

white paper - white paper - white paper - white paper - white paper - white paper - white paper

# protecting your business with embedded network security



Business  
Services



# summary

- 3 executive summary
- 4 setting the scene
- 6 different approach to security
- 8 embedded security
- 11 business advantages of security

# executive summary

Confidential information is increasingly at risk in organizations. This white paper explains how to improve protection in branch offices. Reality shows that perimeter controls alone are no longer sufficient and businesses need to update their security strategies to reflect new working practices. Workers are more mobile than ever and are taking data out of their organizations on laptops; third parties are connecting to corporate networks on devices that the IT department has little, if no, control over; and branch offices with scarce security resources are becoming the mainstay of multinational organizations. These trends have converged to create de-perimeterized organizations where internal security is as important as external security.

Businesses not modernizing their security will inevitably be more at risk for a security breach. And that's not all: any breach will also have a bigger impact on the business because the revolution in converged networks has connected all different types of resources and applications on a single infrastructure. Where a distributed denial of service (DDoS) attack might once have just taken out the email system, the same attack could now take down the telephony and ERP application as well.

Essentially, the corporate environment can no longer be relied on to be a "trusted" zone and, to protect de-perimeterized organizations, it is important to embed security throughout the business. Security controls need to be embedded in the infrastructure layer, the transport layer and the application layer, and Orange is addressing these requirements at all levels.

In this paper we review security at the transport layer with our Network Protect service. This managed service is designed for branch offices that have limited internal security resources because it is easily integrated into the sites' routers. Network Protect offers automated protection through firewall and intrusion detection/prevention so that branch offices are able to secure themselves against threats within the corporate network. Additionally, the rest of the organization is protected from security breaches originating from those branch sites as the appliance also monitors outgoing traffic.

Network Protect improves security throughout the organization by complementing other security services, such as Secure Gateway, that provide protection for larger sites and give organizations much more confidence regarding the application of security rules across the WAN. For a comprehensive view of security status, Security Event Management can provide alarm analysis across an entire organization's security infrastructure.

# setting the scene

Rock-solid security is a prerequisite in the knowledge economy. Intellectual property is at a financial premium, so it is essential to protect it from inadvertent loss and to keep it out of the reach of professional fraudsters. Information is becoming increasingly difficult to secure in companies that have many branch offices with limited internal IT resources and increasing numbers of mobile workers.

The risk of data loss is increasing. A recent study found that nearly 40% of businesses experienced the loss of sensitive information in the past year, with 16% suffering material losses of over \$1 million. But the costs of data loss are not always financial – there are also brand, image and compliance issues. Business regulations, such as Sarbanes-Oxley, HIPAA and Basel II, demand that companies account for all of their data movements, including instant messages, email and fixed media and, in some cases, force companies to publicly disclose data losses.

The task of securing information is being made more difficult by technology convergence. While converged networks have changed how businesses communicate, they also have increased the amount of damage that security breaches can cause. Because different networks and resources are now all connected, companies could find their email, enterprise resource planning (ERP) applications, CCTV systems, building automation and IP telephony systems all taken out of action in a single attack.

## mobility and external parties

Workers are becoming increasingly nomadic. This extends a company's reach, but it also extends its risk. Confidential information is frequently out in the field and away from the direct control of the IT department. A recent study found that more than half of employees accessed their networks remotely with a laptop or mobile device in more than 70% of the organizations studied<sup>1</sup>. Just three years ago, less than one-third of employees did the same. With increased mobile working, it is not surprising that there is a rise in the level of laptop loss and theft, yet less than 8% of companies encrypt data stored on mobile devices<sup>2</sup>.

1 Yankee Group: Anywhere Access Technologies Open Enterprise Networks report, October 2007

2 BERR/Price Waterhouse UK security survey, April 2008

It is not just mobile employees who can put a strain on an organization's security. An increasing number of organizations are inviting third parties into their corporate environments and providing them with company services, such as email, web portals and business applications. In fact customers, suppliers and partners need to access company resources frequently or every day in 87% of enterprises<sup>3</sup>; three years ago it was just a third. In security terms, third parties introduce an unknown quantity into the organization. Their devices may not be properly secured and could introduce malware into the network, or they may not be correctly identified and inadvertently given access to confidential information.

And it is at smaller sites where the risk is most pronounced. Many multinational organizations have moved away from having a handful of very large sites and offices to a decentralized infrastructure with many smaller offices, depots, sites or outlets. Centralized delivery of enterprise applications over the corporate WAN is empowering this change in topology, and it means there is very little IT resource needed at smaller sites. Although this is an efficient use of resources for application delivery, it leaves smaller locations exposed with little or no IT security on site.

### growing de-perimeterization

The increase in nomadic workers and third parties accessing the network requires the enterprise to become de-perimeterized. There's no point in having an enterprise perimeter if workers need to access information when they are outside it. Businesses no longer work in isolation of each other, and systems and personnel interconnect as a matter of course to reflect business relationships. The age of monolithic enterprises has passed and has been replaced by networked organizations, where knowledge is shared with other organizations as a matter of course across enterprise perimeters.

De-perimeterization of the business, the increasing number of branch offices and access by third parties into the corporate network are all increasing the number of vulnerability points of the business. These threats from within are forcing businesses to change their approach to security.

<sup>3</sup> Yankee Group: Anywhere Access Technologies Open Enterprise Networks report, October 2007

# different approach to security

Historically, organizations have relied on protecting the enterprise perimeter with equipment such as firewalls. While this approach might be adequate for an organization that wants to operate within its own closed environment and only communicate with the outside world through email or the phone, it is no longer sufficient for the vast majority of modern businesses.

In the knowledge economy, employees frequently operate outside their organization's perimeter, and third parties with unknown equipment need access to company resources. Even employees who operate primarily from main offices are not adequately protected by traditional perimeter security because an increasing number of applications, such as Web-based services, use technology that can legitimately bypass firewall security. Furthermore, perimeter security is ineffective against security threats, such as malware, that use email or web technology to propagate.

Unfortunately, while business connectivity has changed dramatically in the last ten years, many businesses continue to use an outdated security approach that no longer meets their needs. The Jericho Forum<sup>4</sup> argues that many business and IT leaders have become victim to the myth that good security starts and ends with a hardened perimeter. It warns that most device and network security has been additive over time, with interim solutions, such as VPN technology, applied with little regard to whether or not it is the right approach. In many organizations this has led to an explosion in the implementation of many different security products, making it very difficult to ensure and manage security.

## setting appropriate security

Security threats no longer come chiefly from outside the organization. A recent survey<sup>5</sup> found that 80% of IT directors prioritize combatting internal threats over external ones, and that only 17% believed that external threats posed by hackers were more dangerous. Most spending is being directed toward strengthening internal security, with 35% of IT directors identifying it as a priority investment.

4 A CISO-led security thought-leadership group under the auspices of the Open Group that is focused on the issues surrounding de-perimeterization

5 Secure Computing study of 103 IT directors worldwide, May 2008

To correctly direct their investment, companies need to look at protecting the "CIA" of their data:

- confidentiality
- integrity
- availability

An attack on confidentiality is a third party stealing data; an attack on data integrity could be a third party interrupting a financial transaction and inserting an unauthorized code; and an attack on the availability of a converged network would be one that stopped the organization from making calls.

To understand the impact of security breaches, companies need to identify their information assets and their interdependencies. This will allow them to ultimately measure the cost of any security breach and make the appropriate security investments. Because there are more interdependencies in converged networks, the cost of any security breach is conversely higher. However, it isn't always desirable to have the highest level of security protecting each asset as this directly impacts cost and usability. If security makes an application too difficult to use, then users will attempt to circumvent it, making the investment worthless.

# embedded security

Enterprises need to have consistent and comprehensive security from the edge of the enterprise through the local area network to the end user. All assets and sites need to be protected, as security is only as good as the weakest link. For example, it is no good protecting the Internet gateway if a security breach happens in a small branch office. As research company Current Analysis notes, instead of treating the premises LAN as secure by default, all data, both outbound and inbound, should be considered as potentially suspect<sup>6</sup>. The same can hold true for intrusion prevention, where intrusion attempts may come from inside the enterprise network.

There are essentially four different types of security controls that enterprises can use to protect their infrastructures:

- **manual detective** – allows users to review logs generated by a security appliance
- **manual preventative** – allows users to take action based on what they detect
- **automatic detective** – automatically collects logs
- **automatic preventative** – automatically takes action based on what the appliance detects

The least effective of these controls is manual detective, with which a user simply looks at logs generated by a security appliance. Automatic preventative devices are the most effective, particularly in situations where there are few internal resources to take action against security breaches.

## embedded in all levels

To ensure security, embedded automatic preventative controls throughout the organization at all layers are recommended:

- infrastructure layer
- transport layer
- application layer

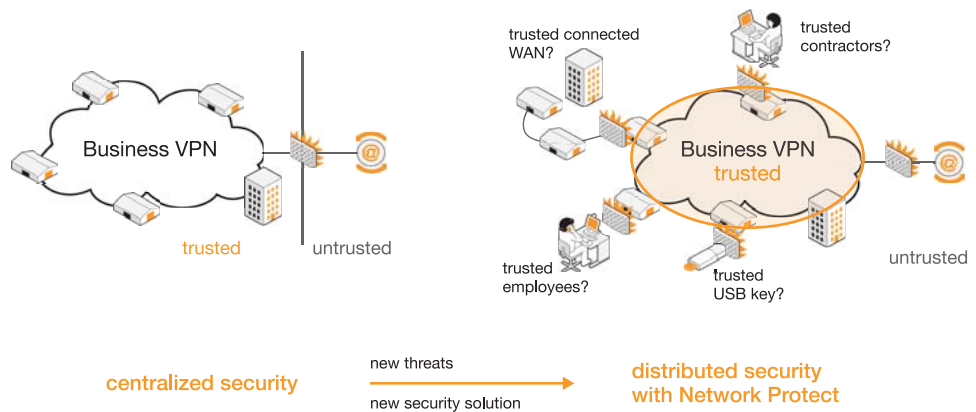
6 "Orange Business Services announces 'IP VPN Protected' for Remote Site Security" by Current Analysis, October 2007

For example, user authentication needs to be embedded within the application to control access to company resources. The level of accreditation needs to be automatically calculated based on the user's personal security level and the device and network from which he wishes to access the resource. End users might be able to access the accounting system from their desktop but not from a computer in an Internet café, for example.

The arrival of de-perimeterization in organizations means that the corporate network can no longer be considered a trusted zone. Security breaches don't just happen outside a nominal boundary that is protected by a firewall; they can happen just as easily inside. For this reason it is essential to embed security in the transport layer so that all communications within the organization are protected from security breaches. These embedded controls need to secure the company network from the gateway right down to the LAN at individual sites and need to be embedded directly in the router.

Embedded network controls are particularly important in distributed organizations with many small branch offices. While larger sites can rely on security staff to tune their protection, smaller sites with no internal resources need automated protection from threats emanating from the corporate network and from spreading threats originating at their own sites.

figure 1 – centralized security vs. distributed security



Our Network Protect service is a vital component of this security architecture and delivers must-have firewall and intrusion prevention (IPS) features. It is embedded in the network and features an automatic preventative device that protects a site from threats originating in the site and in the rest of the organization. Designed to protect smaller sites, Network Protect is an essential complement to larger perimeter security solutions, such as the firewall protecting the main Internet gateway.

Having security within the organization allows an enterprise to isolate selected security breaches to a single location or zone. This is vital in a de-perimeterized organization. For example, partners that may not have the same anti-virus

policy as your company could inadvertently introduce malware into an individual site. Having security within the transport level could stop this from spreading throughout the enterprise.

### managed security

Because Network Protect is a managed service, organizations are able to improve their level of security without increasing their management overhead. This is particularly important when using Network Protect at smaller sites that typically have few internal IT resources. By embedding consistent security devices across the organization, an enterprise can also benefit from reduced complexity and lower costs.

A managed service also allows an organization to focus its resources on the human aspects of security: delivering end-user training and improving security awareness throughout the organization. This includes educating staff on how social engineering is used to extract confidential information, the dangers of throwing away printed documents and best practices.

### richer picture

Network Protect can also contribute to creating a richer picture of the security status across the organization. Through information provided by multiple embedded devices, it is possible to spot trends and proactively prevent attacks. For example, if one site has been compromised, then all other sites can be updated to prevent it from happening to them.

This is possible through Security Event Management, a natural companion to Network Protect, which helps enterprises make sense of all the information being produced by all their security devices. Security Event Management provides a comprehensive view of IT security by consolidating and analyzing alarms collected from all sorts of IT assets, including everything from embedded security right through to the enterprise Internet firewall.

# business advantages of security

For too many businesses, security is still seen as merely an expense, when in fact good security offers many business advantages. Security must be seen as an essential element to growing the business. It not only protects but also enhances productivity by making sure the right people access the right resources at the right time, so that companies can be confident about the confidentiality, integrity and availability of their data and assets.

Security attacks can also be very expensive in terms of clean up, compliance, communication failures and damaged business reputation. Good security can prevent these from happening. By preventing unwanted traffic on the network, businesses can also enjoy better application performance and lower costs.

## comprehensive security services

Orange offers a full range of security services, ranging from embedded security through enterprise-level managed firewalls to security management products. All together they provide comprehensive security at all organizational levels.

- **Network Protect:** Designed for branch offices, this embedded managed security service is integrated into the router. It incorporates a firewall with flexible filtering rules and proactive intrusion detection/prevention that monitors incoming and outgoing traffic.
- **Unified Defense:** Unified Defense incorporates firewall, anti-virus and Web filtering in a single managed appliance. Additional options, such as high availability and user authentication, are also available. The service is based on a managed unified threat management (UTM) appliance from Fortinet.
- **Secure Gateway:** Our flagship managed security suite includes managed firewall, using either Check Point/Nokia or Juniper devices; managed anti-virus based on Trend Micro software; managed employee access, which delivers URL and content filtering based on Secure Computing's Webwasher suite; and cache management based on Bluecoat appliances.
- **Secure Authentication:** This fully-managed service provides secure authentication of users to a wide range of services. It is based on SecurID-ACE technology, a product of RSA Security.

### case study: keeping franchises secure with Network Protect

This Orange customer in France supplies equipment for surveyors through a nationwide branch network. Orange supplies an IP VPN that helps it interconnect its branch and remote sites. Nine new branches have recently been opened to bring the total number of sites to 20, which includes the head office. As the company's branch offices are franchises, it needed a way to ensure the security of the entire network. The company's CIO is not responsible for the branch sites, their local area networks or their security, even though they are connected to the company's WAN.

In order to protect the company and all the franchises from security threats coming from an unsecured site, the company deployed a Network Protect solution. It allows secure communications across the WAN without each franchise needing to procure or manage a separate security solution. The security solution is managed by Orange and is deployed along with the IP VPN. It provides the customer with the simple, cost-effective, predictable network and security that they need.

for more information, visit  
[www.orange-business.com](http://www.orange-business.com)

## regional offices

### Americas

Atlanta  
600 Galleria Parkway  
Atlanta, GA 30339  
USA  
Tel.: +1 866 849 4185

Washington, D.C.  
13775 McLearen Road  
Herndon, VA 20171  
USA  
Tel.: +1 866 849 4185

### Europe

Paris  
190, avenue de France  
75653 Paris Cedex 13  
France  
Tel.: +33 1 46 46 90 00

Slough  
Betjeman Place  
217 Bath Road  
Slough, SL1 4AA  
United Kingdom  
Tel.: +44 (0)20 8321 4000

### Asia Pacific

Singapore  
Block 750 Oasis  
Chai Chee Road #04-02  
Technopark @ Chai Chee  
Singapore 469000  
Tel.: +65 6 517 1000



Business  
Services

orange™