paloalto NETWORKS | Microsoft Azure

Secure Your Azure Environment

A unified solution tackles today's security challenges

Table of Contents

Our Customers' Needs are Changing

Here at Palo Alto Networks, we recognize the critical importance and value of securing your Azure cloud network, protecting your sensitive data, and supporting your mission-critical workloads.

To support our customers, we are helping them by revolutionizing and reinventing how they do business by:

- Enabling innovation and rapidly delivering value from applications by freeing up resources
- Delivering enhanced customer and employee experiences
- Driving differentiation through agility, product and process scalability, and overall business optimization

In this eBook, we will explore key insights into Palo Alto Networks Cloud NGFW for Azure, understand the value of a hybrid or multicloud approach to security, and help you address the unique security challenges of your Azure environment.

paloalto NETWORKS | Microsoft Azure

The Cloud Security Landscape is Constantly Evolving

The dynamic and flexible nature of cloud environments bring forth new security challenges that organizations must address. These challenges include protecting sensitive information, maintaining compliance, and safeguarding against emerging threats that increase the risk of data breaches, unauthorized access, and lack of visibility and control.

Data Breaches and Unauthorized Access

Cloud environments are prime targets for cybercriminals. Inadequate security measures and misconfigurations can lead to data breaches.

Compliance and Regulatory Requirements

Organizations must navigate a complex web of compliance regulations and industry-specific standards when operating in the cloud.

Lack of Visibility and Control

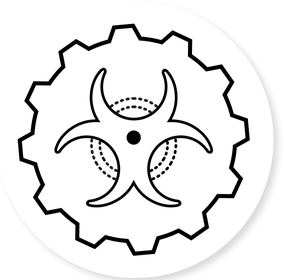
Cloud environments often involve multiple platforms, services, and applications, which make gaining comprehensive visibility into network traffic, user activities, and potential security threats challenging.

Advanced Persistent Threat (APT) Examples

A few examples of APT threats from the last decade include:

Stuxnet:

“First discovered in 2010, the Stuxnet computer worm targeted the computer hardware of Iran’s nuclear program. It was the first malware that targeted industrial control systems and had several variations in operation until at least 2012.”



NotPetya:

“Russian hackers were behind the notorious NotPetya malware that was originally dispatched to knock out government and infrastructure targets in Ukraine in 2017 before spreading widely throughout the world. A U.S. government assessment pegged the total damages brought about by NotPetya to more than $10 billion.”

What is an Advanced Persistent Threat (APT)? | Graphus ›

Exploring Palo Alto Networks Cloud NGFW for Azure

Offering a comprehensive, integrated solution to secure your Azure environment. In this section, we will delve into the key features and capabilities of Palo Alto Networks Cloud NGFW and explore how it can enhance the security posture of your Azure deployments.

Key Features and Benefits:

Integration with Azure:

Palo Alto Networks Cloud NGFW seamlessly integrates with Azure services, providing consistent security policies and visibility across your Azure environment.

Advanced Threat Prevention:

Cloud NGFW incorporates advanced threat prevention mechanisms to detect and block sophisticated attacks, including malware, zero-day exploits, and command-and-control communications.

Secure Application Access and Control:

This solution offers granular control over application access, enabling you to define and enforce policies based on application characteristics, user identity, and context. Ensuring secure access to applications in the cloud, preventing unauthorized access, and protecting sensitive data from exfiltration.

Centralized Security Management:

With a centralized management console, Cloud NGFW simplifies security policy management, configuration updates, and monitoring across your Azure environment. Providing a unified view of security events and alerts, empowering security teams to respond to threats and maintain compliance efficiently.

Scalability and Elasticity:

Palo Alto Networks Cloud NGFW scales dynamically with your Azure environment, adapting to changing demands without compromising security or performance. Allowing for seamless expansion as your organization grows, ensuring that your security infrastructure can keep pace with your evolving cloud requirements.

Exploring Palo Alto Networks Cloud NGFW for Azure

Palo Alto Networks Cloud NGFW protects the following Azure cloud workloads:

Cloud Native Apps

By providing a fully managed, Azure-native service with consistent best-in-class security, Cloud NGFW for Azure allows customers to focus on innovation that grows and delivers business value from applications instead of maintaining underlying infrastructure—all while extending security management seamlessly from on-premises to Azure.

Migrated Apps

Whether migrating legacy applications or building cloud-natives on Azure, fully protecting those applications is crucial. Cloud NGFW for Azure offers the powerful machine learning technology and advanced security capabilities customers need to defend against a quickly changing threat landscape.

Azure Virtual WAN

Our managed firewall service even integrates with Azure Virtual WANs so customers can protect traffic across their entire networks. Behind the scenes, Palo Alto Networks takes care of scaling, resilience, and software upgrades. With Cloud NGFW for Azure, customers can focus their time on security instead of managing infrastructure.

Palo Alto Networks Cloud NGFW for Azure Features

Palo Alto Networks Cloud NGFW offers a comprehensive, integrated solution to secure your Azure environment. In this section, we will delve into the key features and capabilities of Cloud NGFW and understand how it can enhance the security posture of your Azure deployments.

Advanced Threat Prevention

Palo Alto Networks Cloud NGFW incorporates advanced threat prevention mechanisms to detect and block sophisticated and evolving attacks.

It also includes malware, zero-day exploits, and command-and-control communications.

Comprehensive Visibility and Control

The solution offers visibility into application usage, user activity, and network traffic, enabling effective monitoring and analysis.

This enhanced visibility empowers security teams to enforce security policy for a robust and secure Azure environment.

Centralized Security Management

A centralized management console simplifies security policy management, configuration updates, and monitoring across your Azure environment.

Providing a unified view of security events and alerts, empowering security teams to respond to threats and maintain compliance efficiently.

Compliance in the Cloud

Palo Alto Networks Cloud NGFW enables compliance by integrating with frameworks, providing continuous monitoring, auditing, and reporting.

It enforces data protection and privacy through DLP policies, encryption, and access controls.

Advanced Threat Prevention in the Cloud

Threat Intelligence and Prevention

Threat intelligence feeds and machine learning algorithms identify and block known and unknown threats in real time.

Sandboxing and Behavioral Analysis

Sandboxing and behavioral analysis techniques identify and analyze suspicious files and activities in a controlled environment. Palo Alto Networks Cloud NGFW can detect and block zero-day exploits and targeted attacks that may bypass traditional security measures.

Secure Web Gateway Functionality

Similar to a secure web gateway, the solution provides comprehensive protection for web traffic. It prevents access to malicious websites and content by applying URL filtering, web categorization, and SSL decryption.

Threat Hunting and Incident Response

Security teams can proactively hunt for threats and investigate security incidents within their Azure environment. With comprehensive visibility into network traffic and security events, organizations can quickly identify and respond to potential breaches, minimizing the impact of security incidents.

paloalto NETWORKS | Microsoft Azure

Ensuring Comprehensive Visibility and Control

Visibility and control are essential components of a robust cloud security strategy. Let's explore how Palo Alto Networks Cloud NGFW ensures comprehensive visibility into your Azure environment and empowers you with granular control over network traffic and security policies.

Application Visibility and Control

With deep visibility into application traffic, organizations can identify and classify applications running in their Azure environment. Granular application-level controls enable defining policies based on application characteristics, user identity, and business requirements, ensuring secure and compliant usage.

User Activity Monitoring

The solution offers user activity monitoring capabilities, allowing organizations to track and analyze user behavior, access patterns, and potential security risks by monitoring user activity. Palo Alto Networks Cloud NGFW helps detect and mitigate insider threats, unauthorized access attempts, and suspicious user behavior.

Network Traffic Analysis

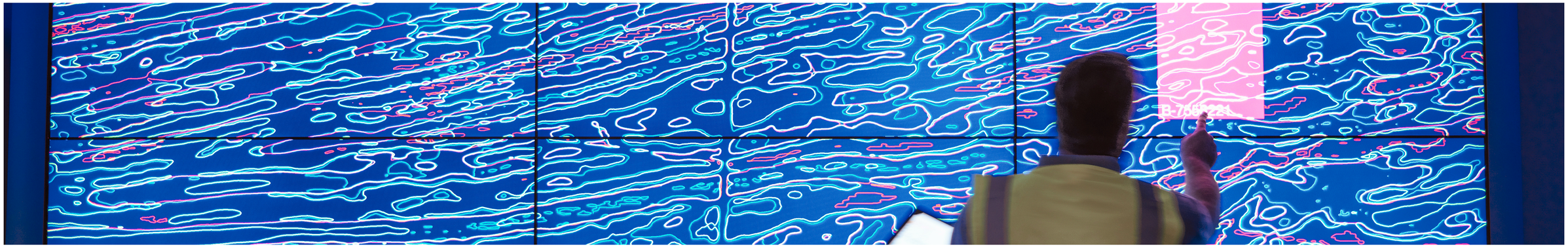
The detailed network traffic analysis gives organizations visibility into network flows, connections, and potential anomalies. Real-time monitoring and analysis of network traffic help identify and respond to network-based attacks and data exfiltration attempts.

Security Policy Enforcement

Organizations can define and enforce granular security policies based on their unique requirements. The solution offers the flexibility to create policies based on application characteristics, user identity, network segments, and other contextual factors, ensuring consistent security across the Azure environment.

Panorama Centralized Security Management

Palo Alto Networks Cloud NGFW is an Azure-native next-generation firewall that leverages machine learning to stop more zero-day attacks than traditional security solutions. Delivered as a managed service, it enables you to easily extend best-in-class security when your network extends to Azure, and enables you to manage network security centrally using Panorama.



Policy Management

The centralized policy management framework enables organizations to define, deploy, and enforce security policies consistently across their Azure environment. Administrators can create and manage policies based on application characteristics, user identities, network segments, and other related factors.

Configuration and Deployment

The centralized security management capabilities simplify the configuration and deployment process for security resources in Azure. Administrators can efficiently manage firewall rules, network settings, and other security configurations from a single interface.

Monitoring and Reporting

The solution provides comprehensive monitoring and reporting functionalities through a centralized management console. Security teams can monitor network traffic, track security events, and analyze logs and alerts from a unified interface, to promptly identify and respond to security incidents, minimizing potential threats.

Scalability and Flexibility

The centralized security management capabilities offer scalability and flexibility to accommodate the dynamic nature of cloud environments. As organizations scale their Azure infrastructure, the centralized management platform seamlessly scales, providing consistent security management and visibility across the expanded cloud network.

Ensuring Compliance in the Cloud

Maintaining compliance with industry regulations and data protection standards is critical for organizations operating in the cloud. Let's explore how Palo Alto Networks Cloud NGFW helps ensure compliance and simplifies regulatory adherence in Azure environments.

Compliance Framework Integration

Palo Alto Networks Cloud NGFW for Azure streamlines compliance efforts by providing predefined security controls and policy templates. It maps security controls to specific compliance requirements, helping organizations meet regulatory obligations effectively, such as GDPR and HIPAA.

Continuous Compliance Monitoring

The continuous compliance monitoring capabilities assess the security posture of your Azure environment against defined compliance frameworks. Real-time monitoring, automated assessments, and reporting functionalities enable organizations to promptly identify and address compliance gaps, ensuring ongoing adherence to regulatory requirements.

Auditing and Reporting

With comprehensive auditing and reporting capabilities, organizations can generate detailed compliance reports, demonstrating adherence to regulatory requirements. Customizable reports, audit logs, and event correlation simplify compliance audits, providing evidence of security controls in place. This helps organizations maintain transparency and accountability in their compliance efforts.

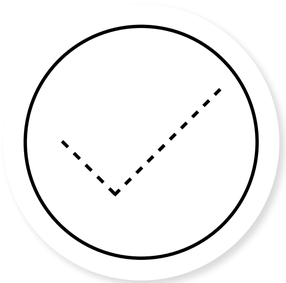
Data Protection and Privacy

Palo Alto Networks Cloud NGFW for Azure helps protect sensitive data and maintain privacy by enforcing data loss prevention (DLP) policies, encryption standards, and access controls. By securing data at rest, in transit, and in use, the solution mitigates the risk of data breaches and safeguards customer privacy. This capability ensures compliance with data protection regulations and builds trust with stakeholders.

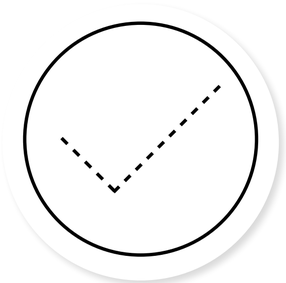
Azure Key Vault Integration

Cloud NGFW for Azure supports Azure Key Vault integration. This integration enables Cloud NGFW for Azure to detect and stop threats in all traffic, including encrypted traffic.

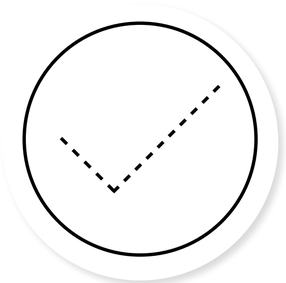
Stay Vigilant in the Face of Evolving Cybersecurity Threats



Palo Alto Networks Cloud NGFW for Azure provides organizations with the tools and capabilities to secure their Azure environments effectively. By embracing this solution, organizations can confidently navigate their cloud landscape, protect their assets, and achieve their business goals with peace of mind.



As you embark on your cloud security journey, Palo Alto Networks is here to support you every step of the way. Our team of experts is available to provide guidance, conduct demonstrations, and assist with integrating Cloud NGFW into your Azure environment effectively and efficiently. Together, we can strengthen your cloud security posture, protect your critical assets, and enable your organization to thrive in the multicloud era.



Cloud security is an ongoing commitment, and you can stay informed about the latest threats, security best practices, and updates by adopting Palo Alto Networks Cloud NGFW for Azure. Explore additional resources, engage with our community, and continue to evolve your security strategy to address emerging challenges and trends in the cloud landscape.

Microsoft and Palo Alto Networks Working Together

Microsoft and Palo Alto Networks have partnered to provide a powerful, seamless cloud security solution.

By combining the strengths of Microsoft Azure's cloud platform and Palo Alto Networks Cloud NGFW's advanced security capabilities, organizations can achieve comprehensive protection for their cloud environments. Microsoft Azure offers unmatched scalability, enabling organizations to easily reach their cloud resources as needed. With Microsoft Azure's constant innovation, you can access a wide range of cloud services, empowering you to build, deploy, and manage applications efficiently. Palo Alto Networks Cloud NGFW enhances Microsoft Azure's security capabilities by providing advanced threat prevention, centralized security management, and comprehensive visibility and control. This partnership ensures that your cloud workloads are protected against progressive threats while simplifying security operations and enabling you to enforce consistent security policies. Microsoft Azure and Palo Alto Networks Cloud NGFW for Azure offer a complete cloud security solution that addresses modern organizations' scalability, innovation, and advanced threat protection needs. Embrace the power of this partnership and secure your cloud environment with confidence.

Secure your cloud environment with Cloud Next-Generation Firewall by Palo Alto Networks, an Azure Native ISV Service—now in preview | Azure Blog | Microsoft Azure ›

paloalto NETWORKS | Microsoft Azure

Next Steps:
Strengthen Your Cloud Security

Contact Us

Get in touch with a Palo Alto Networks representative ›

paloalto NETWORKS | Microsoft Azure