

Protecting Applications on **Microsoft Azure** against an Evolving Threat Landscape



So, your organization has chosen to move to Office 365. Good choice. But how do you implement it? Find out in this white paper.

By Tony Bradley
CISSP-ISSAP, Microsoft MVP

riverbed

As companies explore the various cloud platforms, organizations that are already invested in Microsoft infrastructure are naturally inclined to move to Azure.

The cloud has reached mainstream critical mass. It is no longer just an industry buzzword, or some ethereal concept that only bleeding edge companies are embracing. It has evolved from a tactical advantage for early adopters to a strategic imperative for businesses that want to remain competitive. Organizations that fail to leverage cloud servers and services risk being left in the dust of their rivals.

A study conducted by RightScale in early 2014 found that cloud adoption has achieved virtual ubiquity. Nearly 9 out of 10 organizations reported using the public cloud in some fashion, and 94 percent indicated they are running applications in the cloud, or experimenting with cloud-based infrastructure-as-a-service.

As companies explore the various cloud platforms, organizations that are already invested in Microsoft infrastructure are naturally inclined to move to Azure. Microsoft is a brand that they trust, and Azure provides a cloud experience that feels familiar, and one that is optimized for Microsoft servers and applications. There is no need to re-invent the proverbial wheel, or retrain IT personnel.

Done right, cloud computing can simplify IT management, and help organizations operate more efficiently. It is also much more scalable than a traditional architecture, and provides tremendous flexibility for users to access apps and data from virtually anywhere.

The cloud also introduces some unique risks as well, though. The lack of a “perimeter” means there really is no “inside” and “outside” of the network. The shift in network architecture has enabled attackers to develop new techniques and exploits that render traditional network defenses like firewalls inadequate.

Evolving Threat Landscape

The drive to embrace the cloud, also comes with some sobering concerns as well—like protecting apps and data. According to the RightScale study, security is the top concern—followed closely by compliance—for organizations just beginning to adopt cloud services and apps, and remains a top five concern even for companies with mature, established cloud environments.

Keeping up with the demand to crank out Web apps while eliminating—or at least minimizing—vulnerabilities is a major challenge.

The rush to the cloud has resulted in an explosion of cloud services and Web apps. The problem is that many of the cloud services and Web apps are developed hastily. There is pressure to deliver apps with specific features and capabilities as quickly as possible to give the company a strategic advantage, and that pressure leads to developers focusing on features and performance instead of security.

Developers often rely on third-party development frameworks, or pre-packaged building blocks to accelerate development. Dependence on external platforms and code simultaneously introduces potential security weak spots that can be exploited, while also making security even less of a focus because developers just assume that the security of those elements is the responsibility of the third-party that created them.

A study published in early 2014 found that 96 percent of the Web apps tested contained one or more serious security vulnerabilities—with a median of 14 total vulnerabilities per app. There are tens of thousands of known vulnerabilities, and hundreds more discovered every month. Keeping up with the demand to crank out Web apps while eliminating—or at least minimizing—vulnerabilities is a major challenge.

Web apps are under constant threat from attacks like SQL injection and cross-site scripting. These attacks seek out and target unchecked input data and weak authentication mechanisms. Unprotected applications are an Achilles heel that exposes business-critical data to increased and unnecessary risk.

Advantage: Attacker

As if it's not bad enough that developers aren't focused on security, and continue to rush out new apps riddled with vulnerabilities, attackers have two distinct advantages over you and your Web apps: automation and opportunity.

First, there are a variety of tools available to automate attack reconnaissance. These tools can scan for and identify vulnerabilities in your Web apps or cloud architecture—things like SQL injection, cross-site scripting (XSS) flaws, URL manipulation, authentication / session attack vulnerabilities, and weaknesses that enable cross-site

request forgery (CSRF) attacks to name a few. Once an automated scanning tool finds the weaknesses in your network or app security, the attacker just needs to develop or find an exploit.

The second major advantage attackers have is that they only have to find one vulnerability to exploit, while you have to defend against every possible exploit and attack vector. Even in a best-case scenario where developers have worked diligently to address and minimize the vulnerabilities in a Web app, there is no such thing as perfect code, and the odds are still in favor of the attacker armed with automated scanning tools who only needs to find one weakness to exploit.

It is impractical to approach security strictly from the standpoint of proactively identifying and avoiding exploits.

The Right Tool for the Job

It would be preferable for developers to invest more time and effort to identify and mitigate vulnerabilities in their apps, but with the advantages favoring the attackers, and the fact that there is no perfect code you also need to employ some defense mechanisms. Not just any defense mechanisms, though—it's important that you use security solutions designed for the environments and threats of today.

Traditional security tools like hardware-based network firewalls, and antimalware applications are simply not designed to detect or defend against the challenges facing cloud-based Web apps. It is impractical to approach security strictly from the standpoint of proactively identifying and avoiding exploits. Effective security requires more comprehensive monitoring to detect suspicious or malicious activity as it happens.

A distributed cloud app needs distributed security as well. It is no longer possible to view security through the perspective of simply blocking or guarding against threats outside the “network perimeter”. The security solution needs to be dynamic and scalable to meet the potential demands of the cloud, and it needs to be virtual so it can be quickly and easily deployed across both physical and virtual environments whether those environments are hosted in private, public, or hybrid cloud infrastructures.

The security solution also has to be easy to manage. You need something that can be centrally managed, and gives you granular control on a per app and/or per user basis. It should also be able to monitor

activity and enforce established policies. Finally, it's crucial that the user interface be intuitive so that managing and maintaining the security solution is simple. A poor UI makes using and administering the security solution cumbersome.

Riverbed SteelApp

Riverbed has a simple goal: To ensure business objectives—not technical constraints—drive how applications and data are delivered. A crucial element in achieving that goal is to make sure customers can deploy and manage Web apps securely.

The Riverbed SteelApp Web App Firewall envelopes apps in their own security perimeter.

Riverbed SteelApp Traffic Manager is available in the Microsoft Azure store, and is one of a small handful of tools that have achieved Azure Certification from Microsoft. SteelApp Traffic Manager is a high-performance load balancer that enables faster, more reliable, and more secure access to apps hosted on Microsoft Azure. The SteelApp software inspects, transforms, prioritizes, and routes app traffic—including performing full payload inspection.

Common performance limitations are avoided by using a distributed architecture. Operations are spread across physical, virtual, cloud, or hybrid environments to avoid hardware bottlenecks and web server constraints—enabling efficient Web app performance from virtually anywhere.

The Riverbed SteelApp Web App Firewall envelopes apps in their own security perimeter that establishes a secure session identifier, encrypts cookies and URLs, and enforces site usage policies. It proactively detects and blocks attacks at the application layer, and shortens the window of attack from external threats by reducing risk and exposure.

You can also optimize performance, and accelerate webpage load times with Riverbed SteelApp Web Accelerator. SteelApp Web Accelerator improves Web app adoption, and improves user satisfaction—resulting in a reduction in helpdesk complaints. You can increase revenue with higher usage of customer-facing tools, and improve productivity and collaboration by speeding up SharePoint response times.

**Reliability,
performance,
and security are the
differentiators that
separate you from
the competition.**

Business rules protect applications, mask data, and help organizations comply with PCI-DSS (Payment Card Industry Data Security Standard) requirements. To top it off, Riverbed SteelApp is easy to manage. A central console gives IT admins the power to control things at a granular level, and ensure the speed, reliability, and security of all Web apps.

Protecting Azure

Just adopting cloud services and applications isn't enough anymore. Reliability, performance, and security are the differentiators that separate you from the competition.


Microsoft Azure provides a powerful, comprehensive cloud ecosystem—offering both PaaS (Platform-as-a-Service) and IaaS (Infrastructure-as-a-Service) options—designed to enable Microsoft customers to take advantage of the strategic benefits of the cloud. Azure is an ideal environment for businesses that are already familiar with Microsoft servers and infrastructure to move to the cloud, or adopt a hybrid approach that leverages the cloud.

Moving to Azure—or moving to cloud-based servers and apps on any cloud platform—also comes with unique challenges. Users—whether they're external customers or internal employees—demand performance, and ubiquitous apps that are available across a distributed architecture face increased exposure to attack.

Riverbed SteelApp is certified for Azure by Microsoft. It provides a comprehensive suite of tools to enable you to monitor and manage Web app traffic, optimize performance, and employ security controls at the app level where they can be more effective against the new and evolving threat landscape.

About Riverbed

Riverbed®, at more than \$1 billion in annual revenue, is the leader in Application Performance Infrastructure, delivering the most complete platform for Location-Independent Computing. Location-Independent Computing turns location and distance into a competitive advantage by allowing IT to have the flexibility to host applications and data in the most optimal locations while ensuring applications perform as expected, data is always available when needed, and performance

issues are detected and fixed before end users notice. Riverbed's 25,000+ customers include 97% of both the Fortune 100 and the Forbes Global 100. Learn more at www.riverbed.com. 

Tony Bradley is a Houston-based independent analyst, marketing consultant and writer. He works with businesses to identify market opportunities and develop effective content marketing strategies to take advantage of them. Tony has worked in the trenches as an information security consultant, an IT manager and a marketing executive. He has been a CISSP for 13 years and has been recognized by Microsoft as an MVP for 9 consecutive years.
