

White Paper

A Case for Unified Network Security Outsourcing

By: Dave Piscitello, President



Table of Contents

Introduction.....	1
Sourcing Considerations for MMEs.....	2
Defense in Depth and Outsourcing.....	3
The Virtela Communications “In Depth” Alternative.....	4,5
Virtela’s “Enforcement in Depth”	6, 7
Conclusion.....	7

Introduction

Mid market enterprises (MMEs), especially those with an international presence, are confronted with and often confounded by an intimidating set of security threats. Managing risk has become a top priority in these organizations but the number of vectors attackers employ today is large, diverse, increasingly sophisticated and multi-faceted. MMEs often do not have the budget and expertise to manage risk in Internet time. The enemy is at the gate, in the cities and strongholds, running rough shod along the highways and MME defenses are stretched to their limits.

This assessment may seem overly dramatic, but consider the issues risk management teams must address today. They must devise business and technical strategies to protect public web, e-commerce, and e-business from denial of service and application level attacks. They must consider “endpoint” strategies to maintain productivity in the face of spam, mail-borne viruses, spyware infestations, and unintentional loss of confidential information, not just for company-managed networks but also for mobile employees and teleworkers. Increasingly, they must comply with external requirements from regulatory agencies, supply chain partners and other business collaborative ventures.

Many MMEs struggle to prioritize the litany of requirements to maintain acceptable security, and do so within the compressed timeframes of an Internet-enabled world. Vulnerability awareness, policy definition, talent retention, and the design of mitigation tools must be carefully weighted and related to each other, budget approvals must be sought and solutions deployed. If an MME succeeds in these initiatives, there is still a struggle to manage risk while satisfying the demands of more resource intensive applications and the fatter “pipes” that they require. Factoring security into the performance equation is often more than the typical MME can handle, and security often succumbs when budgetary valuations pit expanded bandwidth against heightened security.

The result is frequently a “one or the other” mindset, and higher application performance is generally considered more valuable to a business than infrastructure security. This is a common conclusion, albeit somewhat misinformed. When implemented correctly, security becomes an asset rather than an expense. A strong security baseline makes an MME a more attractive company to potential business partners, especially those who maintain high security standards. Secure MMEs are more agile as well. Companies that competently manage security are consistently able to introduce new applications more quickly and with fewer difficulties. As part of a secure infrastructure, these applications can be easily and rapidly extended to business partners and clients, which improves collaboration and streamlines services. Highly secure environments tend to have a much more thorough understanding of their applications, and are better suited to accurately optimize performance.

Sourcing Considerations for MMEs

Given the range of threats, vulnerabilities and exposures, the expense of managing risk using in-house staff is difficult to pinpoint and hard to justify. Some MMEs make do with “near horizon” risk management. They treat security as a necessary evil, react to the most pressing concerns and defer less obvious, more expensive and labor intensive efforts for implementation only after current crises expire. Unfortunately, this generally results in perpetual firefighting as the cat and mouse game between hacker offense and IT defense progresses. In an effort to solicit the maximum perceived value from an investment, MMEs often employ security systems until or beyond the point where they are technologically obsolete, giving the hacker an upper hand. The same organization often adds bandwidth as network performance degrades, with modest or no investment in performance analysis. Few staff cycles are available for auditing, event analysis, or long term planning. The overall approach is more risk avoidance than risk management and rarely enhances business objectives. MMEs may see little or no return on their security investments and look to outsourcing as an opportunity to make security “someone else’s problem”.

Alternatively, there are MMEs who try to manage risk through thoughtful and long-term planning, but the difficulty of attracting and retaining security expertise can rapidly hinder those plans. Even if expertise were plentiful, each MME must manage the same set of risks as Fortune 500 companies, but with smaller budgets and resources. This is problematic when external factors force the reallocation of manpower against unexpected regulatory requirements or to recover from a security incident. Some long-term security and network expansion efforts may be deferred, while others may be deployed in an insecure manner. When this pattern persists, the security and performance objectives cannot be fully realized. Increasingly, even MMEs that understand the importance of risk management conclude that they cannot achieve business objectives at justifiable costs through in-house solutions.

The most obvious alternative is to outsource security to a network provider. This model is familiar to those accustomed to building a network by integrating WAN and Internet access from several local or regional service providers. Outsourcing security is something of an organic evolution for such MMEs as a simple extension of the network services already provided through a partner. It seems logical to outsource perimeter security (firewalls, intrusion prevention and antivirus gateway services) to the operators who provide broadband access.

Next in line is the choice of pure-play Managed Security Service Providers (MSSP) who offer premises-based security services. MSSP’s do not typically offer network connectivity and are highly focused on security solutions. MSSP’s are often considered as security requirements evolve, or as MME’s begin to recognize the benefits of higher quality security services.

A third conclusion is an outsourcing strategy with a “best of breed” mindset. MME’s may choose in-house IT for tasks that are less comfortable in outside hands, but use the enhanced tools and expertise of MSSP’s and network providers to enhance internal capabilities. IT departments then respond strictly to events of merit as they define, while their partners manage the more tedious and time-consuming efforts of general maintenance and event validation and qualification.

Defense in Depth and Outsourcing

Efficient, effective security management requires a unified defense in depth strategy that spans local (corporate LAN), WAN (corporate access and infrastructure), and extended enterprise access (partner, mobile and remote access) networks. Defense in depth is a multi-dimensional approach to security that is analogous to the military strategy of deploying multiple defense systems to protect an asset. For example, during conflicts the U.S. armed forces use radar, air support, destroyer and submarine escorts to create multiple perimeters of defense and diverse countermeasures to protect merchant fleets and troop movement. Today, Internet security measures are likewise deployed in layers using firewalls, network and host intrusion preventions systems, and application layer security gateways to combat denial of service attacks, spam, malicious code, and web-based attacks.

Defense in depth requires considerable monitoring, correlation, and coordination across multiple tools with varying levels of administrative scope. Several factors combine to make MMEs less agile or capable to combat the full range of threats they face. The first being an MME's network and security administration is rarely as tightly integrated as a dedicated security entity or network provider. Internally, divisions within an MME may manage voice and data networks and network security separately. Branch offices may independently contract with local bandwidth providers, and outsource parts or all of their security dependent upon local expertise (or lack thereof). Often smaller offices have no IT staffing and are entirely dependent upon corporate support for both network and security. This scenario is far more likely to leave unprotected local resources that allow an easy point of entry into the main network.

Even in the best arrangements, defining roles and accountability across multiple parties adds complexity and decreases the likelihood that security is uniformly implemented. When variations exist in the security posture of different locations, security of the whole can be compromised. Organizations with multi-party outsourcing arrangements cannot easily dictate the types and amount of security and performance information to be collected by each party, whether and how that information is aggregated, and how frequently it is collected. In some cases, MMEs discover event data for their own networks is not distinguished nor easily separated from other organizations served by the provider.

Splicing data to gain insight into performance and security events may be similar to constructing a jigsaw puzzle where some of the pieces are missing. Consider the scenario where a branch office contracts with a local network access provider, a different security services company for firewall management, and uses internal resources for intra-company routing and Virtual Private Networking(VPN). Four interdependent services are now managed by three separate parties in support of a single branch location. Synchronizing these activities can rapidly become a challenge. That challenge is increased by orders of magnitude if the practice is repeated across multiple international locations; especially with regulatory issues and export constraints.

Hidden costs begin to emerge from such scenarios. An MME must invest time and talent to interpret and correlate events from separately administered security systems and network elements. The organization discovers that the event data is not easily correlated across independently managed elements allowing incidents to be missed. The MME may wind up investing substantial time, effort and expense only to see its risk profile shift rather than improve.

An alternative approach is to consider “sole sourcing” network security solutions through a provider whose defense in depth allows MMEs to cost effectively

- Outsource all security services, including campus, WAN, and remote access networks, to one global integrator
- Direct policy implementation through a single, well defined chain of command with minimal authoritative points of contact
- Employ best in class technology and expertise
- Avoid technology investment and obsolescence
- Manage network security, availability, and quality to meet business objectives.

Virtela Communications delivers a Defense in Depth alternative that can satisfy MMEs who want to outsource but avoid the aforementioned pitfalls. Virtela accomplishes this unique feat by extending its exclusive and successful “Super-Integrator” network services model with a comprehensive suite of managed security services.

The Virtela Communications’ “In Depth” Alternative

Virtela Communications is among today’s most successful global virtual network operators (VNOs). Virtela introduced a full suite of managed security services within its portfolio of WAN, remote access, IP data, and IP voice and video services. Virtela provides security in depth delivered over its Global Service Fabricsm through the use of carefully selected and strategically placed best of breed technology. Virtela has relationships with carrier networks in over 190 countries, aggregating and integrating access and WAN services from over 250 network providers to form a global network that serves over 5000 access points worldwide. Virtela’s intelligent routing overlay assures IP traffic is efficiently routed within a network that is optimized to meet stringent availability and service quality requirements.

Virtela’s Global Service Fabricsm offers benefits on multiple levels. Once service level requirements are defined, Virtela designs the network, negotiates and acquires access, configures the equipment, and maintains end-to end operations from Regional Policy Centers (RPC) that assure availability and service quality needs are satisfied. Virtela is the sole business and technical contact. This aspect alone distinguishes Virtela’s approach from multi-provider solutions. However, having Virtela choose cost effective access services and equipment on its customers’ behalf ensures favorable pricing and avoids the contract negotiation hassles inherent in dealing with multiple, and potentially international, providers.

What is a VNO?

Forrester Research defines a global virtual network operator (VNO) as “a managed network services provider whose main business is designing customer-specific network solutions. VNOs also manage network and service contracts on behalf of enterprise customers that include data and converged IP services across multiple geographic regins, and may include foreign local circuits. The VNO aggregates, translates and flattens the diverse management aspects of individual network services to a single contract with a customer centric SLA... (from Global VNOs Are In Your Future 11 Nov 2005).

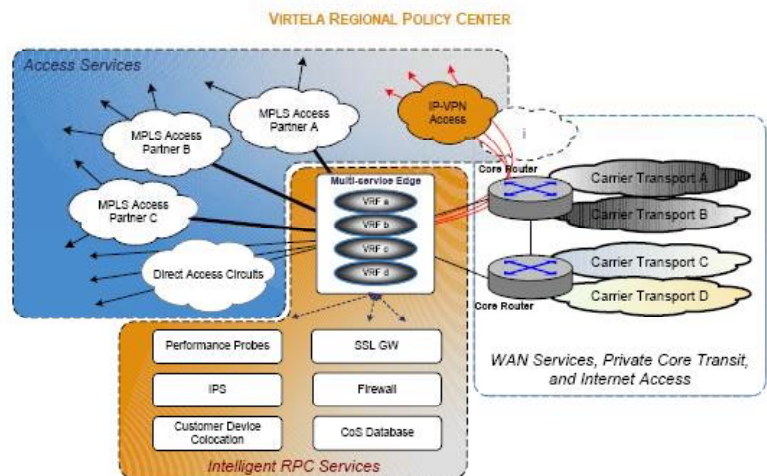
Virtela Security policies and enforcement are based upon Customer-Defined requirements and security industry best-practices.. The customer determines how events should be treated, who to contact, and when - Virtela ensures that it is accurately enforced. Offering a comprehensive suite of security services, inclusive of vulnerability assessments, email and web browsing protection, multi-level premise and network-based intrusion prevention and firewalls, server, router, and switch security monitoring, and VPN connectivity, Virtela has a complete suite of both connectivity and security service solutions. A company that wishes to avails itself of all these security services can maintain their defined policies throughout every internal and external network extension.

As opposed to security outsourcing providers who base their offerings exclusively on premises-based functionality. Virtela sees merit in employing premise, shared network and hybrid alternatives. Virtela can:

- Dedicate and monitor devices on the customer premises to support firewall, real time intrusion detection and prevention and DDOS mitigation.
- Provide network based security services using virtualized or shared systems collocated in Regional Policy Centers (see sidebar), to provide Firewall, IPS, SSL, and site to site VPN.
- Dedicate customer equipment within RPC's for the exclusive protection of a single customer, yet extending the protection of that single device to multiple customer locations.
- Proactively monitor all of these systems through an integrated infrastructure that constructs a complete and comprehensive picture of network and security activity.

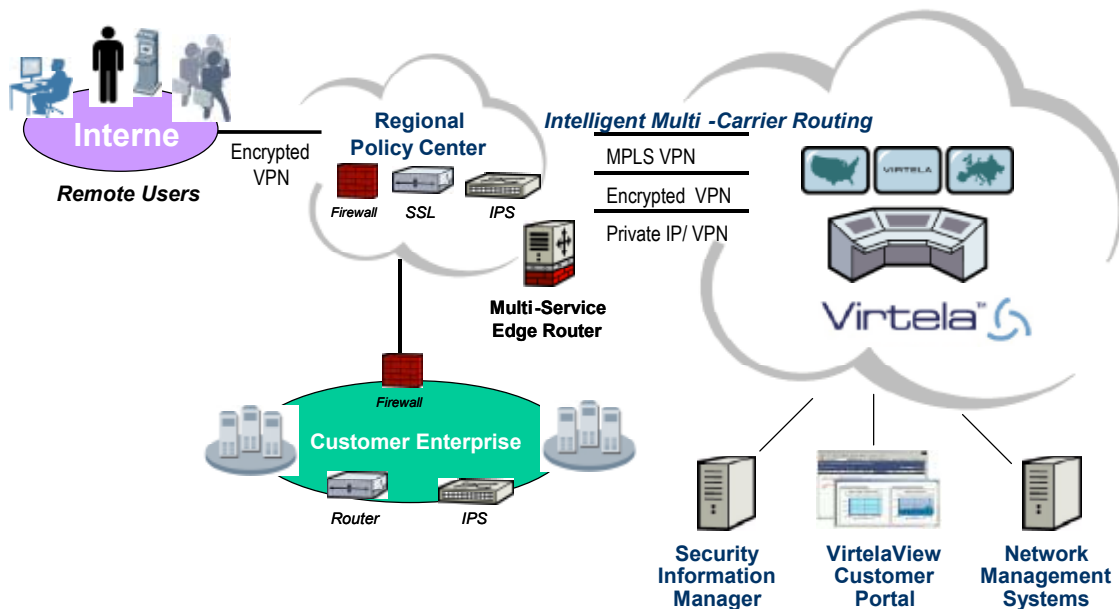
Inside a Regional Policy Center

Virtela manages network and security services from physically secured, strategically located Regional Policy Centers (RPCs) located throughout the world. These centers house core network elements, virtualized and network based service platforms for security services, as well as management and monitoring platforms. Virtela's RPCs provide more redundant and highly available operations than MMEs could afford to deploy.



Virtela's goal in all deployment scenarios is to offer "clean pipes" – secure channels between secure endpoints (client and server), over LAN as well as WAN. Virtela is better positioned to offer such enforcement in depth than any other outsourcing arrangement available today. Configuration management, event monitoring, analysis and response are centrally managed by Virtela alone, assuring a single, well-defined chain of command that cannot be duplicated through arrangements made with multiple MSSPs and carriers. A "Super carrier" can offer managed security services over its own network fabric but only Virtela's Global Service Fabric(sm) eliminates the dependence on a single carrier. And no single carrier extends services to all locations with all the services required for most companies.

Virtela's "Enforcement in Depth"



The security information obtained through device monitoring is hard knowledge. Hard knowledge is the actual output of the device, generated through syslog or SNMP reporting. To make the most of hard knowledge, it must be complemented with soft knowledge. Soft knowledge includes an understanding of the surrounding environment, the assigned value of various assets, the user community, and the general performance history and expectations of network segments. Hard knowledge, when combined with soft knowledge allows a distinction between anomalies and threats. It drastically reduces false positives, which reduces the chances of a midnight call over non-issues. Something of very high value to any IT staff.

The security information obtained through device monitoring is hard knowledge. Hard knowledge is the actual output of the device, generated through syslog or SNMP reporting. To make the most of hard knowledge, it must be complemented with soft knowledge. Soft knowledge includes an understanding of the surrounding environment, the assigned value of various assets, the user community, and the general performance history and expectations of network segments. Hard knowledge, when combined with soft knowledge allows a distinction between anomalies and threats. It drastically reduces false positives, which reduces the chances of a midnight call over non-issues. Something of very high value to any IT staff.

What is Security Information Management (SIM)?

- Security focused network data aggregation and integration platform
- Intelligent correlation of individual device metrics, syslogs, performance and baselines
- Cross-platform correlation of multiple devices across various vendor platforms
- Deeply enhanced knowledge of security events and network performance
- Applies asset valuations within risk assessments

The power of the best-in-breed technology, the collection and correlation of a multitude of events, and the evaluation inclusive of hard & soft knowledge is possible through Virtela's tailored back-office systems and Security Information Management (SIM, see sidebar) platform. Do-It-Yourself (DIY) and multi-vendor solutions generally cannot attain equivalent performance and security information in a timely enough manner to assess and respond to real-time (zero-day) threats. Through these tools, Virtela is positioned to rapidly catch zero-day events. These events are monitored intently to evaluate if action must be taken before a new vulnerability is exploited. Other solutions simply cannot access the volume of security and performance data with enough time to identify and react to real-time (zero-day) threats.

Every organization needs expert staff that can design and implement well defined operational practices and cope with today's demanding security landscape. Network and security operations centers (NOC/SOC) must have extensive experience with Internet Security in general: on average, Virtela's NOC/SOC staff at Virtela has an impressive nine years experience in Tier 2/3 support. Organizations that incorporate equipment from many vendors as part of its best-of-breed solution must also be intimately familiar with a wide range of security technology and applications: Virtela's NOC/SOC staff maintain hands-on training and certification across a broad range of vendors with whom Virtela maintains partner-level status, including CheckPoint, Cisco Systems, F5, Juniper Networks, Nortel, and TippingPoint technologies. Finally, organizations must have sufficient technical staff to handle the administrative load: sixty-five percent (65%) of Virtela's employees perform technical support roles that directly or indirectly touching it customers to assure that knowledgeable and accountable staff are available 24x7.

Virtela's ability to "virtualize" expert staff offers expertise in depth. Few MMEs can justify the cost of hiring the diverse expertise available through Virtela's VNO model. In multi-provider scenarios, the expertise might be available, but coordination efforts skyrocket, and facilitating communications between parties is frequently a challenge, if possible at all. Customers of multi-provider solutions often must retain more expert staff than originally expected just to manage their service providers.

Services, enforcement, information, and expertise in depth distinguish Virtela's Secure Network solutions for MMEs from other outsourcing alternatives.

Conclusion

Gartner, Forrester Research, and other key analyst firms praise Virtela Communications for its ability to combine the best characteristics of a global VNO and facilities based carrier and operate as a "Super-Integrator". By extending the Super-Integrator model to include a comprehensive set of security services, Virtela again distinguishes itself among VNOs as a global sole source provider of secure networking solutions.

About Core Competence

Core Competence provides Internet, broadband, security, and wireless LAN consulting services from offices in Pennsylvania and South Carolina. Our staff are respected and widely published experts in routed and switched internetworking; wireless LANs and WANs; 802.11 WLAN security; secure remote access and VPNs; firewalls, IDS, IPS; network and system security architecture and design. Core Competence received a fee for the preparation of this industry report.