

Solution Brief

---

**Securing VoIP  
Deployments with IDP  
Business Implications**

---

## VoIP Market Overview

Solutions based on VoIP have been in existence for the better part of a decade. As with most new technologies, the VoIP market has gone through several phases of development and maturation to arrive at the current state.

The earlier development focused on voice quality and compatibility with existing equipment such as legacy telephone switches. It was soon followed by the development of customer premise equipment (CPE) for supporting legacy telephones and other telephony features such as (legacy and IP-based) voice mail.

While some deployments of VoIP solutions still face regulatory hurdles, we have seen a huge increase in VoIP development in the past few years. Development of true IP-based phones, multi-media messaging systems and WiFi phones are some of the recent developments.

## VoIP Adoption

It is common to associate VoIP solutions only with the enterprise internal telephony system since it is arguably the most commonly deployed solution. Therefore, if your enterprise continues to use a legacy PBX solution, it would be natural to assume that you do not use VoIP solutions in your daily business. However, this may not be the case due to the widespread use of VoIP technologies.

Anyone who has called airlines to verify a flight schedule or a restaurant to ask for directions will likely have used a VoIP solution at some point. Interactive Voice Response systems (IVR) which often integrate voice recognition capabilities has become one of the most cost effective ways for providing an unattended/automated solution for customer service management.

Another common usage of VoIP technology is for web seminars and on-line meetings. While some solutions require the use of a telephony system (legacy or IP-based) for voice traffic, many solutions broadcast the voice data along with the visual media. The cost savings of using broadband for such activity can be significant compared to the use of a separate telephone system.

## Business Risks

With the apparent benefits offered by VoIP solutions, enterprises are widely adopting it for use in their day-to-day business. However, with the growing dependence on VoIP solutions, it's becoming increasingly critical that the solution be protected to ensure continuing operation.

The type of threats that VoIP solutions can face include hijacking of the PBX or soft switch to make unauthorized calls, eavesdropping on phone conversations and attacks to disrupt the voice communication. Practically all enterprises would incur significant losses should their phone system be unavailable even for a small amount of time.

Aside from voice communication related attacks, VoIP solutions can also face general network attacks. Unlike traditional voice solutions, VoIP solutions would leverage the same network infrastructure as other network devices. Hence, it can be a target of attack to disable not only the voice solutions but the entire network. An attack that disrupts the enterprise network including e-mail and access to intranet or external can result in significant financial loss to the enterprise.

## Security Requirements

Deployment of VoIP solutions, similar to other network appliances, must account for security of the device itself as well as how it can be used to attack the network as a whole. Ensuring secure deployment can be divided into two main areas; preventing attacks from hackers outside the network and preventing inadvertent attacks from within the network.

Thwarting an external attack for a VoIP solution requires a thorough understanding of the VoIP protocols. Through these protocols, external attackers will try to gain unauthorized access into the network and devices by "calling in" to the network. They can also use the VoIP solution to leave Trojans behind which can open up back doors to the network. Hence, knowing what is normal practice and usage of these protocols is essential in identifying attacks from normal traffic.

Many enterprise users use their laptop as a "soft" phone when traveling. This solution can result in significant savings over the use of cellular phones. However, since the user must usually connect to the corporate office first before setting up a VoIP connection, a compromised laptop can use the VoIP infrastructure to send worms, Trojans and other malware to the corporate network. While VoIP infrastructure is only one of several ways an attack can be launched from a compromised laptop, a security solution without the necessary VoIP coverage will provide an unmonitored conduit into the corporate network.

### Market Perception on VoIP security

As VoIP solutions gain momentum, customers are increasingly becoming more concerned regarding the security implications. In a survey conducted by IDC in November 2005, 272 enterprises already having deployed or will deploy VoIP solutions were asked to rate the importance of several factors in selecting their telephone equipment. The following figure illustrates the top five factors identified as very important:

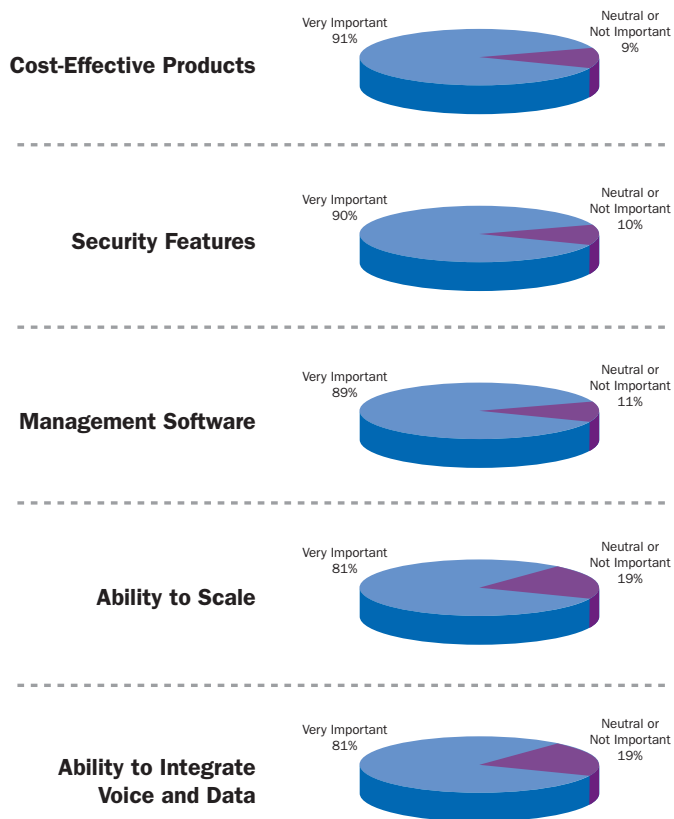


Figure 1 Survey of the top 5 importance factors in selecting the telephony equipment

According to this survey, 90% of the enterprises surveyed determined that security features are very important factors to consider when deploying their telephony system.

### Juniper Networks IDP Solution

Juniper Networks Intrusion Detection and Prevention solution includes several attack detection mechanisms to thwart VoIP-related attacks.

The stateful signature detection feature currently includes several SIP-related exploits as well as the H.225-related exploits. Juniper IDP can track the state of a VoIP connection and scan for specific

attack patterns only in the relevant portion of the traffic. This “intelligence” significantly reduces false positives and improves the performance of the VoIP traffic flow which is especially critical for voice application.

Since VoIP solutions use specific protocols, Juniper Networks IDP solution includes a protocol anomaly detection engine specifically for VoIP protocols. This feature can be used to identify attacks that deviate from the original intended use of the protocol. Without such awareness of the VoIP protocol, an attack exploiting the protocol can go undetected in the network causing significant impact to the overall network.

### Juniper Networks Innovation

VoIP solutions are particularly sensitive to delays in data (latency) and variations in delays of the data (jitter). Latency is usually characterized by delays in the voice transmission. Since most users notice a delay of more than 250ms, it’s important to minimize latency as much as possible. Jitter on the other hand can result in garbled voice transmission rendering the solution unusable.

To minimize delays in inspection of VoIP traffic, Juniper Networks IDP solution inspects the voice control traffic differently from the voice data traffic. Since the majority of the attacks reside in the control portion of the call, all traffic related to the voice control are heavily scrutinized for signs of attacks. The voice data traffic on the other hand, is optimized for efficiency improving the overall user experience of the solution.

### Total Juniper Network Solution

While Juniper Networks IDP solution offers the market-leading security for VoIP deployments, its collaboration with other Juniper products clearly sets it apart from other offerings in the market.

The recent collaboration of Juniper Networks IDP and SA SSL VPN solution allows the network administrator to identify who is (knowingly or inadvertently) launching an attack remotely. Due to the flexibility of SSL VPN solutions, it had traditionally been difficult to pinpoint the source of the attack. Now, the administrator can not only identify the remote user but is able to quarantine the user from launching any additional attacks without impacting other remote users. Such a scenario is very common when using laptop-based or “soft” phones by a remote user.

In addition to the stand-alone IDP appliances, Juniper Networks also offers the award-winning ISG 1000 and 2000 which integrates the best firewall and IDP solution available on the market into a single footprint.



CORPORATE HEADQUARTERS  
AND SALES HEADQUARTERS  
FOR NORTH AND SOUTH AMERICA

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888-JUNIPER (888-586-4737)  
or 408-745-2000  
Fax: 408-745-2100

[www.juniper.net](http://www.juniper.net)

EAST COAST OFFICE

Juniper Networks, Inc.  
10 Technology Park Drive  
Westford, MA 01886-3146 USA  
Phone: 978-589-5800  
Fax: 978-589-0800

ASIA PACIFIC REGIONAL  
SALES HEADQUARTERS

Juniper Networks (Hong Kong) Ltd.  
Suite 2507-11, Asia Pacific Finance Tower  
Citibank Plaza, 3 Garden Road  
Central, Hong Kong  
Phone: 852-2332-3636  
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA  
REGIONAL SALES HEADQUARTERS

Juniper Networks (UK) Limited  
Juniper House  
Guildford Road  
Leatherhead  
Surrey, KT22 9JH, U. K.  
Phone: 44(0)-1372-385500  
Fax: 44(0)-1372-385501