



# Securely Extending the Enterprise With Private MPLS Networks

<b>1. Introduction</b> .....	2
<b>2. Global Working and The Extended Enterprise</b> .....	2
<b>3. A Holistic View to Security</b> .....	3
<b>4. Securely Extending a Private MPLS network</b> .....	4
<b>5. Extending Core Network Security with Professional Security Services</b> .....	5
<b>6. The Bottom Line to Extended Enterprise Security</b> .....	6

## Introduction

Globalization has had a profound, lasting effect on the world economy. With the rise of globalization many companies have, therefore, recognized the need to change how they organize themselves—that is, supporting an increasing amount of home and flexible workers—as well as how they organize and manage their relations with those on whom their business is dependent. That is to say people such as customers, suppliers and partners. They, in short, have had to extend their enterprise to reach out to as many places as possible, providing access to business-critical information to all those who need it, wherever they may be.

The bedrock of the extended enterprise is their IP-enabled networks, yet by extending the enterprise to customers, suppliers and vendors, companies increase the risk they face from electronic attack. Put simply, the more information that enterprises have to distribute and manage, and the more places in which that information is housed, the greater the risk of that information being accessed by unauthorized parties.

This whitepaper will investigate the key questions that need to be addressed and some of the means and resources that will help you shield your extended enterprise from increased risk.

It will start out by examining the general security landscape, and propose that the optimum course of action is to take a holistic view to securing your extended enterprise, in particular advocating that the use of a Private MPLS network can allow you to transact successfully and securely with customers, suppliers, distributors, and partners within an extended enterprise.

Moreover you can support this concept of information security not only through security technology ownership but also by subscription to security services from trusted suppliers. That is, your aim should be not only to employ IT security products and services that offer counter measures against recognized threats, but also to work with IT security product and service suppliers that offer solutions to actively reduce risk to the business.

## Global Working and the Extended Enterprise

Despite the current economic slowdown, globalization continues to impact companies across a wide range of industries. Increasing competitive pressure, rapid technological change and ever growing customer and supplier demand are all by-products of the trend towards globalization in some way, shape or form.

Even though companies have always looked at ways to expand their business and to improve their bottom-line, some argue that globalization has simply increased the pace at which this has happened. Markets are changing; in particular the demands of customers and the needs of suppliers. The plain fact is that in order to stay ahead in the global economy, companies need to act quickly upon these changes that impact the markets they are serving.

One key trend has been the shortening of product life cycles. In the mobile electronics sector for example more devices than ever are launched in shorter timeframes than ever before. Recent events, like the rapid decline in demand for trucks and sports utility vehicles in the US, also showed just how changing consumer preferences in a global economy can affect organizations and their associated partners including suppliers, and distributors, as well customers and staff.

In response to markets becoming more global, companies' workforces have also become more global, with geographically dispersed employees and functions collaborating on company projects. Companies are also extending their enterprise to include business networks, such as their customers, supply chain, distributors and partners to share information or to contract for knowledge and expertise.

The key demand on today's extended enterprise is to become more flexible, adaptable and ultimately more competitive and offer more information to workers in more places. Furthermore, many of the new business relationships created by the extended enterprise are provisional, set up on an as-needed basis to work on a specific project for a specified period of time.

Yet sharing information within the extended enterprise inherently increases the risk of this information being accidentally exposed, leaked or illegally obtained by unauthorized third parties. Put simply, the more information that you have to distribute and manage, and the more places in which that information is housed, the greater the risk of that information being accessed by unauthorized parties.



Those charged with extending their enterprise to more locations have to maintain a difficult balancing act, providing increased access yet under strict control. The most secure network you could have is one with zero access to the outside world: it is probably the most unproductive. Thus you can only gain the benefits of the extended enterprise from networks that offer access to business-critical information along with multiple levels of security protections.

### A Holistic View to Security

Even though, like all firms, you will almost certainly run some security solutions, your security apparatus should be seen as part of an ongoing process that requires those technologies and others like them to be closely integrated.

For a company operating globally, security should not be looked at as a single event or responsibility. In fact, you need it to be an integral part of every decision that your company makes.

The traditional way of protecting electronic information has been to implement a variety of IT security technologies designed to counteract specific individual threats. The principle aim of a security strategy was to protect the company's premises and operating perimeters by keeping the bad guys out. Yet today's sources of electronic attack, or threat vectors, are much more varied and subtle. Businesses, therefore, need to employ equally more subtle and varied approaches for the protection of their business-critical resources.

And it is a dangerous assumption to believe that this unauthorized access will originate exclusively from outside the enterprise; real and present threats also emanate from "internal" sources, including business partners and the enterprise supply chain. The 2009 Data Breach Investigations Report conducted by the Verizon Business RISK team, clearly highlighted the changing IT security landscape and the new vectors that are at play. (See Sidebar 1.)

Highlighting why you need to look at all aspects of the business, inside and out, the report—based on detailed reports of 90 confirmed breaches investigated by Verizon Business forensic investigators in 2008—showed that even though almost three-quarters of breaches resulted from external sources, a fifth of data breaches were caused by insiders and nearly a third were linked to business partners. Not only do they illustrate the diverse nature of security threats, these findings also suggest the amount of complexity that you may face in safeguarding your enterprise against targeted, multi-sourced attacks.

Due to its position at the nexus of business networks, and the frequent changes to its business relationships with the outside world, the extended enterprise has some inherent weak points regarding security.

Attackers are increasingly targeting points of data concentration or aggregation in order to attain more valuable sets of consumer information. Such people are aware that enterprises face a dilemma: they need to reach out and make more business information available in more places, yet this where vulnerabilities can arise.

At its most basic level, managing information security is a balancing act between the costs of a breach to your IT infrastructure—both directly and indirectly—and the efforts you need to take in order to properly secure your infrastructure.

It is essential that you protect, from internal and external threats, your most important assets: that is your business-critical information. By protecting the free transmission to your intellectual property, you boost business reach and flow and limit business disruptions that may jeopardize revenue streams. In addition, your security mechanisms should help you comply with internal and external security compliance requirements. This is an increasingly vital aspect of risk management: if you are working in a regulated industry that mandates strict codes of compliance and governance, the ramifications of security breaches can be business-threatening.

Successful security management involves setting up not only the technologies, but also the practices that can maintain your corporate brand, reputation and customer trust. These are the elements that should go right to the heart of your firm's value proposition. Frequent changes within relationships or partners translate to a constant re-evaluation of the demarcation between private, public and shared resources within the business domain of the extended enterprise.

### Who Is Behind Data Breaches?

- External sources: 74% (+1% compared with 2008)
- Multiple parties: 39% (+9%)
- Business partners: 32% (-7%)
- Insiders: 20% (+2%)

Closely resembling the results from the 2008 report, most data breaches continue to originate from external sources. Though still a third of our sample, breaches linked to business partners fell for the first time in years. The median size of breaches caused by insiders is still the highest but the predominance of total records lost was attributed to outsiders. 91 percent of all compromised records were linked to organized criminal groups.

Source: Verizon Business "2009 Data Breach Investigations Report"

### Sidebar 1: Sources of data breaches



Securing your extended enterprise requires you to take a holistic view to security, considering your internal enterprise assets as well as their relationships with the outside world. You should focus on a number of key areas, namely:

- Securing information
- Securing the infrastructure
- Addressing governance, risk and compliance, paying particular attention to the issue of standards. (See sidebar 2.)

Taking a holistic view of security will mean that you not only understand security from an enterprise perspective, but also view security in relation to others such as suppliers, partners and distributors.

You should adopt a basic strategy that is tailored to your own needs and is process-centric. You need to both assess and prioritize the real-world threats to critical information assets and balance IT security risks with operational priorities, managing costs and implementing security controls that are adequate for your specific business needs.

What is required is a flexible framework to fit your specific business risk and compliance profiles, one that streamlines information security across your entire enterprise and provides ongoing, independent analysis of implemented security controls.

The fundamental principle is that with security one-size does not fit all; technology and service providers have to deliver security solutions designed to your customer requirements and delivered as you need, whether it is out-sourced, co-sourced or indeed in-sourced. The solution simply has to align with your business requirements and working practices and complement your network.

### Securely Extending a Private MPLS Network

The advent of IP networks has opened up huge possibilities and opportunities for businesses. Having a flexible, more open architecture on which to combine voice and data communications is removing a lot of the traditional limits to business imposed by device boundaries and perimeters. This has resulted in a complete transformation in business and technology approaches. You can base your business around large-scale unbounded networks that can virtualize the orchestration of networked communities, communities where the traditional restraints and boundaries of legacy networking no longer apply.

Such networks should provide you with a wide range of access choices, ranging from wireless, Ethernet, DSL to Satellite access solutions. They should support broad connectivity around the globe and provide flexible Classes of Service to prioritize your organization's core applications based on your requirements.

One of the most successful networking technologies of the last decade has been multiprotocol label switching (MPLS). However, even though MPLS networking technology may be considered secure, taking a holistic view to security means that you should look beyond the networking technology itself and examine from an infrastructure, technology and process perspective how it is being used. And there are a number of key issues you should consider when making that assessment.

Security of a network starts with the initial design, and you should allow no compromises at that level. Any MPLS-based IP network should have physically diverse trunking into the rest of the provider's network in order to avoid nodes to become isolated. You should also evaluate, in detail, the expansion plans of your provider so that the company can live up to the availability claims they make in their Service Level Agreements.

The foundation for a secure extended enterprise communication solution should be a secure, Private MPLS network. Within such a network you can prioritize traffic—whether it is voice, video or data etc.—while consolidating your traffic on a single network. This offers you additional flexibility that lets you dictate how traffic is handled across the network, giving priority to mission critical traffic and enhanced levels of control given that you do not share any core network elements with any Public IP network.

You can configure MPLS so that private and public data is logically separated, but network operators who share private and public IP traffic over the same physical circuits and routers may find it more difficult to manage traffic congestion due to the unpredictable nature of public IP traffic. These network operators would need to properly secure the provider edge (PE) elements from attacks and vulnerabilities.

Furthermore, the core of your Private MPLS network should not be visible to outside networks. Even though a breach of this requirement does not lead to a security problem itself, it is advantageous if the internal addressing and network structure remains hidden to the outside world. This would, for example, make it harder for a Denial of Service (DoS) attack to be carried out against core routers.

**One industry standard** that applies to many enterprises is the Payment Card Industry Data Security Standard (PCI DSS). The first fundamental requirement of PCI DSS, is to build and maintain a secure network. A great deal of public discussion has taken place regarding the effectiveness of regulations and control guidelines to prevent breaches, but empirical study of the topic remains scarce. Unofficial post-breach PCI reviews in the Verizon Business "2008 Data Breach Investigations Report" found the average compliance rate across victims to be 29 percent of the 12 (PCI DDS) requirements. In other words, the typical organization had met less than a third of the requirements in PCI DSS. Some fared much better and some much worse, but the point is this: the breaches investigated, in general, did not occur in organizations that were highly compliant with PCI DSS.

Source: Verizon Business "2009 Data Breach Investigations Report"

#### Sidebar 2: The significance of the Payment Card Industry Data Security Standard (PCI DSS)

In November 2008, Verizon Business engaged Symantec to conduct a Network Architecture Assessment focused on its two MPLS-based IP virtual private networks. The objective of this project was to perform a documentation and physical security review to verify that the security levels of the platforms meet the security practices used to protect the networks against the NIST 800-53 Revision 2 standard at the "moderate" baseline. Overall, Symantec found the Private IP network to be very robust in terms of engineering discipline, redundancy, and resiliency. The security frameworks and policies responsible for the management and operation of the networks take a holistic approach and are comprehensive in their mandates, procedures and directed governance of the information systems and the individual users and groups that actively manage them.

#### Sidebar 3: Defining Private IP network security



MPLS uses address space and routing separation so that data between your virtual private networks (VPNs) is not shared. However, it is theoretically possible to exploit the routing protocol to execute a DoS attack against the PE router, which in turn might have negative impact on other VPNs. For this reason, your PE routers must be extremely well secured, especially on their interfaces to your customer edge (CE) routers, and you must configure the network to limit access only to the port(s) of the routing protocol and only from the CE router.

Extended enterprises need both flexibility and control. You should review what assessment services, application reporting and control tools your IP network provider can offer you as an additional service so that you can maintain visibility and control on an ongoing basis. Even though some companies may not have any view on what applications are being used on their network, you'll probably know already that there are many applications that are simply inappropriate for business use: at best, they may clog up bandwidth; at worst, they may allow attackers punch a hole in your security framework.

Deploying a Private MPLS-based network is well suited for the holistic approach needed to secure an extended enterprise. You can exercise a high level of control and maintain tight security, based on your own policies and level of risk tolerance.

You may need to extend your network to reach smaller sites, to provide access to home-workers or roaming users, or to provide a cost-efficient way to provide secure Internet access for browsing. This requires careful planning to avoid compromising the security of your network.

With a Private MPLS network, you should be able to set up a secured gateway to the public IP network to provide your employees, customers, suppliers and partners with all of the extended reach that you intend. You have every right to expect that your service provider can control the gateways, all the while providing integrity and security.

Each element of customers', suppliers' or employees' traffic should be isolated from one another; and, as such, any traffic flowing between the public network and the Private MPLS network should be managed per customer VPN. Your gateway should isolate the private network from the public network until a connection is set up using an IPsec tunnel and only traffic coming in on that tunnel should gain access to the private part of the network.

### Extending Core Network Security with Professional Security Services

As you may know only too well, current economic conditions are driving the need to do more with less, placing the focus firmly on efficiencies and driving cost out of the business. Nice-to-haves have become luxuries.

Protecting your business's most important assets is certainly no luxury and in assessing how to improve the security of your Private MPLS network, you may have to make some very difficult business decisions as to the most effective way of carrying out your plans.

If you wish to achieve your goals by in-house means you will have to make capital investment in technology and infrastructure and also in special trained staff to carry out the job. Given the business imperative to control capital expenditures, it could well be the case that the best solution for securing your Private MPLS network is to rely upon a trusted supplier who provides network security as a managed service—as part of a packaged, outsourced program that is effective at supporting your security risk management strategy, fostering best practices and enabling effective cost control.

There is no need for you to make large capital investment in network technologies or infrastructure—nor invest similar amounts in specialized staff. A managed program can help limit obsolescence in technology and services; you get the state of the art, in terms of technology and services, without having to make capital investments. Furthermore, security and risk reduction is in the hands of people whose full time job it is and who can offer a wealth of knowledge and experience.

Specifically, the service provider should provide you with full security management supported by an SLA, full security monitoring and 24x7 security support. Such a cloud-based managed security service should be identical to a CPE-based security service, so that a company can decide to mix and match CPE-based and network-based firewall solutions throughout an enterprise.

You should evaluate suppliers' IP network by looking at the additional security advice it can provide you by analyzing data from its own global network. Some key providers have equipped their global IP networks

### Verizon Provides Internet Security Assessment

Internet Security Assessment Helps Secure extended enterprise Verizon Private IP customers around the globe can now take advantage of Verizon Business' Internet Security Assessment. This solution provides customers with an innovative and powerful approach to review important aspects of their security posture, and then assess the risks associated with Web-based network infrastructure. The Internet Security Assessment includes Virtual Discovery & Classification and External Risk Assessment, supported by professional services. To help protect an organization's extended enterprise of customers, partners, vendors and suppliers, both components provide customers with a view of their security landscape based on an analysis of their Internet activity coupled with a rigorous scan for vulnerabilities.

#### Sidebar 4: The Verizon Internet Security Assessment

### Verizon Provides Cloud-Based Security Services

Private IP customers can now take advantage of a fully managed cloud-based security offering that enables them to offload the management and administration of the network-based firewall. Verizon's security experts can help customers determine and implement strong firewall policies to serve as an effective first layer of defense against potentially harmful traffic. Verizon Business will work with customers to implement appropriate firewall policies and will monitor and update those policies as business requirements change.

#### Sidebar 5: Maintaining security in cloud-based services



with early surveillance and warning tools, called honey pots. These are traps set on a public IP network to detect attempts at unauthorized access to networks and IT systems. This is then used to gather intelligence to help build specific countermeasures, helping strengthen the security of the network.

The core network security program should provide a centralized secure connection for data transport. In addition to that, as the data enters into your extended enterprise, security mechanisms need to be in place to help protect it and to mitigate the risks around it.

In securing your information, professional services can address data protection for the critical data residing in your extended enterprise, forensics investigations for breaches and compromises of data, identity and access management to administer the right levels of access and control to your data owners and users, and network and application security measures. You may also want to look at support with management and monitoring of the security and non-security devices within your enterprise along with relevant policy reviews, architecture design reviews and security event management support.

In addressing governance, risk and compliance, you can leverage a number of security programs to help address information security compliance requirements, validate due diligence, mitigate risks for your customers, partners and contractors and verify security policies are being adhered to by all.

Such successful managed services should essentially be risk reduction-driven rather than based on management-intensive point-solutions that typically have high associated running costs. Thus, extending core network security with professional security services is a cost-effective and efficient way to help mitigate risks and allow your organization to continue focusing on what you do best.

### **The Bottom Line to Extended Enterprise Security**

Without a doubt, there will be more and more globalization thus driving the need for your enterprise to reach out to more and more people in more places.

While this gives you the chance to be a more flexible entity with more ability to take advantage of more business opportunities in more places, you cannot ignore the commensurate increase in exposure to the risk of attack. It's vital that you take a holistic view of the information security and risk reduction imperatives of your extended enterprise, looking for all areas that may be vulnerable.

In terms of a technical solution, a Private MPLS network offers great benefit in allowing the robust, accessible and effective communications of business-critical information to your employees, customers, partners and suppliers wherever they may be located.

In terms of a cost-effective security solution, the best course of action is to subscribe to services that offer the latest solutions that actively reduce security risk to the business without recourse to high levels of capital investment.

Managed security services can align information security with your critical business goals by providing guidance and decision support around your security priorities, resource allocation requirements and your overall strategic focus. To do justice to your role as a globally operating extended enterprise customer, you should look for a service provider you can trust with the fundamental security of your Private MPLS network and who is able to provide reliable, high-quality service. The provider should allow you to send traffic effectively and enable security controls that help reduce the risk of attacks and deploy robust and constant security monitoring and management.

In short, you should work with a service provider who can allow you to proactively and cost effectively address emerging threats before they present themselves as a business risk, allowing you to concentrate on your core competencies and do better business.

For more information on our Professional Security Services please visit us at [www.verizonbusiness.com/solutions/professional/secure.xml](http://www.verizonbusiness.com/solutions/professional/secure.xml).

**verizonbusiness.com**

© 2009 Verizon. All Rights Reserved. WP14131 12/09  
The Verizon and Verizon Business names and logos and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners.

### **About Verizon Business**

Verizon Business, a unit of Verizon Communications (NYSE: VZ), is a global leader in communications and IT solutions. We combine professional expertise with one of the world's most connected IP networks to deliver award-winning communications, IT, information security and network solutions. We securely connect today's extended enterprises of widespread and mobile customers, partners, suppliers and employees—enabling them to increase productivity and efficiency and help preserve the environment. Many of the world's largest businesses and governments—including 96 percent of the Fortune 1000 and thousands of government agencies and educational institutions—rely on our professional and managed services and network technologies to accelerate their business. Find out more at [www.verizonbusiness.com](http://www.verizonbusiness.com).

