THREAT PREVENTION SECURITY FOR MICROSOFT AZURE HYBRID CLOUDS

INTRODUCTION

Enterprise IT is evolving from a hardware-centric to an application-centric model, enabling businesses to streamline processes, enhance competitive positioning and improve end-user experiences. As a result, IT infrastructure is now viewed as playing a more strategic role in the overall success of the business, putting pressure on IT organizations to rapidly transform in order to keep pace with business demands. The need to run processes more efficiently, improve time-to-market and enhance user experience is subsequently driving more and more businesses to embrace the cloud as part of their IT strategy.

The rising tide of cloud deployments is providing sufficient proof-points of the business benefits and fueling further cloud adoption. It is no longer a question of "if" but "when" an organization will start moving data and workflows to the cloud. Once the decision has been made, the next dilemma is determining which cloud deployment model meets the technology needs of the organization.

Public clouds are a natural fit for organizations that prefer to transfer the management of day-to-day infrastructure operations to a third party provider. Businesses that utilize public clouds benefit from a shared pay-per-use model that keeps costs low and improves business agility, but the public model raises concerns around data security, privacy and compliance. Private clouds, in contrast, are corporate owned and managed, provide greater data control and security but require substantially larger investments. Striking the right balance between costs, control and business agility is a key factor for the rise of the hybrid cloud model.

Hybrid cloud is the combination of private cloud infrastructure with one or more public clouds that are bound together to function as an extension of existing corporate systems and processes. Essentially, hybrid clouds deliver the best of both worlds; the agility, extensibility and cost saving benefits of public cloud environments coupled with the management benefits of leveraging tools and processes already in place in private clouds. Hybrid models enable greater flexibility in deciding where to allocate resources for maximum business impact.

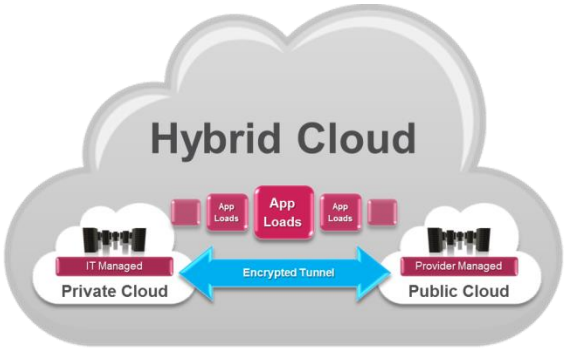

Figure 1: Hybrid Cloud combines private cloud with one or more public cloud offerings

Still, security concerns associated with moving data beyond IT control keeps many organizations from fully embracing the cloud. Businesses want the ability to control their own data and keep it private all while maintaining compliance with regulatory mandates. Thus, enterprise and IT leaders seek trusted partners, such as Microsoft Azure, to close the gaps between agility and security to confidently make the move to the cloud.

Microsoft Azure provides public and hybrid cloud services for a wide range of enterprise user cases. Azure is a unified, multi-tenant platform that utilizes a shared infrastructure to support millions of simultaneous customers world-wide. Foundational to the Azure cloud are enhanced security, operational management and threat mitigation practices that protect the Azure infrastructure, cloud fabric, hypervisors, services and tenant environments. Yet securing the infrastructure is just one piece of the overall cloud security puzzle. A defense-in-depth strategy for the cloud should also include the ability to protect workloads and data from exploits, malware and other sophisticated attacks.

Microsoft recently announced the Azure Security Center to give customers a centralized view of the state of their cloud resource security as well as help identify resources that require additional security services beyond the infrastructure protections provided by Azure. A key component of this strategy is the ability to recommend when and where to provision virtual security devices, such as Check Point CloudGuard IaaS, to protect customer data.

Check Point CloudGuard provides uncompromising protection against even the most sophisticated cyberattacks while dramatically simplifying IT security management. It seamlessly delivers advanced security protections to prevent malware attacks and data breaches while enabling secure connectivity to Azure public and hybrid cloud networks. Taking advantage of the cost efficiencies and automation of Microsoft Azure, CloudGuard is deployed and orchestrated through the Azure Security Center but is managed through a common policy and reporting engine as the corporate on-premises security infrastructure.

CHALLENGES OF MOVING DATA TO HYBRID CLOUDS

The growth and popularity of hybrid clouds continues to drive more data beyond traditional IT security protections – into data center environments no longer owned, managed or controlled by corporate IT groups. On-premises IT security controls do not touch the cloud, leaving customer data at risk from the same types of threats targeting applications in corporate data centers. What's more, malware introduced into the cloud can easily propagate among VMs, attack virtual segments or even ride unimpeded over VPN links back to corporate networks. While Azure provides strong security controls to protect the cloud fabric, it has no knowledge of "normal" customer traffic and thus is unable to determine malicious content from benign.

To fully embrace the cloud, businesses need to understand where the balance of responsibilities lie between protecting the cloud infrastructure (incumbent upon the cloud provider) and protecting the data that resides in the cloud (incumbent upon the customer). Security controls must now be shared between cloud providers and corporate IT, resulting in some rather unique security challenges, including:

- **Visibility into all traffic and threats** – with more and more data extending beyond corporate control, businesses are increasingly challenged to get a clear view of the workloads running in the cloud, including any threats and other malicious activity that could be introduced and/or affecting their data residing in the cloud. What's more, assets tagged or grouped in the cloud may not directly translate to corporate security schemas, leaving security teams guessing as to the exact extent of their attack surface and hampering their ability to mitigate risk.
- **Security management and enforcement** – as security controls are now shared with cloud providers, organizations struggle to maintain a consistent security posture for their extended application workloads and data. The tools and technology used to manage corporate security are quite different than the tools and technology employed by cloud providers, resulting in a lack of consistent security policies and enforcement.
- **Advanced protections against cyber threats –** on-premises solutions provide a rich set of application-level security and advanced malware protections, but similar tools are not part of the cloud security arsenal. Cloud providers utilize a shared responsibility security model – providing only one piece of the overall cloud security puzzle – leaving customers with a false sense of security for their cloud applications and data. Since corporate IT security doesn't touch cloud services organizations, their cloud assets are vulnerable to the same security exploits and threats as their on-premises assets.
- **Secure connectivity between public cloud and on-premises data center** – one of the key questions organizations face when looking into cloud ecosystems is how to create a connectivity strategy that leverages investments in on-premises equipment with hybrid cloud architectures without introducing additional complexity. At the same time, the security and reliability of connectivity are paramount as apps and data now have the ability to seamlessly migrate beyond corporate

controls to cloud. Maintaining consistent visibility and control of data while lowering the costs and complexities are also key considerations.

- **Logging and reporting** – toggling between multiple, disparate solutions makes getting a clear picture of network traffic and threat activity extremely difficult, especially as data and workloads migrate away from IT controlled equipment. Audits and compliance reporting are equally challenging as businesses and cloud providers utilize different tools, maintain and secure logs in different manners, and provide varying degrees of access controls for administration and reporting.

To address these challenges, Microsoft partnered with Check Point to offer customers comprehensive security protections for their hybrid cloud environments. Check Point CloudGuard for Azure provides industry-leading threat prevention security to keep Azure public cloud networks safe from even the most sophisticated attacks. The integration of Check Point CloudGuard enhances the native isolation and virtual networking of Azure to dynamically deliver the visibility, advanced threat prevention security and consistent policy enforcement customers need for protecting their hybrid cloud workloads and application data.

COMPREHENSIVE THREAT PREVENTION ARCHITECTURE FOR HYBRID CLOUDS

As cyber threats and attacks continue to increase in severity and frequency, organizations need comprehensive security protections not only for their physical locations but also to protect critical assets now migrating to public and hybrid clouds. Microsoft already provides the necessary safeguards to keep Azure cloud services and infrastructure secure. Now, by partnering with Check Point, Microsoft Azure can also allow organizations to address their cloud data security needs in a way that works with the elasticity and automation that characterizes public cloud architectures. Check Point provides a complete architecture to help organizations protect their physical and virtual workflows, data and assets.

CHECK POINT APPLIANCES AND VIRTUAL SYSTEMS

Check Point appliances with Advanced Threat Prevention security enable effective multi-layered defense against both internal and external threats. Deployed to protect the data center perimeter and core, these security gateways protect traffic entering and leaving the data center as well as provide robust security to mitigate east-west traffic threats within virtual data centers. As an example, if an infected application inside the data center attempts to communicate with a Command & Control site, Check Point's Anti-bot service will detect and block the communication.

Since hybrid clouds connect to corporate data centers, customers need advanced security solutions to keep these critical links protected. Check Point's line of data center appliances and chassis-based systems provide comprehensive protections for high-speed networks, delivering firewall throughput of up to 1 Tbps with ultra-low latency while providing modular scalability to grow and increase capacity when needed without compromising performance or security.

CHECK POINT CLOUDGUARD FOR MICROSOFT AZURE

Check Point CloudGuard delivers the same advanced, multi-layered security as the physical gateways in a dynamic package ideal for deployment in private, public and hybrid cloud environments. CloudGuard protects assets in the cloud from attacks while enabling secure connectivity from enterprise networks to Microsoft Azure hybrid clouds. Designed for the dynamic security requirements of cloud deployments, the CloudGuard integration with Azure goes beyond basic L2 – L4 capabilities to provide advanced security services including: Firewall, IPS, Application Control, IPsec VPN, Antivirus, Anti-Bot, and award-winning SandBlast sandboxing technology.

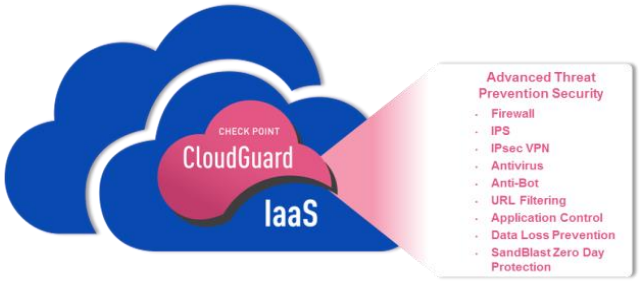

Figure 2: Check Point CloudGuard delivers comprehensive threat prevention security for Azure hybrid clouds

CloudGuard is a security VM deployed within a customers' Azure environment that is integrated with the Azure Security Center. It leverages APIs from Azure Security Center for traffic redirection and inspection, securing traffic coming in and out of a customers' Azure cloud as inter-segment traffic across virtual subnets. When the Azure Security Center identifies security gaps in a customer deployment, CloudGuard gateways can be provisioned and inserted to keep critical assets and data protected.

CloudGuard for Azure makes any Check Point Security Management server cloud-aware through an API integration with the Azure Security Center. This enables Check Point Security Management platforms to adjust security policies to manage any CloudGuard and physical gateways while providing complete visibility into all data center and cloud traffic. This integration allows CloudGuard to utilize objects and tags from a customers' Azure VNET environment in Check Point Security Management policies, providing context-aware policies that are tuned to protecting network topologies instead of IP addresses.

CloudGuard provides consistent security policy management, enforcement, and reporting, making migration to Azure cloud environments painless. Check Point CloudGuard is designed to be dynamically deployed, distributed and orchestrated through the Azure Security Center as a virtual security device, providing security automation with advanced threat prevention to protect customer assets in Azure hybrid clouds. The combined CloudGuard with Microsoft Azure solution delivers best-in-class threat protection and malware prevention for comprehensive security of cloud traffic and data.

CENTRALIZED SECURITY MANAGEMENT, VISIBILITY AND REPORTING

Effective monitoring and incident investigation requires robust security management. Enterprises expect their security visibility and monitoring solutions to provide a big picture view of relevant events without having to manually correlate a variety of screens, tools, or other resources. Check Point smart management solutions centralize and simplify security management for cloud-enabled businesses.

Check Point's SmartDashboard tracks and logs threats across the organization from a single pane of glass, while SmartEvent provides visualizing and correlating of events across the entire distributed network, from the data center to hybrid clouds. Check Point's SmartConsole management solution can manage physical and virtual gateways across both on-premises and cloud networks, allowing IT to set security policies for both environments from a single interface. This ensures consistent security across all gateways without the expense and complexity of toggling between separate management consoles. Seamless integrating with Microsoft Azure enables security policies to leverage Azure objects and tags across both Check Point CloudGuard (for cloud traffic inspection) and Check Point gateway appliances (for data center traffic inspection).

The Check Point Smart Dashboard provides real-time visibility into activity that spans the data center to the Azure public cloud, ensuring that the right level of protections are applied consistently across both hybrid cloud and physical networks. Hybrid cloud workload traffic is logged and can be easily viewed within the same dashboard as other security logs. Customers can even deploy Azure infrastructure services on-premises with Azure Stack enabling management consistency and workload compatibility across both private and public cloud infrastructures, creating a single Azure hybrid cloud.

Figure 3: Check Point SmartConsole delivers consistent security management across public and private clouds

The CloudGuard integration with the Azure Security Center is also designed to provide valuable contextual information about the customers cloud environment. Virtual objects learned by the CloudGuard Controller, such as security groups or VMs, can then be

used in security policies defined via SmartConsole and installed on any CloudGuard gateway. As a result, policy management becomes easier by using less abstract names and security policy creation time goes from minutes to seconds.
What's more, the level of contextual awareness between Azure and the CloudGuard Controller make it possible for security protections to be enforced on virtual applications regardless of where they are created or located. This also enables business group or application aware policies that span and consolidate both data center and Azure cloud network traffic as well as across both virtual and physical security gateways. That level of consolidation extends to simplified operations management, including notification and reporting as well.

CloudGuard for Azure gives businesses the confidence to securely extend their data center resources and workloads to hybrid clouds, providing tangible benefits such as:

- Protection against security breaches, malware, and zero-day attacks in the public cloud that may lead to private cloud / data center breaches
- Unified security management, visibility, and reporting across both private and public cloud networks
- Automated workflows and orchestration to minimize configuration errors
- Elimination of the costs and loss of reputation associated with business disruptions and downtime
- Migrate sensitive workloads, applications and data to the public cloud with confidence

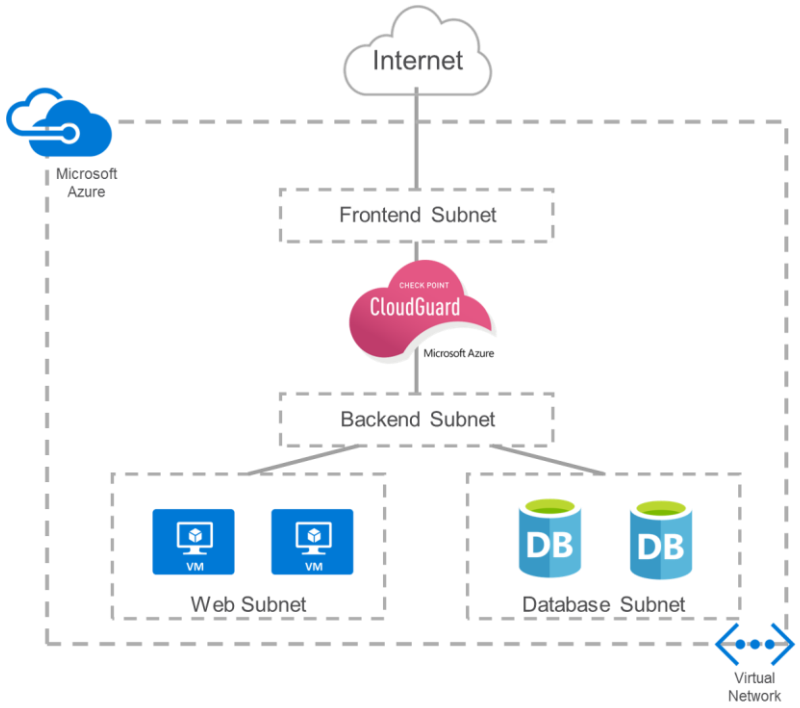

Figure 4: Check Point CloudGuard advanced security for Microsoft Azure cloud environments

SUMMARY

The desire to transform business to achieve greater agility is driving more application workloads to cloud environments. Businesses looking to streamline processes to enhance competitive positioning and improve overall user experiences are also keenly aware of the security concerns associated with migrating assets and data to locations IT controls no longer touch. As a result, organizations are looking for comprehensive solutions to bridge security gaps and deliver consistent protections, visibility and control for their data center ***and*** cloud assets and data.

Check Point Software Technologies provides uncompromising protection against even the most sophisticated cyberattacks while dramatically simplifying IT security management. Check Point CloudGuard takes advantage of the cost efficiencies and automation of Azure while tightly integrating advanced security features designed to meet the efficiency and scalability requirements of public cloud infrastructures. This comprehensive security architecture enables Check Point best-of-breed network security services to be dynamically inserted in Azure hybrid environments for extremely granular control, enhanced visibility and superior threat prevention. What's more, CloudGuard provides the framework to allow organizations to securely adopt cloud-based infrastructure - whether public, private or hybrid - with consistent policies, enforcement, logging and reporting across their physical and virtual infrastructure.

Check Point CloudGuard for Azure enables customers to confidently extend advanced network security to their Azure cloud infrastructure with the full range of protections of the Check Point threat prevention architecture. CloudGuard for Azure prevents network attacks and data breaches while enabling secure connectivity to Azure public cloud environments. Working together, Microsoft Azure and Check Point have integrated their best-of-breed cloud virtualization and advanced threat prevention technologies to enable the efficient delivery of applications and security assurance to realize the full value of hybrid cloud architectures.

Microsoft Azure Certified

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com