CONTENTS

Executive Summary from Scott Sanders 3
Evaluate the Threat Landscape 4
Choose the Right Security Tools - Design for Both Security and Flexibility 6
Prepare for Threats, Breaches and Attacks - Correlate Signals and Orchestrate Responses 8
Expand to a Hybrid Premise and Cloud Security Architecture 9
Conclusion 10
EXECUTIVE SUMMARY FROM SCOTT SANDERS
Senior Vice President
Verisign Security Services

Having a tightly integrated security framework is more critical than ever as cyber-attacks grow and enterprises employ a variety of on-premise and cloud-based computing services to deliver applications. Today’s expansion of enterprise architectures and adoption of hybrid security solutions are adding a new level of complexity for Chief Security Officers (CSOs) and Chief Information Security Officers (CISOs).

To protect against today’s attacks, there is a need to expand the security framework from the ground up and design for the changing computing landscape. The following are recommendations for designing or choosing a framework that allows for a unified, resilient defense of the entire security ecosystem:

• Evaluate the threat landscape
• Choose the right security tools designed for both security and flexibility
• Prepare for threats, breaches and attacks by correlating signals and orchestrating responses
• Expand to a hybrid premise and cloud security architecture

Drawing on Verisign’s expertise and experience, this paper identifies key requirements of a flexible security framework, and explores how enterprises can use application programming interfaces (APIs) to extract signals and use a mix of security components on-premise and in the cloud to enhance their existing security ecosystem.
EVALUATE THE THREAT LANDSCAPE

The first step to architecting a resilient defense and spending IT security dollars is to understand threats in context to protect resources accordingly. To understand threats in context, organizations need timely, relevant and actionable threat intelligence, and the capability to identify relationships among threat elements. Global security intelligence, when complemented by expert analysis and correlation tools, helps enterprises determine which resources are most attractive to cybercriminals, how these resources might be exploited or attacked, and the motivations, tactics, resources and skill level of potential attackers. Evaluating security intelligence holistically enables enterprises to prioritize resource allocation and better defend against attacks.

Threat vulnerability for an enterprise must be evaluated as a continuous process. When examining a diverse application environment, enterprises must reevaluate their risk for any additional gaps that may have arisen as a result of changes made to their infrastructure and processes. This introduction of new systems and services to protect assets may expose new threat vectors. To help evaluate threat vulnerabilities, enterprises must continuously ask and answer four basic questions:

- What makes you attractive to an attacker?
- What are you trying to defend against?
- What is happening in your vertical?
- What pieces of your environment are most vulnerable to attack?

Enterprises are undergoing major transformations as they open their networks to accommodate internal assets; public, private and hybrid clouds; the Internet of Things (IoT); and personal devices. Although this expansion can offer many benefits and opportunities as well as enhance employee and service productivity, it also enlarges an organization’s attack surface and thereby increases its potential exposure to downtime, data breaches, loss of revenue, and damage to both brand and reputation.

"Collating, correlating, assessing and analyzing the information that delivers the intelligence product that is ultimately disseminated can be labor-intensive, and requires specialized expertise that is difficult and expensive to obtain. External threat intelligence services provide a cost-effective method to achieve this." 

According to the Ponemon Institute, companies using security intelligence technologies enjoyed an average cost savings of $1.9 million when compared to companies not deploying security intelligence technologies.\(^1\)

"Collating, correlating, assessing and analyzing the information that delivers the intelligence product that is ultimately disseminated can be labor-intensive, and requires specialized expertise that is difficult and expensive to obtain. External threat intelligence services provide a cost-effective method to achieve this."\(^2\)

The average financial services company uses 1,004 cloud-based applications.\(^3\)

---

Cybercriminals are exploiting the expanding attack surface as they launch increasingly sophisticated, high-volume and targeted attacks against infrastructure operators, cloud service providers, financial institutions, IT services, e-commerce sites, media and publishing companies, and more.

Verisign has observed that no vertical is immune to distributed denial of service (DDoS) attacks. Cyber-attacks today often target specific industries or companies. For example, a recent Verisign DDoS Trends Report\(^5\) indicated that IT/cloud/software as a service (SaaS) providers were the most frequent targets of DDoS attacks, followed closely by media and content providers. Financial, public sector, telecom and e-commerce/online advertising services were also targets. (See Figure 2.)

As an example of increasing scale of cyber-attacks, in December 2015, Verisign mitigated a set of coordinated DDoS attacks against key components of the Internet’s navigation framework under its management, the A and J root name servers. Traffic volume during these attacks reached an excess of five million queries per second, per root name server, more than 10 times the normal traffic volume.\(^6\) Had the infrastructure not been designed with consideration for these types of attacks, the impact could have been catastrophic to global e-commerce and online services. Further analysis of the attack by the Verisign iDefense\(^6\) Security Intelligence team suggests the malware used in the DDoS attacks was first seen in February 2015 based on the patterns exhibited in the spoofed IP addresses. The analysis further suggests that rather than targeting a domain name system (DNS) reflector, one of the more common targets of attack, the intended targets were the root servers themselves as almost the entire IPv4 address space was spoofed to send malicious DNS queries.

---

In addition to strictly targeting service availability, attackers are increasingly exploiting one vulnerability in order to execute an even more surgical or persistent attack somewhere else on the network. As Forrester Research recently observed, “DDoS has historically focused on disruption, but today it is more frequently an opening salvo for more complex attacks that result in theft of sensitive data or valuable intellectual property.”

Security is an iterative process – continuously ask and answer four basic questions:

- **What makes you attractive to an attacker?**
  - Availability
  - Integrity
  - Assets
  - Information

- **What are you trying to defend against?**
  - Hacktivists
  - Cybercriminals
  - Zero-Day Vulnerabilities
  - State-Sponsored Spies

- **What is happening in my vertical?**
  - Public Cloud
  - SaaS
  - On-Premise Virtual Server
  - On-Premise Private Cloud
  - On-Premise Physical Server

- **What do you need to protect?**

**Figure 3 - Continually Evaluate the Threat Landscape**

**CHOOSE THE RIGHT SECURITY TOOLS - DESIGN FOR BOTH SECURITY AND FLEXIBILITY**

It is important to design a security framework that is flexible enough to accommodate a range of business needs and goals in an era when the threat landscape, technology innovations, deployment environments and user trends are undergoing constant change. At any given time, the variables inside and outside the enterprise may alter the manner in which cloud-based or third-party security services are utilized: as a primary solution or as backup or augmentation to in-house solutions.

---


As companies grow they may end up implementing unique, “out-of-the-box” security solutions for each new security need. Over time, this fragmented approach can result in a costly collection of redundant, proprietary or mismatched components that may not offer the scalability, performance and flexibility needed to protect an ever-expanding attack surface. For example, an enterprise may have purchased siloed devices that are incapable of interacting with other best-of-breed security solutions and thus, would not allow the enterprise the ability to use appliances or security intelligence services from diverse vendors.

In contrast, a solutions-based approach focused on choosing best-of-breed tools that work together to address a range of well-defined goals and requirements as well as evolving needs over time is preferred. Through this approach, IT security leaders can choose each environment (on-premise, cloud-based or hybrid) and tool within the context of the entire security solution rather than as a stand-alone component. This allows an enterprise to augment existing implementations, functionalities and environments to meet the enterprise’s specific business needs.

A vendor-agnostic security architecture allows an enterprise to extend on-premise or cloud-based security to public cloud infrastructure, platforms and services (and security features embedded within those resources) as needed to proactively monitor and better protect assets throughout the enterprise. Allowing heterogeneous appliances and services to interoperate in varying combinations across multiple, distributed environments creates a sustainable security framework that can flexibly accommodate unknown threats as they arise.

**KEY TAKEAWAYS:**

1. Design for where you expect your IT environments to evolve – flexibility will accommodate a range of needs and business goals
2. Choose best-of-breed security tools that will grow with you – the same tool may not work in all environments
3. Ensure the tools you choose have well documented and easy to use APIs – talk to your security vendors about the various types of data you can collect and correlate
PREPARE FOR THREATS, BREACHES AND ATTACKS - CORRELATE SIGNALS AND ORCHESTRATE RESPONSES

Having a response plan in place ensures that you can quickly and effectively respond to a security incident. Preparing for a security incident in advance will save precious time, contain potential exposure and prevent collateral damage. A comprehensive strategy should address incident response processes, key personnel required and a detailed communication plan. Determining this in advance will alleviate confusion during the critical times and allow a security team to focus on response and remediation.

Data collection and correlation plays a key role in detecting an incident and taking the appropriate action. To keep up with today’s threats and complexities of infrastructure, enterprises must ensure security telemetry is not only processed at each point of collection but also correlated across the entire security solution. This will shorten response times and reduce the need for extensive human involvement when analyzing a threat to the enterprise. Additionally, by leveraging APIs and enabling automatic collection, correlation, and orchestration of signals, enterprises will increase their overall threat awareness, improve incident response and optimize security protection.

When well designed and carefully tested, these data collection and correlation tactics take the guesswork out of decision-making, ensure a consistent approach and shave precious and potentially costly minutes off of mitigation. They also reduce the burden on IT teams who do not have the time or expertise to manually collect and analyze data, or who need to focus on higher-order tasks that require human intervention.

THE IMPORTANCE OF APIs IN THE SECURITY ECOSYSTEM

An API is a set of processes, protocols and tools for enabling access to devices, services or information; creating connections between these resources; or specifying how they should interact and interface with each other. By decoupling information from the resource itself, APIs allow data and resources to be distributed, re-used, and transformed to provide additional functionality or value. One resource can interact with many other resources to create new synergies. Using an API-centric approach, enterprises can better integrate their on-premise, cloud-based or hybrid application environments, extend and enhance the capabilities of their existing security solution, and close security gaps.

KEY TAKEAWAYS:

1. Prepare for a security incident in advance – develop a comprehensive strategy and incident response plan to take the guesswork out of decision-making
2. Process and correlate security telemetry at each point of collection – monitor telemetry across applications and security devices for an effective response

---

Ponemon Institute estimates the average total cost of a data breach to be $3.79 million.¹⁰

---

EXPAND TO A HYBRID PREMISE AND CLOUD SECURITY ARCHITECTURE

Just as enterprises today are choosing a mix of private and public cloud computing, and Content Delivery Network (CDN) services for performance to meet their needs, the same approach must extend to security services as well.

For certain types of business needs (resiliency, availability, etc.) cloud-based security services often offer more enhanced capabilities, the ability to scale (worldwide points-of-presence and increased capacity to handle large attacks), and greater expertise and global intelligence than a single enterprise can provide on its own—at lower cost and quicker time to deployment.

Given the growing size, complexity and stealth of today’s cyber-attacks, these advantages of cloud-based security services are essential for:

1. In-depth, real-time threat intelligence
2. DDoS attack filtering and mitigation
3. DNS protection

Leverage cloud security providers to fill gaps that premise-based security solutions cannot address in isolation. Evaluate third-party providers of threat intelligence, cloud-based DDoS protection and hosted DNS solutions.

Figure 4: Expand to a Hybrid Premise and Cloud Security Architecture
CONCLUSION

Security architectures are continuously evolving as the enterprise attack surface expands and the threat landscape grows. Enterprises must consider adopting a wide spectrum of on-premise, cloud-based and hybrid security solutions in their defense strategy. These solutions need to be carefully integrated in order to prevent gaps in security and maximize the value of telemetry coming from these investments. A framework that leverages APIs to connect services, share data and automate processes allows enterprises to create a unified, resilient defense against cyberthreats.

Verisign is a leader in cloud-based security services, threat intelligence and standards-based API development that enhance Internet operations and security. APIs are the foundation of the Verisign OpenHybrid™ architecture, which helps enterprises protect their networks, applications and data across distributed environments from DDoS and other advanced cyber-attacks. Verisign OpenHybrid enables intelligence sharing and threat signaling across an enterprise’s entire ecosystem—whether on-premise, cloud-based or hybrid. Using APIs, enterprise resources can interact flexibly and automatically, if desired, with other Verisign resources, including Verisign® iDefense Security Intelligence Services, Verisign DDoS Protection, Verisign DNS Firewall, Verisign Managed DNS, and Verisign Recursive DNS.
VERISIGN SECURITY SERVICES OFFERINGS

iDEFENSE SECURITY INTELLIGENCE
Helps organizations make better-informed decisions by providing timely and actionable cyber-intelligence related to cybercrime, cyber-espionage, hacktivism and vulnerabilities, delivered through a next-generation threat intelligence platform and API.

DDoS PROTECTION
Cloud-based monitoring, superior attack mitigation capabilities, a unique Verisign OpenHybrid™ architecture and a purpose-built global network provide a scalable solution to combat today’s increasingly complex DDoS attacks, both on-premise and in the cloud.

DNS FIREWALL
An easy-to-configure cloud-based service that provides global threat protection and prevents access to unwanted Internet content.

MANAGED DNS
Secure, cloud-based, globally available DNS hosting service provides a 100 percent service-level agreement for DNS resolution, global scale to withstand attacks and reduced cost and complexity when compared to traditional in-house solutions.

RECURSIVE DNS
Secure and reliable cloud-based recursive DNS service built to withstand attacks while offering superior performance and DNS stability.

FOR MORE INFORMATION
For more information about Verisign Security Services or Verisign OpenHybrid™, please visit Verisign.com/SecurityServices.

ABOUT VERISIGN
Verisign, a global leader in domain names and Internet security, enables Internet navigation for many of the world’s most recognized domain names and provides protection for websites and enterprises around the world. Verisign ensures the security, stability and resiliency of key Internet infrastructure and services, including the .com and .net domains and two of the Internet’s root servers, as well as performs the root-zone maintainer functions for the core of the Internet’s Domain Name System (DNS). Verisign’s Security Services include intelligence-driven Distributed Denial of Service Protection, iDefense Security Intelligence and Managed DNS. To learn more about what it means to be Powered by Verisign, please visit Verisign.com.