VeriSign®

WHITE PAPER

Intelligent Infrastructure for Security

Where it all comes together.™

WHITE PAPER

CONTENTS

Where it all comes together.™

Intelligent Infrastructure for Security

In today's rapidly expanding digital environment, organizations are increasingly leveraging the Internet to streamline their operations, share critical information, and interact with their customers and partners.

+ Executive Summary

In the 21st century, online activity has increased exponentially, as organizations have grown increasingly reliant on the Internet for collaboration and commerce, and as people all over the world are accessing online services using a growing number of devices including PDAs and cell phones. However, this increased usage has been accompanied by a significant growth in the scope and complexity of network threats. To remain protected against these emerging, multifaceted threats, organizations cannot solely rely on individual point solutions, as ensuring their intercompatibility can be both costly and inefficient. In addition, organizations need extensive visibility into emerging threats, in order to prioritize remediation efforts, and they need to be able to use a wide variety of security credentials, such as tokens, smartcards, and certificates. This paper discusses the importance of leveraging intelligent infrastructure to provide security services that offer vigilant intelligence monitoring, robust threat prioritization, seamless interoperability, and the ability to immediately respond to crises 24/7.

+ The Transformation of Business Communications

In today's rapidly expanding digital environment, organizations are increasingly leveraging the Internet to streamline their operations, share critical information, and interact with their customers and partners. For example, in 2001 there were an average of 600 million authoritative Domain Name System (DNS) queries a day, involving .com or .net top-level domain names,[1] whereas in the second quarter of 2006 there have been as many as 18 billion a day.[2] IDC estimates that by the end of 2006, approximately 60 billion emails will be sent on a daily basis.[3]

In addition, organizations are expanding their networks for increased levels of remote accessibility. A 2006 study by Edison Media Research found that 81% of American consumers have access to the Internet from any location, and one in ten affluent Americans carries a wireless email device.[4] Already, organizations are responding to this trend; a survey by TechRepublic found that nearly 75% of organizations are enabling their business applications to be accessed remotely to varying degrees, while roughly 20% currently provide remote access for all of their business applications.[5] For many companies, remaining competitive and successful necessitates the shift towards comprehensive remote accessibility.

[1] Authoritative DNS queries are conducted between name servers and root DNS servers, when name servers are unable to resolve local DNS queries; each local DNS query represents a discrete domain-name activity, such as a requested Web page or delivered email. It would be unfeasible to aggregate data from the world's name servers, since they are too numerous, but authoritative DNS queries provide a useful barometer of global Internet traffic.

[2] Source: VeriSign, Inc.

[3] *Worldwide Email Usage Forecast, 2002-2006: Know What's Coming Your Way* (IDC #27975), IDC.

[4] *Internet and Multimedia 2005: "The On-Demand Media Consumer,"* ©2005 Arbitron/Edison Media Research

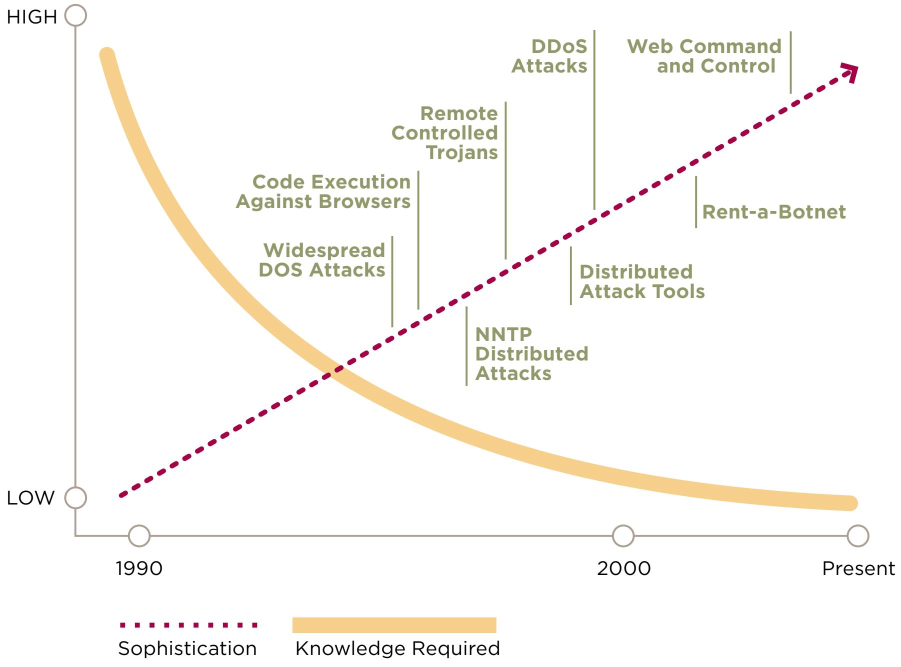
[5] *Enabling the Mobile Workforce: Trends and Issues,* ©2006 TechRepublic

Attacks targeting domain-name servers are growing increasingly complex, as hackers routinely increase the scope and severity of their assaults.

However, this expansion in the number and kind of devices accessing corporate networks is being accompanied by a rapid acceleration in the rate at which security threats evolve and emerge. A 2005 analysis conducted by VeriSign® iDefense® Labs found that attacks targeting domain-name servers were growing increasingly complex, as hackers routinely increased the scope and severity of their assaults, such as a coordinated attack in 2005 where hackers leveraged multiple servers around the world to corrupt more than 2000 DNS servers.[6] In 2002, the term "blended threat" was coined to describe the rare security threats which utilized multiple methods of entry and transmission; today, such attacks are so common that classifying them separately is no longer necessary.[7]

More alarmingly, the level of expertise required to engineer complex attacks is actually decreasing, as malicious code becomes increasingly available online and hackers sell their services for financial profit. Distributed denial-of-service (DDoS) attacks, potentially the largest and most costly threat facing technology-dependent companies, are increasingly perpetrated by purchased code or through automated "bots" which carry out the attack on their own; such attacks are also becoming increasingly sophisticated (See Figure 1). Scams such as phishing, which tricks individuals into revealing sensitive information by presenting them with a false credential, have grown in both sophistication and in the ease with which they can be replicated on a massive level. Even managing email has become an arduous task; integrated message management firm Postini found that unwanted email accounted for 84% of all email sent in April 2006.

Figure 1: Timeline Evolution of DoS/DDos Attacks.[8]



[6] *Top Threats and Trends of 2005: A Forward-Looking View,* ©2006 iDefense, Inc.

[7] *Blended Threats: Four Years Later,* ©2006 iDefense, Inc.

[8] Source: VeriSign, Inc.

A truly effective security infrastructure must be able to adapt to technological and organizational changes, and quickly correlate data from disparate sources, allowing IT managers to set immediate priorities.

+ The Need for Intelligent Infrastructure

Whereas networks could once be effectively protected via a series of individual products and services such as firewalls, password-protected interfaces, and virus-protection software, today's networks require a broader, more integrated approach to data security. Solutions from different vendors frequently display incompatibilities and are often difficult to integrate, creating an inadequate security net. Also, managing a multifaceted threat that attacks multiple networks at once requires engagements with many individual providers, which can lead to inefficiencies.

More importantly, while many individual products are highly efficient at protecting against specific threats, solutions built out of disparate products are often inefficient at providing visibility across the entire network, allowing managers to prioritize remediation efforts. In addition, an infrastructure built out of disparate components is difficult to utilize for data-correlation and risk-profiling, as an administrator must gather information from a number of different devices, creating data that can be time-consuming to correlate. This liability can prove disastrous in the event of a crisis, particularly a threat which attacks numerous services at once. Organizations that rely on disparate services often find themselves in constant fire-fighting mode, losing significant time and resources reacting to the latest crisis.

Organizations must implement a security program that can manage threats across various devices and provide robust security across a variety of authentication platforms, not only through established prevention methods, but through around-the-clock monitoring, risk-profiling and assessment, and adaptive services capable of meeting changes in demand and technology.

A truly effective security infrastructure must be able to adapt to technological and organizational changes, and quickly correlate data from disparate sources, allowing IT managers to set immediate priorities. In short, the optimal security framework must leverage intelligent infrastructure. To mitigate today's information-security threats, such an infrastructure must offer:

+ Strong yet flexible security

One of the key challenges in network security is maintaining the balance between ensuring the highest level of security and allowing for individual customization and privileges. Doing so efficiently requires an intelligent infrastructure that can provide security across the board yet allow for immediate widespread modification.

+ Scalability

Among the most common pitfalls in information technology is failing to quickly scale systems to a rise in demand; relying on smaller stand-alone solutions can prove disastrous with a surge in traffic. An intelligent infrastructure must be able to anticipate spikes in activity and be prepared to respond to them.

+ Interoperability

An intelligent infrastructure must facilitate seamless interoperability across myriad protocols, platforms, security credentials, and devices. Given the complexity of today's security threats, an attack is as likely to come from inside the network, via an email attachment or a remote device, as it is to come from outside. An intelligent infrastructure must be able to operate across all aspects of a network, and to offer unified reliability across any desired form of authentication.

Leveraging an intelligent infrastructure can provide a viable alternative to in-house development, and provide cutting-edge equipment, specialized expertise, and a full-time staff to ensure the safety of all trusted information.

- **Adaptability**
  The surge in popularity of wireless communication devices demonstrates how quickly technology can change network demands. A point solution purchased today may adequately protect one method of access, but technological changes will require additional deployments. An intelligent infrastructure must quickly and efficiently adapt to new technological developments, and provide constant risk-profiling and assessment to remain on the cutting-edge.

- **Availability**
  Many attacks do not occur during normal working hours, but during off-hours, where the staff of individual services may be difficult to contact. An intelligent infrastructure must maintain a support staff that can offer 24/7 monitoring and protection, and can respond quickly to a crisis at any time.

- **Visibility**
  For organizations to implement the customization they require, they need full visibility into their network activity. Gathering this information from various individual providers is a significant drain of resources. An intelligent infrastructure must provide organizations with full and immediate visibility into both their own network and the global Internet environment of which they are a part.

Developing, implementing, and maintaining an efficient proprietary security infrastructure requires an immense commitment of time and resources. Many organizations are increasingly partnering with third-party security providers to whom they can outsource their security concerns. While trusting a third-party with sensitive data may seem like a risk, leveraging an intelligent infrastructure can provide a viable alternative to in-house development, and provide cutting-edge equipment, specialized expertise, and a full-time staff to ensure the safety of all trusted information.

Whereas an in-house security infrastructure requires a sizeable staff to develop and maintain, leveraging the intelligent infrastructure services of a trusted provider can offer the same level of protection and monitoring, and often greater, for a substantially lower price. A study conducted by Stratecast Partners, a division of Frost and Sullivan, found that over the course of three years, medium-sized businesses that chose to outsource their security to independent providers spent half as much on security as businesses that integrated a security system using different software and hardware solutions.[9]

[9] *Bridging the Gap between Effective Internal Network Security and Cost,* ©2006 Stratecast Partners

+ VeriSign Intelligent Infrastructure Services

VeriSign is the leading provider of intelligent infrastructure services for the Internet and telecommunications networks, enabling and protecting billions of interactions every day across the world's voice and data networks. Due to its unique position in the operation of critical Internet infrastructure, VeriSign is able to correlate security events across many devices and enterprises, and develop security services that protect users, networks, applications, and transactions, helping organizations to maximize business opportunities and minimize security risks.

Due to its unique position in the operation of critical Internet infrastructure, VeriSign is able to correlate security events across many devices and enterprises, and develop security services that protect users,networks, applications, and transactions, helping organizations maximize business opportunities and minimize security risks.

VeriSign intelligent infrastructure services are supported by a comprehensive series of assets that include global registries and continuously operated data centers. VeriSign is exclusively responsible for operating two of the world's thirteen root DNS servers, as well as the directories for top-level domains *.com* and *.net*, securely processing up to 18 billion Domain Name System (DNS) queries daily. This grants the company a unique overhead view of Internet traffic, and allows it to offer unmatched visibility and protection. To manage the large volume of information that VeriSign processes every day, VeriSign maintains a series of data centers strategically placed around the globe. Developed to exacting standards, these data centers are designed to maintain continuous uptime, whether they are validating security certificates or housing critical customer data. VeriSign also operates a series of security operations centers, where security experts monitor global threats and manage thousands of devices around the clock.

Supported by global registries and full-featured data centers, VeriSign intelligent infrastructure services can help organizations to mitigate today's complex security threats. VeriSign intelligent infrastructure services offer:

+ Strong Yet Flexible Security

VeriSign leverages its comprehensive experience to offer enterprises a robust security infrastructure that proactively protects them against all modern security concerns. VeriSign services, which include firewall, fraud detection, public key infrastructure and two-factor authentication, have been developed with flexibility as a key principle, and integrate easily and cost-efficiently into existing infrastructures. VeriSign secures 3000 enterprises and over 500,000 Web sites worldwide. VeriSign also provides hosted DNS services that help to mitigate DDoS attacks.

+ Scalability

Having successfully managed the *.com* and *.net* domains through the exponential growth of the Internet since 2001, VeriSign is acutely aware of the need for scalability. All of VeriSign's security services are supported by a robust network of data centers to scale quickly and efficiently. These services have been proven under real-world conditions to scale smoothly from thousands to hundreds of thousands of users, allowing enterprises to operate on an as-needed basis.

+ Interoperability

VeriSign offers organizations a comprehensive infrastructure that enables integration across a diverse variety of platforms, protocols, and devices. VeriSign leverages leading network solutions and cutting-edge technology to ensure that enterprises are easily able to provide security across all types of authentication credentials and a large variety of different networks, operating systems, and protocols.

The unique position that VeriSign holds in the critical infrastructure of the Internet allows it to provide organizations with an unprecedented amount of information monitoring and data-correlation abilities.

- **Adaptability**
  VeriSign offers forward-thinking solutions that can quickly and efficiently be modified to account for technological and organizational changes, and offers solutions for next-generation technologies, such as Voice-over-IP and RFID. To remain on the cutting-edge and proactively defend enterprises against potential dangers, VeriSign employs more than 200 researchers across 38 countries to provide information about threats before they can make an impact.

- **Availability**
  VeriSign intelligent infrastructure services are supported by a robust network of data centers that are designed to provide 24/7 uptime. VeriSign has a strong reputation for operating highly available services. For example, VeriSign currently processes as many as 18 billion DNS queries a day, and has been operating this service with 100% availability for eight years as of 2006.

- **Visibility**
  The unique position that VeriSign holds in the critical infrastructure of the Internet allows it to provide organizations with an unprecedented amount of information monitoring and data-correlation abilities. As the only security provider with full visibility across the 13 root servers, VeriSign enables organizations to dynamically assess their strengths and weakness, and see how changes in implementation will affect their vulnerabilities and regulatory compliance. VeriSign employs a highly-qualified staff that works around the clock to monitor the status of security devices, run vulnerability assessments, manage intrusion detection and firewall systems, and ensure interoperability with the latest technologies.

Due to its unmatched security infrastructure, cutting-edge information gathering services, and widely recognized international presence, VeriSign is highly knowledgeable in the operation of intelligent infrastructure services, capable of protecting against the information-technology threats of today and tomorrow.

Visit us at www.VeriSign.com for more information.

00023044