes resulting in redundancy and wasted resources.
- 27% of organizations’ security staff is too busy responding to alerts/events and not enough time with training, planning, or network security strategy.
- 25% of organizations have a problematic shortage of IT security skills.
- 26% of organizations are challenged by security policies that are too complex and can’t be enforced with the current network security processes and controls.
The 2015 Cost of Data Breach Study: Global Analysis by the Ponemon Institute reveals the business impact of not having the appropriate security policies, controls and products in place:

- $3.79 million is the average total cost of a data breach globally.
- $6.53 million is the total average organizational cost of a data breach in the U.S. in 2015.
- $170 is the average cost per lost or stolen record caused by a malicious or criminal breach.
- 23% is the increase in total cost of data breach since 2013.
- $1.57 million is the total average cost of lost business in 2015.
- 47% of all breaches were caused by malicious or criminal attacks (the highest cause).
- 256 days is the average it takes to discover a malicious attack.

Today’s enterprise businesses are no longer asking whether they will be breached – but when they will be breached. This has increased the need to select technology partners and products that can help protect against malicious intrusions.

Security by Design

With over 100 years of experience, Unify approaches security seriously. We believe that real security is a process that begins at product inception and extends throughout your lifecycle experience.

Unify’s Approach to Security: Built-in, Not Bolted-on

Our process approach to security is what separates us from other unified communications providers as we focus on the five critical areas impacting enterprise communications security:

1. Adherence to strict baseline security policies
2. Secure application design and development and vulnerability intelligence processes
3. Deep security expertise and consulting experience
4. Partnerships with leading security firms
5. Proactive involvement with emerging security standards, technologies and vulnerabilities

Additionally, our security experts are available to consult, design, monitor, and even help manage our customers’ communications solutions. To understand how we deliver true mission-critical security, we need to take a closer look at each of the individual security measures that are part of our unique security approach. Omitting any one of these components can expose an enterprise to communications security risk.

“Unify have supported our University Hospital with a future-proof solution to our communication infrastructure. They have met the high requirements of our University Hospital in the areas of: information sharing, collaboration, security, flexibility and efficiency of support - for the benefit of patients, staff and students alike.”

Universitätsklinikum Halle (Saale)
Adherence to Strict Baseline Security Policies

Baseline security starts at the very beginning of each product’s lifecycle to ensure secure development, test, release, and then the sustaining of the product. This includes secure coding based on security standards such as OWASP, static and dynamic code analysis, continuous vulnerability scanning, default hardening based on CIS (Center for Internet Security) Benchmarks, implementation of password policies, use of standardized and best-practice crypto-algorithms. We design and build our products so that they can be installed, operated and maintained securely, using our thorough Baseline Security Policy and according to each customer’s specific IT security guidelines and policies. As we deploy a communications solution we also engage our Service team so they can fully understand and support the security measures we’ve implemented for the customer’s environment.

Secure Product Development and Vulnerability Intelligence Processes

Our product development process integrates security requirements throughout the entire product lifecycle to ensure secure development, test, release and sustainability of our products (e.g. secure coding based on security standards such as OWASP, static and dynamic code analysis, continuous vulnerability scanning, default hardening based on CIS Benchmarks, implementation of password policies, use of standardized and best-practice crypto-algorithms etc.).

We use AES-128bit encryption algorithms to protect the confidentiality of digital data stored or transmitted via the Internet or other networks. This is vital in securing IT and communications systems, and provides confidentiality, authentication, integrity and non-repudiation.

We perform two comprehensive Security Assessments:

1. **Theoretical Security Assessment:** a threat and risk analysis during product design. It evaluates the product’s security architecture and identifies weaknesses and associated risks. This important threat and risk analysis evaluates the product’s security architecture and identifies weaknesses and associated risks. During the system test phase, we perform a Practical Security Assessment that includes penetration tests that evaluate the product’s realization (implementation/coding) and a typical installation to identify vulnerabilities.

2. **Practical Security Assessment:** a penetration test during the system test phase that is performed in-house or by 3rd party penetration test companies:
   - Miercom (US)
   - SySS, n.runs, P3 Consulting, Detack (Germany)
   - Search-Lab (Hungary)

Our Security Checklists are used to document how we’ve adapted the Unify systems’ default settings to our customers’ security policies. Our Proactive Vulnerability Management process ensures that each Unify product’s security levels are maintained or improved, and any security weaknesses are fixed until the very end of the product’s software support.
Our Vulnerability Intelligence Process continuously monitors security vulnerabilities, analyzes their impact to Unify products, and informs our customers and the public via Security Advisories. We follow the industry standards ISO/IEC 30111 and 29147 for vulnerability handling and disclosures. When a vulnerability is reported and disclosed, our first step is to determine which Unify products are potentially affected, which ones are confirmed affected, and which ones have the highest risk. There are different solutions to each product, based on the level of risk involved. For example, a security advisory is immediately published for high risk products. For Windows applications such as OpenScape Xpression and Contact Center, an immediate patch of the Windows operating system is implemented. For OpenStage Xpert, our Trading solution, we publish mitigation/hardening measures such as firewall settings, and an updated security advisory, as soon as the final correction is available. After the solution is delivered, we collect feedback from users and make the necessary updates if needed.

Our Proactive Patch Management process helps protect against vulnerabilities, increase stability and availability, and simplify administration and maintenance to ensure security of the overall environment. We do this by publishing release notes and information about current vulnerabilities, and by planning, supplying, and implementing software fixes and patches. With more than twenty years of experience in performing remote services on thousands of systems worldwide,
we are sensitive to the importance of security when accessing our customers’ systems for remote service. The servers in our global customer support centers are fully protected using state-of-the-art technology. This prevents intrusions of infection by worms, viruses, Trojans, or other attacks. Local virus checks are performed continuously on our servers, which reduces the likelihood that a virus infection be transmitted to your system from ours.

Deep Security Expertise and Consulting Services
We leverage decades of deep in-house security expertise, including Centers of Competency and a Global Trust Office, to ensure our customer communications solutions reflect the latest security best practices.

This includes:

• Analyzing each customer’s unique security needs
• Specifying and designing tailored security solutions, policies and processes
• Integrating security solutions into each customer’s existing network and operations with minimal disruption
• Augmenting our customer security policies
• Security audit workshops delivered by our professional security consultants
• Deep understanding of both legacy and emerging technologies for keeping our customers’ network, data, and communications safe

Qualify of Industry Partners
To ensure you benefit from the most comprehensive coverage, we partner with some of the most trusted security firms in the industry. Together, we help each customer define and implement tailored communications security strategies that best fit their organization’s resources, size and budget.

Our partners include:

• Trend Micro
• Fortinet
• Atos
• Extreme Networks

Proactive Monitoring of Emerging Security Standards, Technology, and Vulnerabilities
For the past three decades, we’ve led an evolution for IT security by staying ahead of the curve in understanding what’s coming in communications security. We stay on top of the constant changes in security standards and requirements and of the latest security technologies. Most importantly, we’ve helped shape security and compliance strategies in government, defense, finance, and healthcare.

We actively participate in emerging and new industry technology standards groups such as the IETF, and have memberships with security standards organizations such as Cloud Security Alliance, CIS Benchmarks Division, IMTC, Fedramp, JiTC, and ISO 27001.
Unify Security Solutions for Enterprise Communications

We recognize that every customer has individual requirements as it relates to security. That is why we have designed and developed a wide range of security solutions to meet the needs of enterprises businesses in many different industries. We deliver mission-critical communications security to multiple industries including manufacturing, healthcare, financial services, public sector, and more.

**OpenScape Solutions**

Our OpenScape Voice, OpenScape Branch, and OpenScape Session Border Controller solutions were tested against 10,800,231 advanced cyber attacks and protocol mutations, and all breaches were successfully repelled, earning us the highly respected and recognized Miercom Secure Certification. These superior results reflect our commitment to building solutions to the highest security standards.

<table>
<thead>
<tr>
<th>Solution Highlight</th>
<th>Business Use</th>
<th>How Unify Delivers Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OpenScape Session Border Controller</strong></td>
<td>Protection for the SIP trunking to your network, remote offices and your home workers</td>
<td><strong>OpenScape Session Border Controller</strong> is our next generation security solution for unified communications that enables VoIP networks to extend SIP-based communication and applications beyond your enterprise network boundaries. It provides three key functions: 1) to secure termination of SIP-based trunking from a service provider, 2) to secure voice communications for remote workers and 3) it connects remote branch offices as part of a distributed OpenScape Voice deployment.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution Highlight</th>
<th>Business Use</th>
<th>How Unify Delivers Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OpenScape Web Collaboration</strong></td>
<td>Online confidential meetings, Secure file sharing (internal or external)</td>
<td>OpenScape Web Collaboration’s Secure Connect Service (SCS) is our unique way of securing all your web conferencing experiences. SCS uses multiple layers of security including data-encryption between clients and Web Collaboration servers, secure end to end Data Control signaling between Web Collaboration clients, and encrypted storage and transfer of Web Collaboration “payload”. This makes it impossible to decrypt content at the OpenScape Web Collaboration server, making it the ideal collaboration solution. It also offers password protected collaboration sessions, the ability to see the entire participant list, expel anonymous participants, and lock the session. All sessions are 256-bit AES encrypted and cannot be decrypted on the server. All collaboration sessions are temporary, leaving no residual data and do not make any entries in the registry.</td>
</tr>
</tbody>
</table>
### Solution Highlight: OpenScape UC Firewall

<table>
<thead>
<tr>
<th>Business Use</th>
<th>How Unify Delivers Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Unified Communications Within Data Centers or VoIP Environments</td>
<td>OpenScape UC Firewall prevents IP-based attacks and unauthorized access from untrusted networks. This improves security and reliability by providing intrusion detecting optimized for VoIP, as well as outages caused by attacks on application servers. It provides the highest level of security assurance (EAL4+).</td>
</tr>
</tbody>
</table>

### Solution Highlight: Circuit

<table>
<thead>
<tr>
<th>Business Use</th>
<th>How Unify Delivers Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Cloud-based Communications and Collaboration</td>
<td>We've deployed a security management framework according to ISO 27001. This means that all your conversations with other Circuit users are encrypted and secure. Multiple layers of security protect access to Circuit. This includes firewalls, complemented by built-in security to the Circuit application which protects information, and restricts access to intruders. Our data centers are protected against unauthorized access and are only accessible to authorized individuals. Access is monitored via smart cards and biometric controls at all physical access points. Video cameras are employed to deter and detect unauthorized access. Audits and re-validation of authorized individuals are performed quarterly. Our data centers maintain security management systems that are independently reviewed by independent auditors. Access to data center systems is monitored and logged and regularly reviewed.</td>
</tr>
</tbody>
</table>

### Solution Highlight: Managed Security

<table>
<thead>
<tr>
<th>Business Use</th>
<th>How Unify Delivers Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outsourced Management of Security to Reduce Costs While Improving Compliance</td>
<td>We offload the IT burden of ongoing security management. In a predictive manner, security patches for the security components are rolled out remotely by our security professionals in order to keep the device on its most-current security level. These security components are monitored 24x7 to ensure that they are up &amp; running to protect the customer's IT infrastructure. Optionally backup and recovery services are available to guarantee a required restoration of a security device as fast as possible. A dedicated Service Level Manager performs a continuous improvement process and delivers security-relevant reports for audit and compliance.</td>
</tr>
</tbody>
</table>
Our OpenScape solutions were tested against 10,800,231 cyber threats and repelled them all.
Key Insights for IT Communications Professionals

For IT communications professionals, there are several themes to consider when selecting a unified communications partner that can protect the security of your sensitive communications and data:

1. No two enterprise businesses are identical, so neither are their security needs. Ensure your communications partner can tailor a solution that fits the security needs of your enterprise.

2. IT and communications systems are not 100% secure, however, proactive design of security into communications solutions and ongoing proactive maintenance are keys to bringing the odds into your favor.

3. Unify offers a mature software development lifecycle with security built-in, not bolted-on. This means technology stability and security following ISO and CIS standards. Is your current vendor applying the same level of investment and process rigor to their security offerings?

4. Unify manages software security vulnerabilities proactively and openly as a true business partner. Challenge your communications vendors to articulate their processes.

5. Proactive measures are always more effective than reactive measures when it comes to communications security. From product concept, to product development, to ongoing maintenance -- security designed into a solution offers the best protection against malicious breaches and cybercrime. Challenge your communications vendor to articulate how they approach security.

If you are interesting in learning more about enterprise security in Unified Communications or how Unify can help support your business growth, contact a Unify solutions consultant or visit www.unify.com for more information.