

# **Best Security Practices for a Converged Environment**



**April 2005**

## 1.0 Introduction

With the Introduction of IP Telephony a few years ago, a small number of leading edge IT organizations began to deploy a converged network to support myriad traffic types, including voice, data, and video. Today, driven by desire to reduce transmission costs, increase operational efficiencies, and enable new integrated applications, IT organizations either already have, or are now starting to implement a converged network.

When the movement to adopt converged networks began, the conventional wisdom in the industry was that voice should be treated as just another application traversing over an IP network. While there is some validity to that argument, it ignores some of the unique characteristics associated with deploying Voice over IP (VoIP). For example, a VoIP deployment will result in a dramatic increase in the number and types of endpoints that access enterprise information and applications, and hence significantly increase the security vulnerabilities.

This fact is now widely recognized. For example, late last year Steven Taylor conducted a survey<sup>1</sup> of over 500 networking professionals. Nearly 50% of survey respondents indicated that security concerns were the number one impediment to deploying VoIP to their organizations.

While IT organizations are still in the process of fully deploying a converged network, some leading edge IT organizations is now beginning to deploy converged communications. *Converged communications* refers to two related concepts. The first concept is the integration of business applications such as SAP and Siebel, with Business Communications Applications, such as internet protocol telephony, conferencing, and unified messaging. The second key concept is the embedding of these integrated applications into a company's key business processes, such as supply chain management, and customer relationship management.

The embedding of integrated applications into a company's key business processes does not mitigate the need for security - it increases the need. As a result, whether an IT organization is deploying a converged network, converged communications, or a combination of both, it is imperative that organizations take advantage of industry experience in building security best practices all the way from policy development, through architecture and design, to installation and ongoing management. The goal of this white paper is to provide some general principles and guidelines for such best practice.

---

<sup>1</sup> Steven Taylor, "2004 VoIP State of the Market Report," October 2004, Distributed Networking Associates, Inc.

## 2.0 The Challenges of Convergence

A key aspect of converged communications is the focus placed on capabilities and control specifically for end users. Converged communications enables users to be connected to enterprise information resources from anywhere, according to their individual preferences and availability. Converged communications also enables users to employ whatever mode (i.e., wired or wireless, speech or text/display) and whatever devices are most convenient to them, in order to access any resources for which they have authorization. The combination of more endpoint devices of more different types accessing more applications under more user control dramatically increases the need for good security.

In a converged communications environment, the sheer number of endpoints accessing enterprise information and applications from more locations (e.g., employees, customers, suppliers, and partners using an ever-increasing array of phones, PCs, PDAs and other appliances) raises the level of vulnerability of resources to potential compromise. In addition, threats typical of data networks, such as viruses, worms, Trojans or impersonation, and denial-of-service (DoS) attacks, now apply to all applications and services that run over the converged IP infrastructure. Placing voice mail, call management systems (CMS), call centers, interactive voice response (IVR), and other servers on a converged enterprise network exposes their proprietary customer information to additional threats of eavesdropping, data compromise (unauthorized access, outright theft, or loss of integrity, etc.), or information inference from patterns and monitoring of traffic flow.

To be effective, security must begin with policies leading to procedures that are put into practice using appropriate capabilities and mechanisms. People and processes are the critical elements... without them, the best policies and mechanisms will have no value. Thus the role of security must encompass the mechanics:

- establishing trust between communicating entities (points),
- securing the communication pathway, and
- enabling authorization and enforcing access control inside and at the network boundaries of trust;

*and* the processes:

- establishing a formal process for identifying key information resources,
- developing methodologies to protect and audit these resources to ensure ongoing security compliance, while
- demonstrating a process of protecting these resources.

In a converged communications environment, it is important that no one business or communication application overshadows the needs of another. This is not always easy to accomplish, particularly when IP is the technology chosen for the underlying infrastructure. By providing only best-effort delivery, IP does not

easily support applications that are delay-sensitive, need priority resource allocations, or require performance guarantees. Although more and more organizations are finding that if their network is down they cannot deliver goods and services, many are still tolerant of variable performance and do not have the comprehensive security practices required to protect mission-critical resources. Because voice applications are mission-critical, it is particularly important to partner with a knowledgeable and experienced solutions provider.

Finally, compliance with more and more privacy and security regulations is increasingly important. In the United States the primary legislation of importance includes: Sarbanes-Oxley for financial controls and reporting, Gramm-Leach-Bliley on information sharing and protection practices, the Health Insurance Portability and Accountability Act (HIPAA), the USA Patriot Act, and others. International agreements are being developed to provide similar guidelines and controls, such as the BASEL II accord for risk assessment and management in financial services, the EU Data Protection Directive, and associated U.S./EU Safe Harbor agreement on the protection of personal data, to name a few. For enterprises doing business globally, the challenges are complex because regulations can be so different from country to country or across regions. With converged communications, such regulations may encompass information well beyond their original scope. For example, HIPAA requires individual patient data to be kept private. In a dedicated voice network, the security of a conversation between two physicians discussing a patient would seldom be an issue. However, convergence might well expose such a conversation to eavesdropping through voice packet capture.

### 3.0 Planning for Security is Critical

Security does not just happen – it develops from careful planning for policies and procedures that are put into practice consistently across the enterprise. Generally speaking, security imposes restrictions, limitations, or constraints on how and what people can access from among enterprise resources. It is a balancing act between risk mitigation and resource allocation, so it needs to be tailored to each individual network. In addition, educating users on the importance of security, and providing the right incentives are crucial to engaging people in appropriate practices and behavior. Typically this process begins with engaging stakeholders in setting policies to establish guidelines and expectations, as well as getting management support for both the policies and their enforcement. Next an architectural framework is designed, encompassing processes and infrastructure to implement the policies. Finally, people and systems perform the processes. In other words, security basically comes down to people, processes, and technology, in that order of importance.

For converged communications, policies developed for data networks must evolve to a more integrated, comprehensive view that covers all information and

communication resources appropriately, including voice. This may require a change in mindset for IT professionals who have been responsible for data security. Voice cannot be treated as ‘just another’ type of traffic. Real-time, reliable delivery is crucial to fulfilling the mission-critical role of voice applications in the enterprise.

Policy development creates an opportunity for stakeholders from different areas of responsibility to learn from each other and their vendors and to broaden their views about how to identify and close any security gaps that result from bringing together previously separate networks. For example, access devices will include phones as well as PCs and PDAs, remote access will occur via the public switched telephone network (PSTN) as well as the Internet, and mobile workers will need access as well as workers in fixed locations. Further, service needs will expand to include voice mail as well as email, long distance as well as Internet access, interactive voice response as well as command line and graphical user interfaces, to name just a few examples. For many of these, new servers or servers in new locations of vulnerability will have to be protected. Previous policies may need to be modified or extended (e.g., when outgoing calls should or should not go VoIP over the Internet) and new policies added (e.g., all voice traffic should be encrypted) to account for security threats and vulnerabilities that might not have been an issue in the distinct voice and data networks.

One of the most important considerations prior to defining policy is risk assessment. This is where systems, processes, and procedures are evaluated in terms of their importance to the enterprise and their likely vulnerabilities. Clearly, the more important a resource is, the more attention should be paid to its security. Remember that both import and risks must be reviewed on a regular basis to keep up with changes in the enterprise environment.

With policies in mind, an architecture can be designed and deployed that encompasses all the important elements, from access to applications and infrastructure to management, using a multi-layered approach. Layers not only provide multiple boundaries where defensive mechanisms can be deployed, but also define zones within which resources can be scrutinized both for mismatches in the levels of security provided and for sufficient capacity of the devices and mechanisms. The security architecture should be developed holistically rather than simply pasting together what worked in previously separate networks in order to uncover and address potential gaps. Exactly what data flow and access should be allowed across various boundaries within the enterprise perimeter may be as important as what crosses the perimeter itself. Remember that a majority of security threats still arise from poor mechanisms or practices within the enterprise. Each boundary needs to be carefully considered and drawn to provide maximum protection for mission-critical assets (Figure 1).

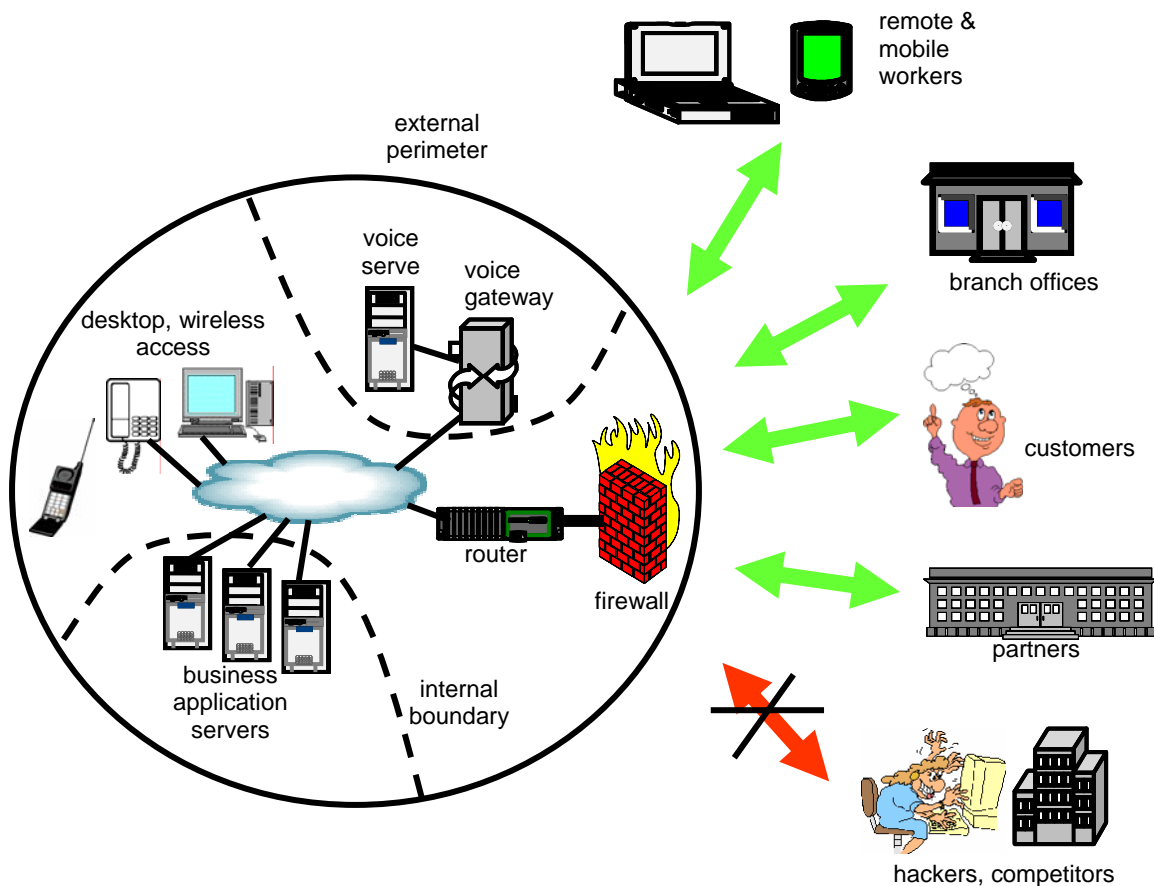


Figure 1. Traditional Perimeter and Boundaries for Converged Communications

Ideally, business applications, communication applications, and the network infrastructure should all be designed together with security in mind, so that policies can be put into practice through procedures and mechanisms for effective policy implementation. This always means careful examination of all application and infrastructure requirements and capabilities in order to address design shortcomings before deployment. Selection of products and services that fall within the guidelines of the security architecture requires fewer exceptions and workarounds, simplifying the infrastructure and its management, improving operational effectiveness, and reducing costs. These considerations are particularly important for meeting voice, data, and other enterprise requirements with a converged communications approach. Designing the security for all applications together helps to avoid conflicts and contradictions that could ultimately erode the ability to provide appropriate security for each individual one.

Overall converged networks require converged security that expands traditional data security policies and procedures to protect the privacy of all network

information, including IP telephony traffic. A holistic approach is also important because simple extension of traditional data security practices can erode the quality of IP Telephony voice if not engineered correctly. In general, there are many more security considerations within voice application layer controls that should be considered, scrutinized, and addressed accordingly.

Finally, security planning must include disaster recovery, and ideally the whole consideration of business continuity, to ensure that applications and services will function properly in spite of incidents such as power failures or storms, or can be restored quickly following them. What converged communications typically adds to these requirements is a range of new and different types of devices such as IP phones, voice communication servers, and media gateways. Planning needs to consider both preventive (e.g., redundancy, fail-over, back-ups, and emergency power) and reactive (restoration) measures for all types of applications and traffic (e.g., both voice and data). For example, if there are communication servers at multiple locations and one becomes unavailable, another should take over its tasks with no loss of functions or features.

#### 4.0 A Trusted Communications Framework

The overall purpose of security architecture should be to set the stage for “Trusted Communications”, meaning communications that are both secure and reliable. A fundamental principle is that security must be from end to end, keeping in mind the aphorism that a chain is only as strong as its weakest link. In this regard, security must encompass everything from the access device through all links and devices to the resource being accessed and back again, and all steps of the accessing process, from user identification/authentication/authorization to access and manipulation permissions to appropriate completion or closure of the operations and access path, and from one user of a business or communication application across all intervening resources to another user, for all data and voice solutions alike. Another way to represent this end-to-end perspective is down and up the layers of the Open Systems Interconnection (OSI) reference model, where all layers and interfaces from application down through infrastructure and back to application must be appropriately secured.

It is important to recognize that the best architectures and designs are easily compromised by poor practices in implementation. One way to address this potential risk is to select products, services, and vendors that embed good security practices. In other words, look at what security characteristics are included by default for safe deployment ‘right out of the box’ as opposed to what must be established by configuration. Embedded features minimize the opportunity for inexperienced installers to compromise the security of other resources when putting in something new. Configuration processes should also be designed so that security options and consequences are simple, clear, and easy to use, even for unsophisticated operators. Whatever manufacturers and service providers can do

to ease secure configuration not only provides better security for customers, but also tends to improve enterprise productivity by minimizing system downtime.

## 4.1 Secure Communication

### 4.1.1 Secure access

Access security has much broader scope in converged rather than traditional communications environments because more people tend to use more and different types of devices to access more and different types of data. For example, a user may want to retrieve voice mail stored on a PC or have email read through a text-to-speech interface. Access requests may come from employees, customers, suppliers, or other partners, using phones, PCs, or PDAs over wired or wireless infrastructure from enterprise or external locations, to run applications or to create/store/retrieve voice, data, or fax information. Traditional mechanisms such as user ID (identifier) and password or protective firewalls must be reviewed carefully to ensure their scope and positioning is sufficient to secure enterprise information, applications, and resources. The basic elements of access security include:

- identity establishment for both users and resources,
- authentication to verify claimed identities,
- ensuring that requestors are authorized for access to requested resources, and
- keeping out users and traffic that does not belong.

### 4.1.2 Application security

Beyond access, application security also has a broader scope under convergence. Applications may run in more places, perhaps distributed over servers at multiple sites or even across desktops instead of being centrally limited to a single server or mainframe located in a secure data center. Applications may be narrowly focused, as in custom software to manage or draw from a proprietary database with built-in security mechanisms, provide generic services with no special security using packaged software, as word processing for document creation, or anything in between, as a Customer Relationship Management package that has been tailored to particular enterprise needs. Furthermore, applications will have a very large range between the few considered mission-critical and the majority supporting routine business activities. For important applications without built-in security, consideration should be given to providing a security wrapper, where the application can only be run through a special interface that provides the required security features. Applications have major responsibility for data consistency and integrity, without which no enterprise can survive for long. Thus they must be

protected by appropriate change management procedures as well as from abuse, misuse, and unauthorized use.

#### 4.1.3 Secure infrastructure

Infrastructure security is a very broad and deep topic - , however, there are a few issues specific to converged communications worth mentioning in this paper. First there is the question of what additional threats are posed to servers previously isolated in secure physical locations when they become attached to a converged network. At a minimum, access controls need to counter such threats. A second consideration is what traffic should be protected by encryption from eavesdropping or misdirection and to what extent this can be selected by end users. What data should be encrypted for storage is a similar consideration. While user control may be desirable in some instances, the risk of bad practice (e.g., forgetting to enable encryption) is higher than when policies are automated within the infrastructure. Finally, the procedures and tools for intrusion detection and prevention must be extended to encompass all vulnerable resources on the converged network, including voice as well as data applications, servers, and storage.

#### 4.1.4 Secure management

Systems and network management involves configuring, policing, and regulating shared resources. Compromising a management subsystem or tool is an easy way to nullify all the security built into secure solutions and a communication environment. The management framework is the last of the links in the proverbial chain that cannot afford to be weak. Secure management practices consist of using appropriately secure protocols and interfaces to perform role-based administrative procedures that implement suitable resource management policies. Of course, such practice must itself be based on strongly provisioned authentication mechanisms to deny access to unauthorized users. The management process elements of concern are provisioning, network and systems management, identity management, and policy management. Network management itself typically consists of configuration, change, performance, security, and accounting management for the network elements. Systems management provides similar functions for end-user and server-type devices. Overall, management security must provide an umbrella to cover policy, processes/procedures, systems, and tools. Protecting the management subsystem is an essential part of enterprise security and must include secure methods of access and update to all management repositories, servers, and consoles.

## 4.2 Important Security Characteristics

When moving voice communications from a dedicated, circuit-switched network into a converged communications environment, the traffic becomes vulnerable to some specific new threats based on greater accessibility to packets as they traverse the network. Consequently the following areas need to be explored thoroughly and addressed by the security architecture.

### 4.2.1 Real-time encryption

By capturing VoIP packets from the network, hackers can potentially eavesdrop on confidential or private conversations using tools that can be downloaded freely from the Internet. Encryption is an important preventive measure that provides privacy for voice streams. *All* endpoint devices, from IP telephones to various software phone implementations (i.e., “softphones”), must have the capability to encrypt in real-time to avoid degradation of the voice quality and protect the conversations. Encryption should extend end to end from caller to destination, for single and conference calls, through bridges and call transfers. Media gateways should also be able to recognize and keep traffic destined for another enterprise site trunked in encrypted format for safe travel over intervening public IP networks. When associated connections such as computer-telephony integration (CTI) links are also encrypted, additional protection against eavesdropping on confidential information is provided.

### 4.2.2 Toll fraud protection

In a converged communications environment all the old possibilities for theft of long-distance services still apply; there are just more potential points of unauthorized access from the IP network. It is important to understand and use built-in mechanisms to prevent inappropriate transfers and call forwarding (e.g., voice mail to dial tone), user authentication and authorization codes, and restrictions of access (e.g., international calling). Procedures for and regular monitoring of call detail records can help to detect patterns of inappropriate calling or long-distance abuse. Remember the value of user education also, to keep people from forwarding remote calls for example.

### 4.2.3 Security hardening

There are a number of hardware and software characteristics to expect from converged communications products. Hardware, for example, may have embedded security features such as - the ability to protect configurable settings from compromise or tampering.

PCs and servers should all be protected by appropriate perimeter firewalls and have signature-based anti-virus protection. In addition, host-based intrusion detection systems (HIDS) can be a powerful way to ensure that the servers are not subject to tampering either by internal or external crackers. Operating systems need to be kept up to date with latest security patches. For PCs it is preferable that what can be is checked automatically every time the device logs on to the network, such as whether permitted versions of software are running and anti-virus signature files are up to date.

Server operating systems are particularly important points at which to minimize the potential for compromise. Hardening procedures include: removing all unneeded services (e.g., HTTP), disabling other services until they are needed (e.g., Telnet, FTP) removing unneeded executables and registry entries, preventing direct login to the root level, restricting shell access, and taking maximum advantage of built-in capabilities such as DoS protection, firewalls, and filtering that are part of standard operating systems.

#### 4.2.4 Survivability and failover

Security and reliability are interdependent characteristics. Inadequate security certainly undermines reliability, but unreliable systems may also compromise security. While voice systems have traditionally been designed for high reliability, convergence adds new concerns. Not only must communications servers and gateways be reliable, so must the underlying network and access. Multiple links, alternate paths, hot stand-by routers, and fast failover protocols that switch traffic from one path to an alternative in a matter of milliseconds while maintaining security parameters and characteristics are all important to reliable delivery of voice traffic, applications, and services.

Another aspect of survivability is to remember that quality of service (QoS) degradation may hamper some converged applications more than others. For example, a denial of service attack may not take down the network, but it could introduce enough extra delay that voice services become unusable. In this situation, failover might consist of adjusting traffic priorities in an attempt to minimize the change in QoS.

#### 4.2.5 Security zones

In traditional voice networks, it was easier to protect specific resources by locking them in restricted areas and limiting access to dedicated administrative ports and terminal devices. For converged communications, critical assets must be protected minimally behind a firewall and intrusion prevention system (IPS), preferably in their own

'private,' protected security zone (e.g., DMZ). Such zones become isolated network segments dedicated to specific functions or services, accommodating only the data for which they are built and protecting them from both external and internal attack. Separating servers into distinct zones minimizes the opportunities for unauthorized access to services and data held by any one server.

For another layer of security, the server software should further restrict access on a port basis. Where access is allowed, only secure protocols such as secure shell (SSH) or secure web (SSL and HTTPS) should be used. Dedicated, private, control LANs may also be used to connect servers to the switches providing the network ports for connection of IP telephony devices and other servers. Overall, multiple layers of well-designed security mechanisms and practices provide a better defense-in-depth approach to protecting mission-critical server and data resources.

#### 4.3 Critical Security Practice

Whether it is nearly impossible or just extraordinarily difficult to provide security against every possible threat, enterprises must be able to demonstrate due diligence. This means vigilantly maintaining a proactive stance toward communications system security, practicing careful design, deployment, and operation at all times. For many, this means drawing on the expertise of an experienced, trusted third party to ensure nothing gets overlooked.

### 5.0 Implementation and Ongoing Management

The implementation and ongoing management of a secure converged communications environment has become much more challenging because of the complexity of applications running on this network. An ability to manage the environment from a holistic viewpoint is critical, as events need to be correlated across the voice and data realms that have traditionally been treated as independent silos.

#### 5.1 Implementation

Given the complexity of the task, implementation of a secure converged network requires sophisticated project management capabilities. In addition to being able to manage a large number of activities, the project manager must have detailed knowledge of and experience with many different technologies. Many enterprises find it useful to engage a trusted vendor to assist with security planning and implementation in order to bring additional expertise and significant experience to bear on their projects.

Another common practice for large or complex networks is to stage the implementation. Staging allows the network organization and/or its partner to perform extensive testing of components and the whole before going into live operation. For example, outages both simple (loss of a line or port card) and complex (loss of an application server) can be simulated safely in a laboratory rather than potentially compromising a production environment. Similarly, load testing can be used to check both network capacity and specific defenses against threats such as a DoS attack. In addition, testing can be useful to establish appropriate thresholds for alarms and notification procedures.

## 5.2 Ongoing Security Management

An important element of ongoing security is to remember that the job is never 'done'. The environment is always changing, both on the business side in terms of needs and priorities and on the technology side where threats are ever-present and the ingenuity of attackers continues to grow. Consequently, a comprehensive security policy must include requirements for periodic review of both policy and architecture, as well as for assessment of the actual infrastructure. Such reviews should take place regularly, with the frequency determined by:

- how likely a target the enterprise is considered to be (a company like Microsoft would need to review more often than a grocery wholesaler),
- how much the enterprise has to lose through a security breach (financial services firms should review more often than an independent video store), and
- how much change has occurred or is planned for the company and the converged communications infrastructure (new service rollouts, corporate mergers, or extending the infrastructure to encompass customers and suppliers should all trigger major reviews).

With change fairly constant in most enterprise environments, reviews should be conducted particularly when a significant change is due in any of the four major elements: access, applications, infrastructure, or management. Piecing together change after change, even in a layered architecture, creates additional complexity and business rules that get harder and harder to manage and maintain properly over time. Periodic reviews allow architectural adjustments that typically keep implementations simpler and make security easier to administer consistently across the enterprise.

Another ongoing concern for security is maintenance, including all types of moves, additions, and changes, across systems, devices, access, permissions, etc. It is crucial to maintain audit trails for these activities, both for diagnostic and accountability purposes. In fact, authorization, authentication, and accounting for maintenance purposes should be centralized for the same reasons. The best security implementations may fall prey here to bad practices, creating significant vulnerability to internal threats from disgruntled employees as well as to external threats. Audit logs and reviews must be rigorously enforced and automated as

much as possible. A companion issue for maintenance is providing secure remote access for supplier or vendor partners. Ideally such access should use one-time passwords and be supplied over ports with special controls. Typical settings that can be turned on and off include: ‘no access allowed,’ ‘one access only allowed,’ ‘multiple accesses allowed,’ or ‘access allowed only from specified port address.’

### 5.3 Using Managed Services

Due to cost and human resource considerations, it is not generally feasible for most enterprises to develop and maintain sufficient expertise and coverage for all areas of security. However, it is certainly worth investigating options for selective outsourcing to experienced and trusted partners, particularly partners who manage the converged communications environment holistically with security as one aspect of the areas being managed. Managed services specific to security include at least the following:

- Monitoring – remote secure monitoring for security breaches and for perimeter protection across multi-vendor applications and networks, on a 24x7 basis
- Managed firewalls –configuration, installation, and ongoing operational management of firewalls using business rules that reflect the enterprise security policies and architecture
- Managed VPN – configuration, deployment, and operation of resources needed to create a virtual private network; may include support services for mobile workers with a variety of access configurations and devices (e.g., laptops, PDAs, smart phones); often coupled with remote site Internet access services
- Managed intrusion detection – monitoring of specified resources for unauthorized access or modification; may include servers, databases, applications
- Managed vulnerability protection – security patch tracking and management; may include periodic vulnerability assessment through penetration testing with specific recommendations for correction

## 6.0 A Call to Action

Security is a 24x7 requirement, creating a set of jobs that are never done. Some organizations may choose to develop their own depth of expertise and employ enough staff to handle all their requirements. Others will be interested in out-tasking or using managed services to augment their own staff capabilities. All need to depend on suppliers with sufficient expertise and experience to provide appropriate and capable products and services.

Whether building an in-house team or assessing partner candidates, the following questions will help establish enterprise preparedness to provide security for converged communications:

1. What expertise and experience is available to foster development of comprehensive security policies?
2. What expertise and experience is available to design the security architecture and apply it to an existing network of IT resources?
3. Is project management capability adequate to test, implement, and ensure a secure network infrastructure?
4. Are processes, procedures, systems, and tools adequate to manage ongoing operations to maintain appropriate levels of security for all business and communication applications as well as for the infrastructure itself?
5. Are capabilities to review and adjust policies, architecture, and infrastructure sufficient to ensure ongoing security across a continuum of business and environmental change?
6. Is there a strategy for and capability of managing the converged communications environment holistically, including management of security aspects of the environment?

Remember that people and processes are the heart of good security practice. Without the right people involved in and processes for consulting, planning, implementing, and ongoing management of security, even the best technology could be of little value to the enterprise.

Sponsored by Avaya, Inc.

For more information about Avaya solutions, go to [www.avaya.com](http://www.avaya.com)