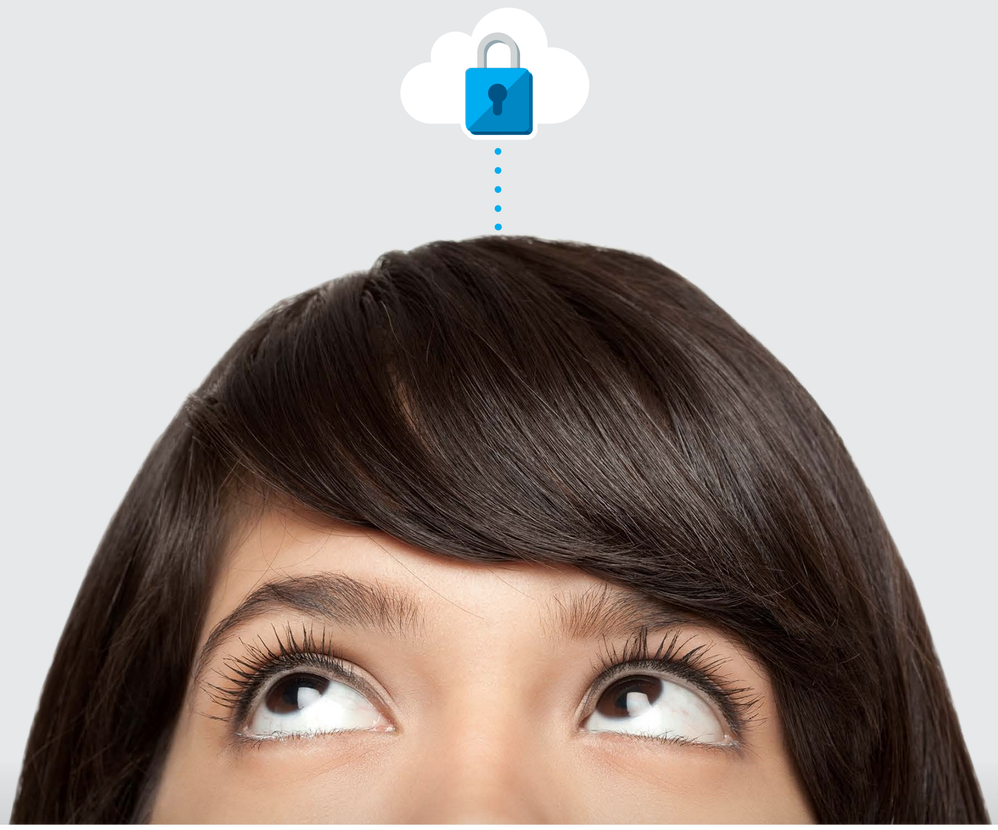
THE RIGHT DEFENSE FOR THE THREAT

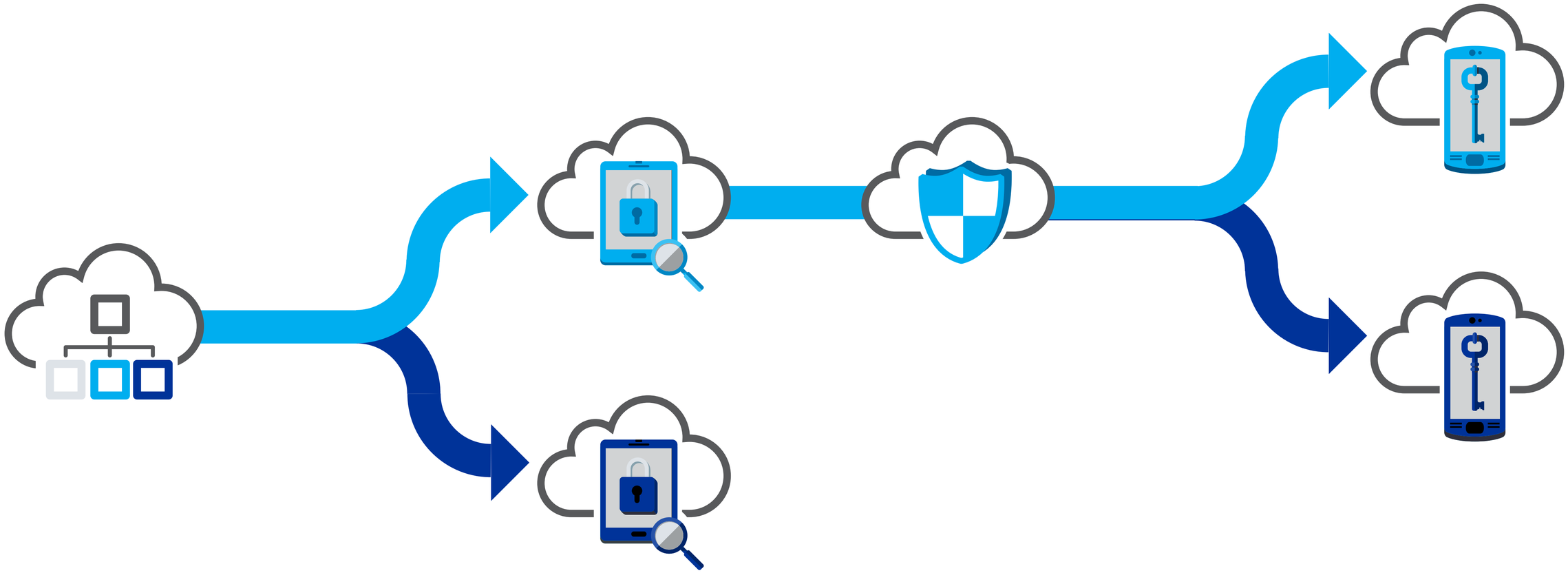
THE NEXT GENERATION OF MULTI-LAYERED CYBERSECURITY



Microsoft | TREND MICRO™

DIFFERENT JOURNEYS. DIFFERENT THREATS.

Every organization that migrates to the cloud will take its own path. And with 80% of organizations surveyed making the journey, that's a lot of different paths. Depending on where you are in your shift to the cloud, your security vulnerabilities will change, as will the cyberthreats you face. The question is, how do you protect against ever-evolving threats at each stage of the journey with a single strategy? And it's not simply about datacenter, firewall perimeters, or cloud-only measures. It's an ever-changing combination of targets and threats. This e-book offers one way to address all these threats within a single security framework. But first, we need a little context on cloud security.



SECURITY IN THE CLOUD IS A SHARED RESPONSIBILITY

Even experienced IT professionals often believe their cloud provider (Azure, AWS, Google, or others) provides security for everything that happens in the cloud.

It's important to know that's not the case. Microsoft Azure and other cloud environments secure the infrastructure and do provide some native threat protection, but protecting your applications and data running or stored in Azure, for instance—that's your responsibility.

Here's how the security responsibilities are divided in the Microsoft Azure cloud:

MICROSOFT CLOUD SHARED RESPONSIBILITY MODEL

ON-PREMISES
You are responsible for all security and operation.

INFRASTRUCTURE AS A SERVICE (IAAS)
You are responsible for things like buildings, servers, and networking hardware, as well as securing and managing the operating system, network configuration, applications, identity, clients, and data.

PLATFORM AS A SERVICE (PAAS)
Your provider is responsible for platforms established on IaaS deployments, as well as managing and securing the network controls.

You are responsible (or may share responsibility) for securing and managing applications, identity, clients, and data.

SOFTWARE AS A SERVICE (SAAS)
You are responsible for ensuring that data is classified properly and for managing your users and end-point devices. This is true even though your vendor may provide applications and abstracts.

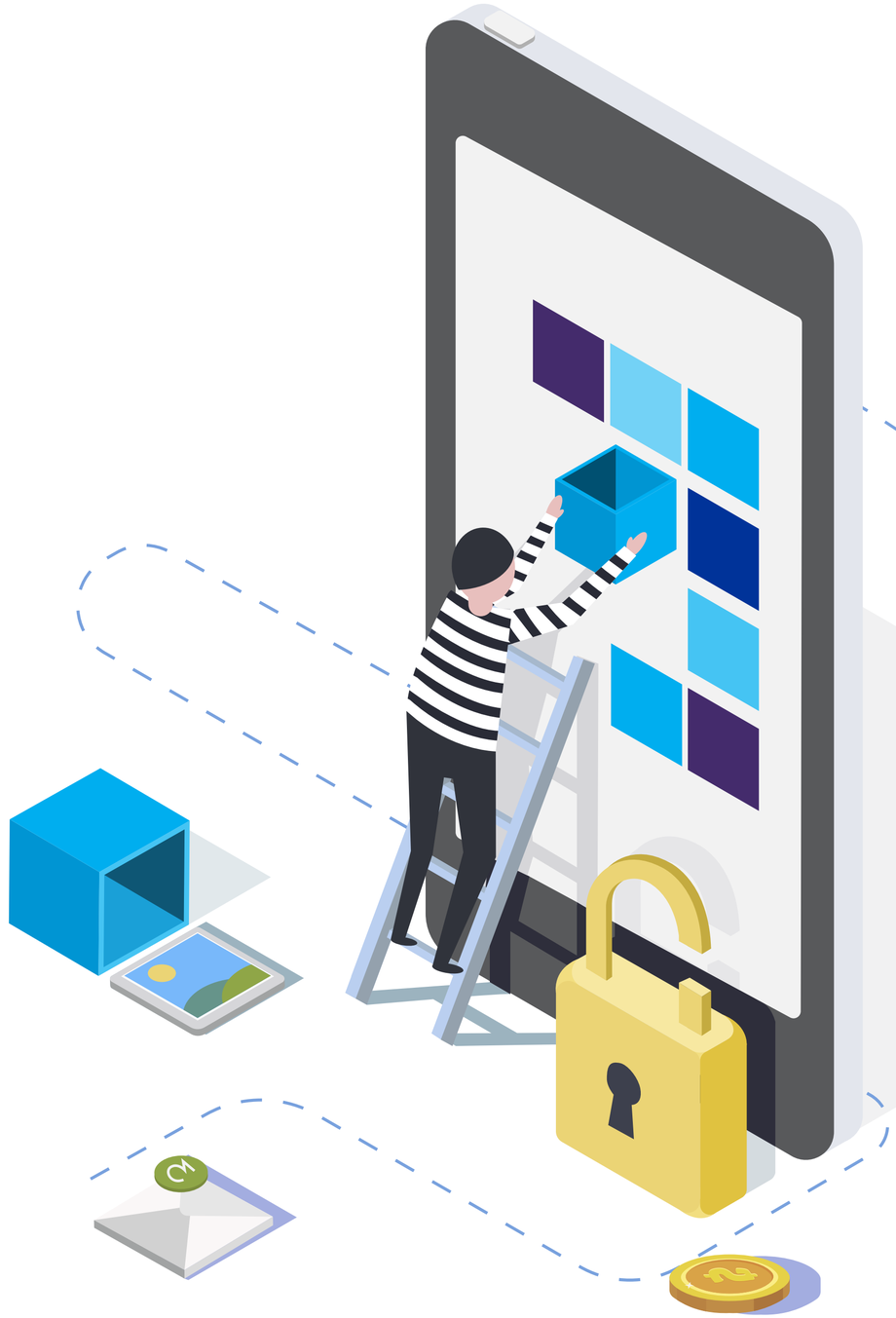
DESIGNED FOR AZURE. BUILT FOR SPEED.

Of course, the Azure cloud environment works best with security measures designed for it. Security products like those offered by Trend Micro are designed to work within Azure, making it easier for you to bake security automation into cloud workload platforms. Solutions like these, which are deeply integrated with Microsoft Azure, simplify security management for physical, virtual, and cloud workloads because they rely on a single comprehensive product with the ability to scale security at the speed of your business.

THE LAYERED THREATS IN A CLOUD JOURNEY

OLD-SCHOOL ATTACK: ON-PREMISES SERVER

Even if you're moving to the cloud right now, you may be leaving some critical applications and services on-premises for the foreseeable future. The threats to those physical resources will continue to be real as you maintain the applications, hardware, and any traffic patterns, right up until the moment you unplug them. Traditional security providers often specialize in datacenter security, but they tend to be slow to update hybrid and cloud measures. Ransomware is just as dangerous to the data stored down the hall as in the cloud. Security measures still need to be flexible, scalable, and easy to manage. However, cloud protection technology and approaches must be built to secure new access points and vulnerabilities. Security products such as Trend Micro Deep Security deliver multi-levels of protection within one solution that fits the needs of today's cloud environments. They're all part of an effective strategy, whether your environment is made up of physical, virtual, hybrid, or multi-systems for greater availability (blue/green deployments).



DANGLING END POINTS: "BYOD" IS "BRING YOUR OWN THREAT"

With the explosive growth of bring your own device (BYOD) and mobile cultures, end points are not only devices—they are people. And more people with devices means more risk. Those mobile workers using web-based services—email, web, and cloud apps—make users, not devices, your perimeter. For example, business email compromise (BEC) has resulted in billions of dollars being stolen through simple false invoices sent to executives. Sophisticated phishing and spear-phishing attacks have proven that people can still be a weak point. And ransomware often attacks through mobile and personal devices.

Once through the initial gateway to your system, threats can also capitalize on virtual machines to propagate, move without detection, and steal valuable data. The countermeasures for this kind of tactic include automated processes to quickly detect new virtual machines or changes to code and rapidly counter them, ensuring constant monitoring of your workloads.

THE FUNNEL APPROACH TO MULTI-LAYER DEFENSE

To counter all these threats with a single strategy, Trend Micro has found that a multi-layer funnel approach puts protection close to critical workloads, protecting servers and applications with a blend of threat defense techniques from modern to next generation. Using the right technique at the right time gives you the best protection against the broadest range of threats, with the most efficient performance for each environment, whether physical, virtual, or cloud.

At the top of the funnel, a wide range of powerful techniques allow known good data and actions through, but recognize and stop threats. At this stage, all known malicious or bad attempts are rejected. These techniques are highly accurate and efficient, and include:

- Antimalware and content filtering
- Intrusion prevention and firewall
- Integrity monitoring and log inspection

Once the relatively easily known threats are identified and dealt with, the remaining threats encounter increasingly sophisticated detection techniques that are more computationally intensive. But they are applied to a smaller number of attacks left in the funnel, reducing risk, conserving computing power, and preserving processing speed.

Security administrators know there is no silver bullet. Taking a pragmatic, multi-layered approach to security reduces the risk associated with single capability solutions or traditional security methods. One powerful technique deployed further down the funnel is machine learning. This technique looks at file features to predict maliciousness. Machine learning correlates threat information and performs an in-depth file analysis to detect emerging unknown security risks. This helps you determine if malicious code has slipped through and is sitting patiently, without being noticed.

Trend Micro Deep Security also provides behavioral analysis as part of a layered security solution. Behavioral analysis looks for actions that indicate maliciousness, such as encryption of files with ransomware. This final layer sends unknown suspicious files to a custom sandbox for specialized analysis in a contained environment. If these files are discovered to be malicious, that information is shared for enhanced protection across the enterprise's servers *and* end points.

Every threat protection technique has pros and cons, and there is no single technique that can detect every type of threat, particularly across multiple physical, virtual, and cloud environments. That's why the Trend Micro Hybrid Cloud Security solution, powered by XGen, delivers leading layered threat protection techniques that shield you from the broadest range of both known and unknown threats, end to end across the hybrid cloud.

CASE STUDY: ARMOR—BEYOND HOST SECURITY

Armor is a leading innovator and cloud computing security provider offering both public and private managed cloud services. Security is an important element of what Armor, based in Richardson, Texas, does at their datacenters in Dallas, Phoenix, Singapore, Amsterdam, and London.

"We put security at the front of every decision we make," says Jeremy Droege, Vice President of Cloud Operations at Armor. "That's essential if we're going to keep our customers secure."

When it comes to protecting Armor's multi-cloud environments, delivering end-to-end security is key. For example, with a prior security vendor, Armor had challenges rolling out security agents that would sometimes create disruptions for its customers. Droege explained, "Operating systems must get updated all the time and we struggled with new upgrades and patches."

As an innovative multi-cloud provider to customers with a wide range of use cases, Armor must secure credit card data subject to PCI regulations; healthcare data regulated by HIPAA; e-commerce data; and other sensitive information—a tall security and compliance order for any company.

Who secures the security company?

Droege described Armor's decision-making process: "When we evaluated security solutions, we found vendors that were strong in one area, but didn't meet our needs for an end-to-end security platform to run on any workload. Trend Micro Deep Security provided that platform."

As they adopted Deep Security, Armor immediately saw a marked uptick in the number of viruses and malware they were finding on their systems. "For us, that's an important proof point that Trend Micro's threat intelligence is truly world class," said Droege.

Deep Security allows Armor to secure virtual private cloud VMs—as well as Azure virtual machines—to provide customers with a single view of security. Armor relies heavily on Deep Security's APIs and security automation functionality to ensure security is in place and working. According to Droege, "Armor's primary goal is to provide security in a multi-cloud world. Trend Micro Deep Security helps us deliver that vision and keep our promise to customers."

In addition to providing security across virtualized environments, including Windows and Linux, Armor leverages Deep Security for all workstations inside their corporate environment. "With Deep Security, we have one platform that allows us to synchronize the host level security across both our customer and our own IT environments," said Jeff Schilling, Chief Security Officer at Armor.

SECURITY EVALUATION CHECKLIST

Ensure that your cloud security solution includes the following critical elements before moving forward.

- [ ] A single security offering across physical, virtual, cloud, and hybrid deployments
- [ ] A layered security approach that addresses threats with the most effective countermeasures
- [ ] The use of modern methods like artificial intelligence (AI) and behavioral analysis where they are most effective
- [ ] Protection of your enterprise at the right perimeters, whether at the datacenter, on mobile devices, or in the cloud
- [ ] Flexible licensing aligned to cloud deployments that shifts costs from CapEx to OpEx
- [ ] Deep integration with Azure, including full discovery and visibility of workloads across on-premises, hybrid, and cloud, as well as multi-cloud environments
- [ ] Comprehensive controls in a single product
- [ ] Automated high-performance security that fits the cloud and DevOps model

Microsoft Azure + TREND MICRO™

PUT YOUR DEFENSE WHERE THE THREATS ARE

As you move up to the cloud, traditional approaches to cyberdefense are not enough. Nor will resource-hungry bleeding edge technologies alone be your most effective protection. Trend Micro's comprehensive defenses are designed specifically to work with the Azure environment to provide you with security measures that meet the attack where it can most effectively be shut down.

Take advantage of an array of cloud computing resources and find out how moving up to the Azure cloud puts your organization on the road to improved business performance.

MOVE UP TO THE CLOUD.

CONNECT WITH **ZONES** ▶

ZONES

For more information, contact your
Zones account executive, or call 800.408.ZONES.

Microsoft