Security and Reliability in a cloud-first world
The Cloud and the state of modern security and reliability

As cloud computing continues to transform businesses and governments at an unprecedented rate, the new flexibilities and innovations it provides a work force come with new security risks. This is a familiar story, and one that rings as true today as it did at the advent of the .com boom. Companies looking to move to the cloud, want to be certain that their service provider provides equal or better reliability and uptime in exchange for giving up control of critical assets.

The advent of cloud computing has enabled modern workforce mobility, the flexibility for employees to work where they need to, on the device they want. This, enables international corporations with employees operating out of several different locations to maintain a high degree of unity and productivity despite geographic boundaries or an on-premises footprint. However, this advantage creates a proliferation of end points that require protection, encryption and control, magnifying security risks even as the new model facilitates growth and flexibility. Moving critical solutions to the cloud allows businesses to easily scale, but requires the trust that the service provider can maintain and improve upon the uptime of critical solutions.

Moving to cloud services is the best and most cost-efficient way to modernize a business. The challenge lies in choosing the right cloud service provider, and choosing one whose commitment to security and reliability mirror your own.

Let’s start out by talking about security.

Microsoft Cloud Services Security

Microsoft is building a platform that looks holistically across all the critical end-points of today’s cloud and mobile world, acting on the intelligence that comes from their security-related signals and insights, and nurturing a vibrant ecosystem of partners who help raise the bar across the industry. Microsoft’s investments occur across four categories: identity, apps and data, devices, and infrastructure.

Identity

To ward against identity compromise, Microsoft has implemented multi-factor authentication, moving beyond simple passwords to provide more secure means of identifying individuals logging into the platform. Breaches are identified early with behavioral analytics that work to detect any suspicious activity and automatic responses elevate access requirements based on perceived and identified risks.

Apps and data

For customers using applications in the cloud, Microsoft provides controls to help secure corporate data, in keeping with customer organizations’ rules and regulations. With an increasingly mobile workforce – these controls prevent costly leaks of corporate data while still enabling employees to use their own devices.

Devices

Suspicious devices are blocked and quarantined automatically, ensuring customer’s peace of mind without the need to tightly manage their own solutions.
Infrastructure

that all of an organization’s security policies are enforced on cloud resources. Machine learning helps to enforce these policies, detecting deviations. Early signs of compromise are identified early through behavioral analysis.

Ultimately, for a company looking to invest in cloud services, the key decision is to align with a provider who values security and who takes their own steps to ensure their customer’s data is secure, and their endpoints are detected. For Microsoft partner, Avesta, in conjunction with the Government of Iraq, this message of emphasized security became far more than a talking point for their peace of mind.

In 2015, the technical staff of the Ministry of Defense contacted Avesta Group looking for help. Its website had experienced a number of DDoS attacks from neighboring countries and groups, which frequently brought the site down and prevented the ministry from doing its job. Avesta Group migrated the site to Microsoft Azure in an effort to increase security. Once migrated and with the new security features in place, the DDoS related outages were mitigated, virtually eliminating DDoS attacks.

Microsoft is deeply committed to the security of its products and services. Beyond security, however, Microsoft understands that service reliability is equally important for customers and partners to dependably perform mission critical processes.

Doubling down on transparency and reliability

In any discussion on service reliability, Microsoft feels deeply committed to being open and transparent with their customers, providing unmatched insights into known issues in real time, and helping protect and mitigate against outages via a proactive and open approach.

Microsoft invests heavily in the reliability of the Azure platform. While other cloud service providers may speak to 49’s availability, (99.9999%) Microsoft takes this message beyond a generalized marketing statistic and holds itself contractually accountable to reach that standard. In 2016 there was a year-over-year reduction of 66% in planned maintenance time. Additionally, Microsoft has just implemented a new maintenance approach requiring no VM reboots for critical host OS updates.

There are hundreds of engineers employed by Microsoft whose responsibility, first and foremost, is to work on and improve Azure reliability. Microsoft has also developed machine learning that helps predict instances of hardware and network failure, calculating risk assessments to stay ahead of potential outages.
Extensive telemetry and analysis of downtime helps assess issues and allows for quick resolutions, while massive investments in hardware keep datacenters maintained and operating with the most modern hardware available. Recently, Microsoft developed a public-facing dashboard relaying specific root cause analysis for any issues that impact the Azure platform making Microsoft the only major cloud service provider to do so. (aka.ms/azurereliability)

Finally, with over 22 datacenters currently online in 30 different regions, Microsoft’s cloud footprint is the largest in the world, with 2.5 times more coverage than AWS and 7 times more coverage than Google.

**Microsoft reliability helps nonprofits secure global health objectives**

Blackbaud is a Microsoft partner committed to helping non-profit organizations throughout the world, including the American Red Cross, the Wounded Warrior Project, and Water Mission, an international NGO committed to providing clean safe drinking water throughout the world.

Having built with Microsoft products in the past, Blackbaud has since moved to Microsoft Azure for its primary fundraising solutions. For the small but growing organizations they support, like Water Mission, successfully securing funding for projects is critical for staying afloat. For the people Water Mission helps, securing this funding can be the difference between whether or not they have clean water to drink.

Blackbaud has over 35,000 clients and growing, with offices in over 60 countries.

Working with philanthropic organizations, Blackbaud’s solutions are critical in ensuring that these organizations are able to maintain their funding. For Blackbaud’s clients, who rely on donations to stay in business, an unexpected or lengthy service outage can critically impact their work.

Currently, $100 billion of the $358 billion raised in the US for non-profit organizations was either managed or processed by Blackbaud solutions. When processing nearly 1/3 of the philanthropic budget for one of the wealthiest countries on earth, Blackbaud depends on a trusted service provider with a reliable platform, one who is transparent in their approach and proactive in making the investments needed to improve the reliability of their services. For Blackbaud, that provider is Microsoft.

**With over 22 datacenters online in 30 different regions, Microsoft’s cloud footprint is the largest in the world, with 2.5 times more coverage than AWS and 7 times more coverage than google**
Helping partners achieve reliability excellence

Microsoft’s security and reliability story goes beyond the boundaries of what Microsoft can do for its customers and partners, extending to what Microsoft has enabled their partners to do for themselves. Grant Peterson, the CTO of Docusign, an ISV and Microsoft partner on the forefront of paperless technology stated in an interview,

“We took on a strategy two years ago that involved very granular instrumentation in our software. Every moving part is monitored. Tools built on our own technology, in conjunction with Azure, monitor about 400 million discreet events per day in real time. That is frankly one of the biggest aspects of our own reliability and security story. With the level of instrumentation possible within Azure we are able to micro-evaluate our operation. This has taken us from a situation where we had to work tirelessly for 99.9999% availability and moved us to a situation where we can comfortably approach 99.9999% availability. The monitoring resources available in Azure enable us to see problems when they are minor before they become critical which dramatically increases our own reliability as a result.”

Continuing the Investment

In dealing with cloud services there are always realities that need to be taken into account. The world is an unpredictable place, and problems will inevitably happen in complex systems. What’s important is that every step that can be taken to mitigate against these inevitabilities is taken. To prepare for incidents, Microsoft continues to invest in support resources, having recently reduced average time to resolution in Azure cases by 40%. In instances where an outage impacts a customer, the customer will be notified immediately, with 24x7x365 updates available. For customers looking to upgrade support, Microsoft is offering free 12-month support upgrades for all existing and new customers with enterprise agreements.

When making the transition to the cloud, security and reliability are the two most important factors. Finding a cloud provider who shares your values in this regard is crucial for safely modernizing your business. Microsoft is consistently making the adjustments and the investments necessary to be the most reliable and secure cloud provider, offering customers peace of mind that their cloud services will reliably work for them.

The monitoring resources available in Azure enable us to see problems when they are minor before they become critical which dramatically increases our own reliability as a result.”

Grant Peterson, CTO, Docusign