## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>3</td>
</tr>
<tr>
<td>THE LIFEBLOOD OF MANY BUSINESSES IS UNDER ATTACK</td>
<td>3</td>
</tr>
<tr>
<td>IT LEADERS FACE A DIFFICULT BALANCING ACT</td>
<td>3</td>
</tr>
<tr>
<td>Companies are Exposed in the Cloud</td>
<td>5</td>
</tr>
<tr>
<td>Threat Challenge: Seeing and Connecting Threats across All Environments</td>
<td>6</td>
</tr>
<tr>
<td>HARNESSING CLOUD-BASED PROTECTION FOR BETTER BALANCE</td>
<td>6</td>
</tr>
<tr>
<td>CONCLUSION: ADOPTING A HYBRID SECURITY APPROACH IS KEY TO APPLICATION RESILIENCY</td>
<td>7</td>
</tr>
<tr>
<td>ABOUT VERISIGN</td>
<td>7</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Organizations relying on online applications to deliver services to customers and generate revenues for the business must contend with an increasingly hostile and complex threat environment. The challenge is complicated when IT leaders move these applications to a public, private or hybrid cloud. Without communications and interactions between on-premise security and hosted applications, organizations lose visibility and control over application security and availability. As organizations move to the cloud for agility, efficiency and cost savings, they need to align their security approach accordingly, and adopt a novel – yet proven – approach for striking a balance between availability and security of applications in the cloud.

THE LIFEBLOOD OF MANY BUSINESSES IS UNDER ATTACK

Today’s enterprises increasingly rely on Web-based services and applications to power their businesses, including those fueling online commerce, service delivery, support, communication, collaboration and more.

These applications and services drive significant revenue and profit, making them the lifeblood of these organizations. Yet, it’s no small matter ensuring these diverse and complex services and applications are always available and working without fail. This is especially true in a world characterized by a growing range of sophisticated security threats and massive distributed denial of service (DDoS) attacks. It’s no wonder TechTarget’s 2014 IT Priorities Survey indicates that 45 percent of respondents will be adding new capacity in network security and 35 percent plan on adding threat detection and management.

The mandate for today’s CIOs and CSOs is to prevent outages, reduce the risk of and thwart any and all attacks, and minimize network exposures. Doing so is vital to securing non-stop business operations, protecting brand reputation, and satisfying customer and employee expectations.

IT LEADERS FACE A DIFFICULT BALANCING ACT

One could argue that this is a balance long required of those in charge of IT infrastructure. However, they now face a much more difficult challenge and delicate balancing act. Because of the need to support large and compute-intensive databases and a huge volume of users, applications have grown very large and complex.

To handle this explosion of large, complex applications in the midst of significant budget constraints, tech leaders have been driven to leverage a variety of environments to host and deliver these applications. These include various cloud environments – including public, private and hybrid – often interconnected to ensure an always-on operating environment.

---


Fewer than 30 percent of organizations are prepared for a DDoS attack against their extended network infrastructure.
The benefits of this distributed approach seem clear. David Floyer, CTO of tech community site Wikibon, states, "Wikibon forecasts that the total worldwide value created by the industrial Internet alone will be $1,279 billion in 2020, with an IT spend of $514 billion...Our initial finding is 90 percent of the value comes from the business, through faster time-to-deploy and change, and increased availability of resources to develop new applications. About 10 percent of value comes from lower IT costs and in some cases lower IT budgets, particularly from lower OPEX costs for supporting applications."3

Application Environments and Online Threats are Diversifying
(Source: VeriSign, Inc.)

At the same time, CIOs and CSOs are facing an increasingly complex threat landscape, spanning cyber crime, new system and application vulnerabilities, hacktivism and espionage. With applications hosted in the cloud, tech leaders must contend with a bigger attack surface and threats that are so large, sophisticated and malicious, they have reached Internet scale. In just one example, Verisign’s Quarterly DDoS Trends Report showed that the number of DDoS attacks exceeding 10 gigabits per second (Gbps) grew substantially between the second and third quarters of 2014.4 The issue is complicated by all the ways online applications are accessed. In addition to connecting via corporate networks, employees, customers, partners and others often access online services via mobile devices from anywhere. Each of these end points can serve as conduits for potential security threats.

It’s no wonder IT and security staff struggle to stay abreast of and maintain knowledge and understanding of the ever-changing scope of threats. More importantly, these attacks are beyond the control of organizations using reactive strategies.

As the average attack size increases and networks are flooded, it is more difficult—sometimes impossible—for organizations to mitigate DDoS attacks using traditional security devices. In fact, attacks that saturate an organization’s network pipes render on-premise security devices ineffective, leaving applications vulnerable.

**Companies are Exposed in the Cloud**

Consider these two examples:

A global media company with 20,000 employees maintains many private data centers around the world. The company’s CIO faces significant cost pressures as he or she expands the organization’s network to support a global customer and employee base. At the same time, the CIO must support new online applications and services, including traditional websites, e-commerce in many markets, and applications in many languages. He or she chooses to move many of those applications and services into a new public-cloud environment for cost savings. However, the tools the organization has relied on for years to proactively manage security in its data centers don’t integrate with the new cloud environment. This leaves the CIO’s security approach out of balance and exposes the organization to problems.

Or consider the case of a quickly growing niche software-as-a-service (SaaS) company with 300 employees. The company’s hugely popular and proprietary application is hosted by a very large public-cloud services firm in the U.S. To support the company’s global expansion, its CIO recently signed hosting agreements to offer localized versions of the application in numerous markets around the world. For legal reasons, the data generated by the application must also be hosted in many of the local markets, including Germany, the U.K. and others. The CIO is worried about load balancing across all those locations. Perhaps more concerning is that the traditional flow-based monitoring tools the organization had used to proactively address security are not available from all of the new hosting providers. In these different cloud environments, this organization is now exposed to new threats.

In short, while many organizations are compelled to host their applications in the cloud, they are bumping up against shortcomings when it comes to extending their traditional security tools and approaches into these new environments. Simply put, what worked in more contained environments—and in a simpler threat landscape—doesn’t provide the threat awareness, visibility or control needed to cover the size of the new attack surface and the scale of today’s threats.

In fact, because today’s attacks can completely overwhelm any on-premise security solution, industry experts and analysts recommend a hybrid approach to mitigating the impact of DDoS attacks.

---

http://bits.blogs.nytimes.com/2014/12/02/hacked-vs-hackers-game-on/
HARNESSING CLOUD-BASED PROTECTION FOR BETTER BALANCE

Relying solely on traditional premise-based or discrete threat solutions is insufficient and won’t provide balanced protection across more complex environments. CIOs and CSOs need to consider an approach that complements their existing security strategies while enabling interoperability between environments and protection against DDoS and other threats. Leveraging a comprehensive, interoperable approach will enable proactive threat intelligence.

and make applications more available and secure. With CIOs and CSOs more prepared to protect applications and data across different environments, CIOs can deliver on their promise to the business of uptime and always-on services.

Cloud-based DDoS protection services divert and filter attack traffic before it reaches an organization’s network. Besides mitigating the entire attack outside the organization’s environment, these protection services complement on-premise solutions so businesses can cost-effectively address a range of threats.

**CONCLUSION: ADOPTING A HYBRID SECURITY APPROACH IS KEY TO APPLICATION RESILIENCY**

A growing reliance on Web-based applications, an evolving threat landscape and fragmented security has yielded new IT challenges. Businesses increasingly rely on network availability as applications and systems that support business-critical applications move to cloud environments. As more companies shift their workloads onto public, private and hybrid cloud infrastructure, they are exposed to new security risks and the potential for application downtime. The challenge of balancing availability and security is complicated by the fact that attacks are growing in size, complexity and frequency – and that traditional tools often prove inoperable or ineffective in cloud environments.

A hybrid approach that calls upon open standards helps ensure interoperability between diverse environments and addresses the new operating and threat landscape. A combination of on-premise security devices communicating with cloud service providers, augmented by cloud-based DDoS protection and actionable threat intelligence is paving the way for non-stop availability and secure applications.

Combining on-premise security devices with cloud-based DDoS monitoring and mitigation provides a powerful foundation for application and service availability. By taking advantage of this opportunity, organizations can effectively defend against today’s increasingly massive and complex DDoS threats, and help ensure the uninterrupted flow of their lifeblood.

To learn more about ensuring application availability and security in the cloud, visit [www.verisigninc.com/DDoS](http://www.verisigninc.com/DDoS) today.

**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 Network Intelligence and Availability 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 [VerisignInc.com](http://VerisignInc.com).