INFRASTRUCTURE AND MANAGEMENT:
FOCUS OF BUSINESS CRITICAL INTERNET SECURITY

A WHITE PAPER

ZONA
RESEARCH INC

By
Zona Research, Inc.
June 1999

INFRASTRUCTURE AND MANAGEMENT:
FOCUS OF BUSINESS CRITICAL INTERNET SECURITY

Abstract: *Less than a decade ago, the Internet was known only to a relatively small number of participants, many of who knew each other well. In the early 1990s, security technology on the nascent Internet was largely nonexistent among the academic computers that composed a large part of the publicly available network. As part of its evolution, the Internet and Intranet have been extended out to partners, customers, suppliers and the general public. This extended Intranet is playing an increasingly critical role in what Zona has dubbed the Business Critical Intranet (BCI). In this paper, we will examine the dynamics of the ever changing and sometimes-inconsistent demands on security systems triggered by the rapid growth of the Internet and BCIs.*

TABLE OF CONTENTS

Without Blueprints, or a Net 5
It Wasn't All That Long Ago… 5
Pulled in Both Directions 7
Threat-By-Threat Deployment 8
The Next Generation 10
Some Approaches to Holistic Security 10
- Check Point's OPSEC 11
- Network Associates Event Orchestrator 11
- Pilot Network Services 12
- IBM's FirstSecure 13

Conclusion 14

Without Blueprints, or a Net

The Winchester Mystery house, located in San Jose, California, is a tourist attraction due to its unique construction. The house began as an 8-room farmhouse in 1884. For the next 38 years until 1922, the house's owner went on a building binge without rhyme or reason.

This feverish, non-stop construction was the product of fear. The house's owner, Mrs. Sarah Winchester, was the heir to the Winchester rifle fortune. When her husband died, Mrs. Winchester consulted a spiritual medium that informed her that her late husband was taken by the angry spirits of those killed by Winchester rifles during the country's westward expansion. The medium also told Mrs. Winchester her life was next.

The medium told Mrs. Winchester she must build a home to house these angry spirits if she did not want to join her husband. So build she did. And apparently, it worked—at least for 38 years.

During that time, Mrs. Winchester added more than 150 rooms to the house, with hundreds of doors and windows, dozens of fireplaces and a handful of kitchens. The house was built out in a haphazard way, with no blueprints of any sort. Stairways were built that led to nowhere; doors were added that opened on bare walls. Whatever Mrs. Winchester thought the evil spirits wanted, she built. As long as she built new rooms, the spirits would be appeased.

The original, tidy eight-room farmhouse disappeared into the confusion that became the Winchester Mystery house. Since no blueprints existed, there was no real way to map or organize the house. It was a mishmash of plumbing and electrical wiring. If something broke, it had to be found by means of a room-to-room search. Directions to a place in the house were all but impossible. Sending someone unfamiliar with the home meant that they were certain to become lost in a maze of disorganized hallways, rooms and stairways. Only a builder, a long-time servant or Mrs. Winchester herself would have the knowledge to make his way around the house without consistently getting lost.

Which brings us to enterprise network security issues at the close of the 20th Century.

It Wasn't All That Long Ago…

Internet security products have come a substantial way since the early days of the Internet. Less than a decade ago, the Internet was known only to a relatively small number of participants, many of whom knew each other well. In the early 1990s, security technology on the nascent Internet was largely nonexistent among the academic computers that composed a large part of the publicly available network.

The debate surrounding security in the early 1990's seems almost quaint less than ten years later. Many academics argued against even the most rudimentary security measures, instead advocating open access for anyone with interest in the computers and the networks that connected them. Even simple passwords for accounts were frowned on by many.

The early Internet was not a commercial environment. Nor was it a means by which businesses bought and sold materials or products. Most companies had little or no Internet presence, and furthermore, information available in computers attached to this network was not of high commercial value. The demand for extensive security infrastructure was soft.

Fast forward to the present. Millions of people are online, with more expected every day. Internet usage is becoming mainstream at both work and home as Internet access begins the trek toward becoming as ubiquitous as telephone service. At both work and home, life is becoming increasingly difficult without Internet access.

The growth of the Internet might best be measured by the stratospheric growth seen in the enterprise deployment of IP networks in the past five years. These Intranets are not only multiplying across divisions within enterprises, they grow more complex each day. In fact, the only apparent constant in the deployment of an Intranet is the constancy of the deployment.

The more advanced Intranet is deployed not only to serve internal needs. As part of its evolution, the Intranet has been extended out to partners, customers, suppliers and the general public. This extended Intranet is playing an increasingly critical role in what Zona has dubbed the Business Critical Intranet (BCI).

The Business Critical Intranet is an increasingly complex network and presents an ever-changing array of challenges for network managers. It includes supply chain management, electronic commerce and a whole spectrum of activities between the enterprise and its customers, partners, suppliers and the general public. In this environment, the effort to maintain appropriate levels of security can pose a difficult and complex series of decisions for the network manager.

In many cases, the IT manager has responded to the diverse requirements of the BCI by creating and filling out a shopping list of best of breed point products. In doing so, the IT manager was creating a shopping list of measures intended to meet so-called security "requirements." Deploying this shopping list of products was in large part more about job security than network security.

The demands of the BCI are pulling IT managers in opposite directions. As the extended Intranet becomes a more substantial part of BCI, it creates the potential for multiple security vulnerabilities. On one hand, greater access to the Internet and suppliers, customers and partners creates a wider range of potential hostile visitors.

On the other hand, the information exposed throughout the BCI may have much higher value, as it is being used by suppliers and partners. Not only is the information available more sensitive and strategic, opportunities for unauthorized access increase with the addition of each new partner, customer or supplier.

In short, a higher number of possible thieves can steal ever-increasing value stored on the BCI.

Chart 1 highlights the demands being placed on IT managers by the Business Critical Intranet.

IS Demand	Behind the Demand
Security and network management must be integrated	The network manager wants control across the range of applications deployed on the BCI
The BCI must leverage existing resources, within the context of the newer IP network	These applications must all communicate with one another – they must interoperate now
The BCI must integrate with new or yet-to-be-deployed applications and maintain interoperability	For security products, this means that virus-scanning software must work with firewalls, firewalls must work with remote access, and so on

Pulled in Both Directions

Studies conducted by Zona Research indicate the depth that IT managers are being pulled in opposite directions by the demands of the BCI. On one hand, demands for greater access are being made on IT managers from the executive suite who would like to open up the BCI as an extended Intranet to customers, suppliers, partners and the like.

On the other hand, IT is being asked to ensure the security of the data stored on the network itself. Zona's studies show that IT managers are attempting to clamp down on information access. In one study, Zona asked a series of six high-level questions related to security and information access in order to gauge general trends and attitudes among enterprise network managers.

More than three-quarters of our sample disagreed or strongly disagreed that their information access policy is free and open. Our respondents are keenly aware of security issues and are deploying security technology to limit access.

Similarly, nearly two-thirds of our sample indicated information on their networks is centrally controlled, more than twice the number that indicated information was managed in a decentralized way.

With respect to policy changes, nearly two-thirds of our respondents indicated their information access policies had become less open in the last year, in sharp contrast to those (less than 25%) that had made information more open during the same period. At the same time, an overwhelming majority stated their information access policies would become less open in the coming 12 months. This is a margin of more than three-to-one over those expecting information access policies to become more open. From this we conclude the desire to control access to information is a trend that will continue into the foreseeable future.

At the same time, network managers report that they continue extending the network, which in turn will make its management even more difficult. Nearly 9 out of 10 respondents indicated they would be expanding access to the Internet, more than 14 times the number not doing so. In addition, 70% indicated they would be expanding their BCIs and the extended Intranet portion of the BCI. Clearly, networks are not static but growing and changing, which means the IT manager continually faces a new series of challenges. Security requirements, as a reflection of the network itself, must also change over time. In this dynamic network environment, flexible, scalable security is of great value.

Maintaining tight control on information access while simultaneously extending the network outward are by definition conflicting goals. One cannot simply lock down the network and at the same time grant Internet connectivity or communicate with partners and customers over an Extended Intranet. Nor can one provide security while allowing free access to data. IT managers routinely face these situations in managing the Business Critical Intranet.

Threat-By-Threat Deployment

Studies conducted by Zona Research also confirm the threat-by-threat deployment of security technology in response to the desire for increased control of information in an increasingly hostile environment. While nearly two-thirds of respondents indicated that they expected their security budgets to increase in the coming years, the same respondents indicate different levels of security technology deployment.

First in the door and nearly ubiquitous is anti-virus technology. More than 80 percent of those surveyed indicated that they had deployed one or more anti-virus products in an effort to protect their BCI. In most cases, the IT departments decided that redundancy was valuable. Like Mrs. Winchester and her multiple kitchens, the IT departments decided that better security could be had by running both McAfee and Norton anti-virus products simultaneously.

The same respondents also had fairly high percentages of access control technologies. This category is broad in definition and can range from merely deploying passwords on desktops to simply denying whole parts of the enterprise access to internal or external data. Access control can be difficult to scale, and can leave large numbers of both Intranet and extended Intranet clients without access to key information on the BCI.

Firewalls also enjoy substantial penetration in the growing BCI market, with companies deploying one or more brands. We believe in many cases, multiple firewall brand deployments merely provide the facade of security, while offering little in the way of hostile event prevention.

Zona's studies illustrated that high percentages of IT professionals will continue making security purchases well into the future, with firewalls, intrusion detection, authentication, encryption and digital signature technology all on the shopping list. IT departments, like Mrs. Winchester, obviously feel they must build, build, and build to keep the evil spirits away.

Products like firewalls, anti-virus software, encryption, and access control among others have responded to threats as those threats have made themselves widely known. Those products are regularly updated or improved incrementally, and the vendors of these products promise upgrades and improvements on a regular basis. Regardless of the improvements, these products largely remain as point products with greater applicability to an Internet environment that did not include the Business Critical Intranet. The BCI requires a fluid, coordinated security environment that allows IT to deploy security in a coordinated, coherent fashion.

This "threat by threat" response to security concerns does not address the problems posed by the ever-evolving BCI. Like Mrs. Winchester, IT managers have built out their security in an ad hoc fashion. A firewall here, anti-virus software there, authentication somewhere over here and encryption scattered about. Also, like Mrs. Winchester, IT managers have deployed security technologies without a blueprint, and navigating an ad hoc security framework presents much the same challenge as that to a visitor of the Winchester Mystery House.

The Next Generation

Providing interactive security has proven to be a challenge in an environment populated by a wide variety of point security products. The next generation of Internet security will require a more holistic approach that allows network administrators to oversee and manage a security framework centrally.

To date, the Internet security market has not seen vendors offering this holistic approach. Largely, the Internet security vendors have formed interoperability alliances and vowed to make products work with each other. Such offerings do not resolve the challenges of the enterprise network manager.

We believe that the next real breakthrough in BCI security will come in the form of an infrastructure through which various point security products can be deployed and managed. Not only will this approach bring coherency to security deployment, it will eliminate the urge to redundantly deploy various security technologies as evidenced by Zona's market studies.

We also foresee security technology as an enabler of the many facets of the Business Critical Intranet. The old security objective of "keeping the bad guys out" must evolve to a new objective that also includes "letting the good guys in." To support that new objective, security frameworks must move away from the disjointed, threat-by-threat response to security concerns. In a more integrated environment, security is an enabling and proactive technology, not a reactive cash sink. Security should enable opportunities for the Business Critical Intranet.

Some Approaches to Holistic Security

A number of different strategies are being deployed to address the security concerns brought on by the growing maturity of the Business Critical Intranet. In this section, we will examine a few of these strategies, services and products.

In each case, the thrust of the effort is to move away from Mrs. Winchester's model of construction to a more centrally managed and planned environment. Simply stated, the goal is to provide a security framework more in line with the demands of the Business Critical Intranet.

We have chosen a broad spectrum of approaches to give an overall impression of the markets demands and attempts to meet that demand. Each of the four examples below has unique strengths and weaknesses.

Check Point’s OPSEC

One of the first strategies to emerge in the face of ad hoc security deployment was the security vendor alliance. The most notable example of this strategy is Check Point Software’s Open Platform for Secure Enterprise Connectivity (OPSEC) Alliance.

Check Point formed OPSEC in an effort to “integrate and manage all aspects of network security through an open extensible management framework.” To this end, the company provided a software development kit to “better enable the integration of these security system components with” Check Point products, including firewalls.

This approach makes a great deal of sense for many IT organizations when one considers that firewalls are seen as the foundation of enterprise security deployments. While a firewall alone is no security guarantee, it is a starting point that few enterprise security managers wish to skip. For this reason, drawing a circle of promised security product interoperability around the firewall makes sense.

Check Point, of course, hopes to put itself in the middle of this multi-vendor initiative based on its product's position as an absolute security requirement. Check Point’s leading position in the firewall market also gives the company the credibility it needs to establish this alliance.

Such alliances, however, are just that – voluntary agreements to promise to do something. While many of Check Point’s OPSEC partners – like IBM, Bay Networks, HP and the like – have bundled Check Point products in their own offerings, the voluntary agreement to inter-operate is enforced by the mutually beneficial nature of the relationship. When these vendors find other partners or approaches to a holistic security offering, OPSEC may sag under its voluntary nature. While we believe that such an initiative is a step in the right direction and was groundbreaking when first announced, we maintain that more formal technology integration will be the wave of the future. In short, IT managers will need more reassurance than multi-vendor promises of inter-operability.

Network Associates Event Orchestrator

Network Associates – a well-known provider of a wide range of security products – has recognized the need for a more holistic approach towards its own suite of security products. While the company gained some clear advantages offering a suite of products to its channel, IT managers were faced with many of the same problems created with multiple-vendor deployments of security products.

Event Orchestrator is a software product that allows IT managers to coordinate and manage their various and sundry security products. Not only does the product offer to reduce the number of management consoles an IT manager must monitor, it is designed to allow IT to more aggressively manage its security architecture.

For example, Event Orchestrator can note how a change in a firewall will affect an anti-virus module. Event Orchestrator can also be used to create trouble tickets for the IT desk when, for example, an intruder is detected. This product can also automate many of the responses to hostile activities, including closing ports, isolating subnets and the like.

Event Orchestrator maintains its own security by running authentication checks between itself and the various components of the Intranet security architecture. In this way, it assures that alerts and events are actually coming from the various security components and not from a spoofed attack.

Event Orchestrator is designed to offer a certain level of security product integration without being a full-blown network management infrastructure like a Tivoli or OpenView. While not attempting to replicate those network infrastructure products, Event Orchestrator does offer a “plug and play” environment to connect various security products to each other and a central policy management console. Event Orchestrator does allow third party software to be incorporated into the holistic security environment.

We believe the Event Orchestrator is a significant step toward a more unified and coherent security framework within the Business Critical Intranet.

Pilot Network Services

Yet another approach to providing a holistic security environment would come from outsourced solutions. Enterprises wishing to escape the hassles and vulnerabilities associated with managing and configuring a variety of security products could simply allow a third party with some experience in this area to take over the management of their security infrastructure.

A very good example of such a solution would be Pilot Network Services. PNS offers its customers secure environments behind the company’s Heuristic Defense Infrastructure, which features “multi-layer filtering, application gateways and proxy services with proprietary deterrence and defense techniques.”

PNS positions itself as “the Security Utility,” offering subscription-based security services. PNS offers 24-hour a day, 7-days-a-week Internet connectivity with security monitoring and reporting as well as hosting services for Web, FTP and News servers. The company also offers secure telecommuting, authentication and encryption, Web filtering and virus scanning as well as Corporate Partner Privacy programs for enterprises seeking to do business with clients not using PNS services.

PNS has four major Network Service Centers in the U.S., it offers services to a host of high-profile media, high technology, financial and industrial customers who have decided that outsourcing security infrastructure is a reasonable way to approach the problem.

We believe Pilot's model is a viable one, and the expertise the company brings to its customers offers a real value proposition. Significant numbers of Fortune 5000 companies will, we believe, seek outsourced solutions to the problems of ad hoc security deployment. At the same time, however, the remainder may attempt to create secure environments on their own. For these enterprises, an outsourced solution is not an option.

IBM's FirstSecure

IBM has also recognized the need for a more holistic security solution and has approached the problem from the perspective of a systems provider with a series of both product and service offerings that will provide an infrastructure on top of which various security point products can be deployed, integrated, and managed. IBM's FirstSecure is a standards-based, policy-driven security solution designed to address companies' security concerns as they deploy Business Critical Intranets.

FirstSecure is composed of five product components, the central product being the Security Policy Director. The SecureWay Policy Director will define and implement policy across each of the security components. Release 1 focuses on managing access control for web-based (e.g. BCI) applications. Future releases will enable third party security software integration, allowing enterprises to leverage existing security technology investments.

Another key component is the SecureWay Boundary Server, which provides protection for internet-based business transactions through the use of firewall and content filtering technologies. In addition, FirstSecure includes a public key infrastructure (PKI) component that provides a trusted environment that supports key e-business activities by enabling companies to register new e-business entities on-line, and to issue and manage certificates.

First Secure also includes intrusion detection and protection against a broad range of security exposures. In Release 1 this function is provided by Norton AntiVirus/IBM Solution Suite. A Software Development Kit is also included.

FirstSecure includes technology from IBM and other leading security vendors such as Finjan, Content Technologies, RSA, Security Dynamics, Symantec, and Intel. The FirstSecure components are based on industry standards and have been tested together by IBM. Additionally, IBM support is provided for the entire solution, that is, all product components are supported.

IBM’s SecureWay Policy Director is the technology underlying its holistic approach to BCI security. While IBM provides key point products for this infrastructure, as the Policy Director and its programming interfaces (APIs) evolve and are publicized, other vendors products can be enabled to be deployed within the infrastructure. We believe such flexibility will be key to IT managers, especially those who have invested heavily in non-IBM point products to date.

The Policy Director will allow the IT manager to apply policy-based responses to various security events such as firewall alerts, intrusions or anti-virus alerts. In doing so, it allows the IT department to coordinate the various facets of the security infrastructure, giving the IT manager the flexibility necessary to securely manage the Business Critical Intranet.

We believe that IBM’s services organization (IBM Global Services), combined with its First Secure products will give it a leg up on competition which cannot demonstrate a global service network. Regardless of the level of automation built into the next generation of Internet security products, consulting and services will still be a key component of any successful security infrastructure on the Business Critical Intranet. Furthermore, future integration of the FirstSecure product line into the Tivoli network management software will make an even more compelling product to many IT managers.

For large enterprises with sizable investments in both network and security technology, on their existing BCI, the IBM offering can provide more powerful leverage opportunity. Such advantages will be substantial, especially in those BCIs that are mature and actively participating in electronic commerce in all of its facets.

Deploying IBM’s FirstSecure solution offers the Internet-savvy enterprise the opportunity to address the problems of its ad hoc security environment in a comprehensive fashion. We believe that IBM’s comprehensive approach to security is, in fact, how secure networks will be deployed in the future.

Conclusion

As the 20th century draws to a close, a modern, scientific man stands poised to connect every person to every other person on the planet. Communications and technology advances made in the last 50 years would truly appear as magic to those of just a few generations ago. Like Sarah Winchester, perhaps.

We suspect, however, that Mrs. Winchester would recognize some behavior still found on the eve of the millennium. One such behavior would be that found in many, if not most IT manager when it comes to security. Just as Mrs. Winchester built and added on to her home in a willy-nilly fashion to ward off evil spirits, so too is the IT manager slapping together a ramshackle security infrastructure to ward off threats, both real and perceived.

Zona Research firmly believes that the next wave of Business Critical Intranet security deployments will have a much more substantial focus on infrastructure and management. Not only will security products have to work in harmony with each other, they will have to be manageable from a central location with the capability of autonomously adjusting to changing security conditions.

Any enterprise seeking to provide itself, its customers, suppliers and partners a safe yet useful environment on which to operate a Business Critical Intranet will need to consider the investment in security infrastructure. Without such an investment, the IT manager, like Mrs. Winchester, could be building forever.

Zona Research, Inc.
Web: www.zonaresearch.com
Email: info@zonaresearch.com

Headquarters
900 Veterans Blvd, Suite 500
Redwood City, CA 94063
V: 415.568.5700
F: 415.306.2420

European Office
P.O. Box 7817
London SW12 8XL
V: +44.0181.675.7588
F: +44.0181.675.7589