

# Enhancing security and backup for a trusted cloud- computing solution





## Table of Contents

1. Identifying threats and neutralizing them
2. How Microsoft Azure and our partners help create a trusted cloud
3. Worldwide security experience matters
4. Security in the Cloud is a shared responsibility
5. Reducing complexity, not adding to it
6. Conclusion



In 2015, Rightscale asked over 900 IT professionals questions about how they run their data center. Among those surveyed, 93 percent said that they are using the cloud and 82 percent of them have a hybrid cloud strategy—up from 74 percent in 2014. But, while the cloud has immediate cost-effective benefits that doesn't offset the fact that data centers are more complex than ever and that security remains a large concern. In fact, some IT professionals believe that security is the largest concern for the "cloud movement."

In addition, IT managers are over-burdened with the day-to-day effort of managing their existing on-premises infrastructure. Tied to this management effort is an ongoing push to consolidate servers and leverage virtualization to drive down costs. What they could use is a system that helps automate these tasks, and that's a large part of what Microsoft Azure can help them achieve.

Automation not only eases IT managers' jobs and saves money, it allows them to go beyond thinking about servers to supervising their entire infrastructure—including computer, networking and storage resources. So the end game is to create a secure, well-orchestrated, heavily automated and innovative hybrid data center that can become a trusted, shared delivery service for the entire business.

The purpose of this white paper is to provide an overview of the security and backup challenges that exist in the hybrid cloud data center and how Microsoft Azure and its partners can provide solutions to overcome them. It also examines how, by rethinking old processes and introducing the cloud into your data center (while continuing to leverage existing skills and resources), scalability and security increases while time wasted managing infrastructure decreases.

The Cloud Security Alliance recently listed the top twelve security concerns for cloud computing in 2016. They



## Identifying threats and neutralizing them

include: Data breaches, compromised credentials and broken authentication, hacked interfaces and APIs, exploited system vulnerabilities, account hijacking, malicious insiders, the APT parasite, permanent data loss, inadequate diligence, cloud service abuses, DoS attacks and shared technologies/shared dangers.\*

With that many serious security threats and most organizations taking advantage of the cloud, it's clear that security will continue to be a top concern for IT. Microsoft Azure is proud to partner with four top-tier companies that bring the best possible security and backup solutions to the table.

### How Microsoft Azure and our partners help create a trusted cloud

For Microsoft (and many other companies) Commvault delivers a complete storage software solution for today's enterprise and SMB companies. With deep integrations and a single platform for end-to-end data management and protection, Commvault is built and optimized for Microsoft solutions to provide access to data that's easily accessible regardless of location.

When deployed on Microsoft Azure, Commvault can help reduce administrative overhead by up to 80 percent by enabling Microsoft to handle datacenter updates, patching and maintenance that simplifies administration and reduces infrastructure—without adding staff. Commvault also gives IT the option to move lower-tier data to the Azure cloud for online eDiscovery/searchable access and archives. That way, IT can leverage Commvault for all hybrid data which helps reduce management time and resources.

Built from the ground up, Commvault is a perfect companion for Azure to help IT manage heterogeneous data so that they gain insight across systems from a single console. This aspect of Commvault's solution allows IT to centralize data management,





disaster and granular recovery, end-to-end encryption, global deduplication and eDiscovery across on-premises to make data more secure and accessible.

“Commvault and Microsoft also offer years of joint experience with each other’s products. Commvault has utilized Azure for over 9 years while Microsoft has used Commvault for 17 and 15 years at the Microsoft Office Products Group and Xbox. These joint experiences lead to Best Practice guidance for our customers and confidence in scale,” Randy De Meno, Commvault Chief Technologist said.

“We wanted a data management solution that was not too complex, but it needed to meet a lot of different criteria. CommVault provides us with the peace of mind that the process can be managed end to end,” said Shawn McCoy, Principal Operations Lead, Microsoft Office product development group.

## Worldwide security experience matters

Barracuda delivers powerful yet easy-to-use security and storage solutions to over 150,000 organizations in more than 100 different countries. With a strong heritage in email and web security appliances and an award-winning portfolio, their clients can confidently protect their users, applications and data with Barracuda solutions.

As a Microsoft Azure partner, Barracuda helps bring security to web applications, secure and scale elastic applications, publish SharePoint in Microsoft Azure and secure and connect VNETS. They provide secure high speed VPN connections (>1 Gbps), deploy secure multi-tier network architectures and their spam firewall prevents zero-day and targeted attacks on email users, ensuring that sensitive information stays within the organization.

Jan Poczobutt, Senior Director, Public Cloud at Barracuda adds, “We’ve taken a unique approach to solving customers security concerns in Azure. We enable them to bring their best practices for security with them (like multi-tier architectures) while at the same time optimizing to deliver the benefits of the cloud in areas like architectures, automation, and orchestration. Customers get the best of both worlds. The rapid adoption of our solutions in Azure is proof that customers are finding this a great combination,” Jan Poczobutt, Barracuda Senior Director, Public Cloud said.

Theirs is the first integrated, proven and highly scalable security solution on Microsoft Azure, offering comprehensive protection for web applications and for confidential data hosted in the cloud. Their NextGen firewall F-Series ensures highly secure, encrypted traffic from, to and within Microsoft Azure providing secure remote and site-to-site access and centralized management. They provide advanced threat protection with spam and virus filtering for Microsoft Azure, ensuring best-of-breed, advanced email security and management.

The United Kingdom based movie and television streaming business, blinkbox has over a million customers with over 20,000 movies and TV episodes available online. They were faced with the challenge of backing up 1 PB of data safely and securely while meeting logistical complications. The solution they were using required waiting for weeks to receive additional web encoding servers. They also needed more security to keep their customer's data safe while maintaining excellent customer service.

Barracuda and Microsoft Azure provided them with automation of new threat blockers. They saved them time, costs and resources so blinkbox could concentrate on improving their customer experience and implementation required little additional training. In total, blinkbox estimates that with Microsoft Azure and Barracuda Web Application Firewall, they will save millions of dollars.

"The physical data center model no longer works for a company like ours. Microsoft Azure and the Barracuda Web Application Firewall provide everything that a dynamic company like ours requires," said Sarju Mashru, Principal IT Operations Engineer, blinkbox

## Security in the Cloud is a shared responsibility

With over 25 years of expertise, Trend Micro offers security solutions that protect end users on any device, optimize security for the modern data center, and secure networks against breaches from targeted attacks. They deliver top-ranked server,

network, and cloud-based protection that stops new threats faster, detects breaches better and protects data in physical, virtual, and cloud environments.

Trend Micro Deep Security offers comprehensive protection for cloud, data center and hybrid environments with a single host-based agent. Optimized for Microsoft Azure, Deep Security scales automatically as new VMs launch without compromising the speed and agility of the cloud.

“Aligning with pioneers and innovators, such as Microsoft, reinforces our commitment to help end users protect data across their entire IT environment, from the desktop to the network and the cloud. The flexibility and reliability of the Microsoft cloud platform empowers enterprises to address growing business needs, while Trend Micro’s comprehensive solutions are specifically designed to deliver cloud security to maximize ROI and utilize the full benefits of the Microsoft cloud platform,” Partha Panda, Trend Micro’s Vice President, Global Channel and Strategic Alliance said.

Trend Micro understands that even with Azure’s secure infrastructure, customers remain responsible for protecting their operating systems, applications and data—and that security is the number one barrier to cloud deployment. Their solutions, coupled with Microsoft Azure, defend against network attacks, keep malware off workloads, virtually patch software, uncover suspicious changes and meet customer’s speed compliance requirements.

Trend Micro gets that securing virtual machines in the cloud is different and that security needs to be as agile as Azure. So their security solutions “speak cloud” with a complete set of security capabilities for cloud VMs, offering automatic workload-aware VM protection and deployment right from the Azure Marketplace. With Trend Micro, IT can automatically catalog VMs, detect and protect new VMs and automatically scale in both stand-alone cloud and hybrid deployments.



Square Enix, a video game developer headquartered in Tokyo, Japan with 3,581 employees, required a secure platform for the launch of its latest on-line role playing game, "Rise of Mana." Targeting mobile users, the platform needed to dynamically scale without impacting their performance. At the same time, the high-profile brand and collection of billing information made security a top concern.

Square Enix selected Microsoft Azure and Trend Micro Deep Security for its secure cloud platform which was rolled out in early 2014. Azure and Trend deployed a full suite of security capabilities on a high-performance, 24/7 gaming platform with millions of users. They also streamlined and automated security and monitoring to reduce operation costs. By August, one million users had enrolled. The end result is that the Azure and Trend solution allows Square Enix to focus on its top priority: the development and growth of its business.

"Thanks to Trend Micro Deep Security we can concentrate on our main business without being distracted by security issues."  
–Square Enix

## Reducing complexity, not adding to it

New Signature's Cloud Management Portal (CMP) is a Microsoft partner that brings clarity to Azure users for administration and financial analysis of billing data at the enterprise level. Their dashboard and reporting features can reduce cost, help avoid surprises and maximize efficiency.

Their solution enables ease in managing and planning Azure usage, including meaningful trend insights for budgeting and capacity planning, custom views and reports on current and past usage. In addition, CMP allows IT to manage all Azure subscriptions using one simple interface. That way, IT can easily identify peak usage and view costs to enable chargeback and showback for all Azure subscriptions. CMP also helps IT to create

notifications and custom billing reports to enable optimal cost management across organizations.

Aden + Anais has brought the legacy of muslin together with fashion-forward design to create a line of products that are as stylish as they are useful. With their products popping up in magazines, virtually every celebrity gift registry and in stores around the country, they needed to streamline their processes and software architecture as they scaled their operations to meet an ever-growing demand for their products.

New Signature implemented a suite of cloud technology including Microsoft's Dynamics CRM Online and Office 365 to overhaul the way they collaborate, go-to-market, sell their product, and serve their customers.

"As a luxury brand, we are focused on quality and providing the highest levels of customer service. We are happy to say New Signature shares these values and were pleased both with the quality of their services and their ability to meet our tight timelines."

—Mark Miles, Vice President of Technology, Aden + Anais

As we move forward in our journey to the cloud, Microsoft sees the lines between how applications run on all forms of devices blurring and the Cloud OS becoming the backbone for all of it. By delivering a powerful, secure cloud solution on top of a consistent operating platform that spans across development and management, identity, virtualization and the data platform itself, Microsoft Azure is providing the future of cloud computing: a trusted cloud.

With strong, innovative partners, Azure will give IT the ability to manage their apps' environment and the infrastructure of

commercial IT in a way that goes beyond the boundaries of their data centers, so that they're able to take advantage of innumerable applications in a seamless way, immediately. This capability will give IT agility that they've never had before so that secure cloud computing is more than a possibility, it's a reality.



For more information, please visit

**MICROSOFT AZURE  
MARKETPLACE**