Azure Stack security
What Microsoft has done and why

For enterprise IT, 2017 was quite a year! On the downside, an unprecedented surge in cyberattacks including: Massive personal data thefts, like the Equifax hack which affected 148 million Americans; A plague of ransomware, including Wannacry which hit over 200 thousand systems in 150 countries; Destructive "wipers", such as NotPetya, intended solely to wreak havoc with no apparent financial motive.

On the upside, the year saw a "step change" in C-Level embracing of digital transformation, together with some significant technology developments: The meteoric rise of AI as a "digital enabler" for, well, almost everything; The emergence of decentralized "edge computing", complementing the public cloud model; The arrival (at last) of true hybrid cloud solutions such as Microsoft's Azure Stack.

Azure Stack is a unique "cloud edge" system which, with the help of select partners including Atos, extends Azure into the local data center.

Still, in these dangerous times, an inevitable question is: what about cybersecurity and Azure Stack?

The shared responsibility model

To answer that question, we first need to be clear about who is repsonsible for what.

In a public cloud, security is a shared responsibility: the Provider is responsible for the security OF the cloud and customers for what they run IN the cloud.

Since Azure Stack is a local extension of Azure, a similar model applies, with two "security posture" layers. The Microsoft layer comprises the cloud infrastructure, which goes from the hardware up to the Azure Resource Manager, and includes the Administrator and Tenant portals. The customer layer – essentially the workloads that tenants create, deploy, and manage – is under customer responsibility, possibly with help from a security partner like Atos.

In this post, I'll focus on the infrastructure security posture of Azure Stack which, in my view, is quite an achievement. Let's start with the "big picture" and then take a brief look at some of the high points of the design.

Azure Stack: a paradigm shift for on-prem infratructure security

Under the traditional on-prem infrastrucure model, suppliers usually provided general purpose "building blocks" (such as hardware, OS, middleware, networking), leaving customers or their partners with the job of making everything work together. Administrators had powerful elevated privileges because, under this model, they needed them. Operating systems had to be open and flexible, both to support a variety of hardware and to accommodate third party software (drivers, agents, etc) with potentially dangerous access to system internals.

As hackers and their victims can attest, this traditional infrastructure model is almost impossible to completely secure and lock-down.

Azure Stack represents an entirely different model. Microsoft collaborates closely with selected platform partners for the hardware specifications, the software and the configurations. Customers choose a Microsoft qualified partner (like the Atos-Dell EMC tandem) and the configuration they need, leaving the work of on-site deployment to the partner. The cloud infrastructure is composed of well-defined components that work together only in pre-defined ways and there is no third party software inside. Administrators and applications talk to Azure Stack as a single entity and only Azure Stack can talk to the hardware.

The bottom line: Azure Stack is a completely integrated system that - by design - can be completely sealed to achieve an order of magnitude improvement in security.

The design of the infrastrucure security posture

With this new model, Microsoft has built an innovative and robust infrastrucure security posture based on two complementary principles: Assume Breach and Harden by default.

Assume Breach is a modern - and entirely lucid - approach to security in dangerous times: cyberattacks are surging, serious breaches occur with depressing regularity and everyone's a target. That's why the security posture of Azure Stack is designed to detect and limit the impact of intrusions, instead of only trying to prevent attacks and hoping they don't succeed. Roughly speaking, this translates into three design imperatives:

- **Constrain the administrator role... no more "keys to the kingdom"**

  If robbers attack banks because "that's where the money is", hackers attack the traditional administrator role to get "the keys to the kingdom", in other words, its elevated set of permissions to do almost anything.

  With Azure Stack, if an admin credential is compromised, no such luck! Like the administrators, attackers can only perform "normal" pre-defined actions, instead of having unrestricted access to every infrastructure component.

- **Limit the "blast radius" of a breach**

  If an intrusion occurs, the first priority is to limit the "blast radius". In other words, compromise of one component shouldn't result in the entire system getting taken over.

  Fortunately, like football coaches and military officers, the Azure Stack security team understands defense in depth. Multiple layers of defense make it very hard for an attacker to move laterally inside the infrastructure after compromising one component. Examples include Access Control Lists applied at multiple levels, strict limitations on internal account privileges and anti-malware for all components. To make life even harder for attackers, only authorized whitelisted software can be executed, as opposed to, say, hacking tools.

  Another advantage: intruders trying to move inside the infrastructure would make lots of "noise", in other words, generate security incidents… which leads us to the next point.

- **Detect and diagnose intrusions fast**

  Security breaches often go undetected for months, leaving plenty of time for a hacker or sophisticated malware to work through a system and exfiltrate data. In many cases, companies first learned about data breaches from their own customers!

  In Azure Stack, Microsoft has implemented security logs of each component, centrally stored for easy visibility into the entire infrastructure. Using an API, qualified SIEM solutions can ensure continuous 24x7 monitoring. Microsoft is working on new features here, because fast detection and diagnosis is critical.

While Assume Breach is a modern and powerful approach to security, Microsoft also leveraged the classic but complementary approach of "system hardening", to reduce the attack surface and to enable and validate additional security features that make systems less vulnerable.

Hardening general purpose systems usually requires a great deal of on-site work by customers. With Azure Stack, Microsoft has the entire infrastructure under its control and has chosen to Harden by Default, the second design principle for its security posture. As Fillipo Seracini, head of the Azure Stack security team said recently: "We don't hand over a manual of instructions on how to harden Azure Stack; the work has been done already."

Since the engineers have done so many things here, I'll just cite three of my favorite examples.

- **Harden the OS to military standards**

  Customers hardening systems typically rely on a Security Technical Implementation Guide (STIG) which specifies what should be done to enhance security and further reduce vulnerabilities.

  Microsoft chose the toughest of them all, the Defense Information Systems Agency STIG. Essentially, it's a long list of detailed requirements (which I'll skip) that translates into a huge job of implementation, testing and validation. Fortunately, Microsoft did the work so that customers didn't have to.

- **Keep the cloud infrastrucure up to date… and patched**

  Keeping a system up to date and patched is critical for security. While the customer is responsible for the tenant area and its workloads, Microsoft has implemented an automated process for the infrastructure.

  Before a patch with a new feature or perhaps a security fix is sent to customers, the Azure Stack team tests and validates it on the various qualified platforms. Customers then have a reasonable window of time to apply the patch, using an orchestration engine that applies it seamlessly across the entire infrastructure… even while the system is up and running!

- **Encrypt all data everywhere**

  While encryption of data in transit is generally accepted, Azure Stack also provides disk-level encryption of all data at rest, including both infrastructure and tenant data.

  Since encryption requires secure key management, all qualified hardware platforms support TPM 2.0 (Trusted Platform Module), an international standard for a secure cryptoprocessor.

  Encryption is the best of all defenses against data theft, because encrypted data is worthless to hackers. If the Equifax hack data had been encrypted, 148 million Americans would sleep easier at night.

  The bottom line: Microsoft has "raised its game in security", and set the bar very high indeed. Even so, cyberattacks will become increasingly sophisticated and protecting customers will be a never ending challenge… which is why the Azure Stack security team has told us to expect more news in the coming months.

What about the customer security posture?

A robust infrastructure security posture is the indispensable foundation for cybersecurity. Even so, virtually all cloud data breaches take place in the Tenant's area of responsiblity.

Enterprise IT organizations need to work closely with their security partners (such as Atos) to ensure a strong customer security posture for the workloads they run on Azure Stack. Both Microsoft and third party specialists provide a number of useful tools, but processes and people are just as important.

Gary Burt
Global Product Manager,
Atos