53% of Organizations

Consider security concerns to be their top challenge when moving to the cloud

42% of Companies

are deploying additional security software to protect data and applications in the cloud

Use Cases:

- Enterprises
- Managed Service Providers
- Government Organizations
- Universities
- Hospitals
- Highly Secure Organizations

Industries:

- Aerospace and Defense
- Automotive
- Banking
- Consumer Products
- Defense and Security
- Engineering and Construction
- Healthcare
- High Tech
- Higher Education and Research
- Insurance
- Life Sciences
- Media
- Oil and Gas
- Professional Services
- Public Sector
- Retail
- Telecommunications
- Travel and Transportation
- Utilities
- Wholesale Distribution

5nine Cloud Security for Azure

The only security suite specifically designed and optimized for Microsoft Azure

As organizations move their services to the public cloud, security becomes increasingly complex as administrators no longer have access to physical hosts and networks. This means that all of their computing services need to be virtualized and managed remotely, including security. While public clouds offer many security benefits, the generic solutions provided by Microsoft Azure are limited and not purpose-built for the rapidly changing security needs of today's enterprise. Until now, users still had to rely on multiple third-party vendors to obtain end-to-end protection for their environments.

5nine Cloud Security for Azure is a new Azure Marketplace solution which addresses all of these challenges by taking the industry's leading security solution designed for Hyper-V and adapting it to the public cloud. With knowledge gained from almost a decade of experience protecting and managing Microsoft virtual machines on behalf of our customers, 5nine now offers a virtual router which monitors and inspects network traffic in Microsoft Azure. Now organizations can use 5nine to manage and protect their private, public and hybrid clouds.

5nine Cloud Security protects Azure virtual machines, networks and disks. Organizations can take advantage of a simple GUI console, which includes a virtual firewall, agentless antivirus with optimized scanning, deep packet inspection, intrusion detection (IDS), and network analytics with granular user and tenant access control. Today, businesses of any size can meet their industry's compliance and regulatory needs without deploying multiple point solutions.

53% of organizations consider security concerns to be their top challenge to moving to the cloud
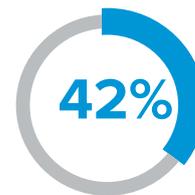
42% are deploying additional security software to protect data and applications in the cloud

Source: CloudPassage

Introducing Cloud Security for Azure

5nine Cloud Security provides the most comprehensive security suite for Microsoft Azure, delivering a virtual firewall, antivirus protection, intrusion detection (IDS), deep packet inspection, and network analytics in a single solution.

Manage Azure Subscriptions: 5nine Cloud Security for Azure lets IT administrators enter their Microsoft Azure credentials directly into the 5nine console to easily protect their Azure VMs. With 5nine Cloud Security, admins simply select the resource groups that they want to monitor, and 5nine takes care of the rest.

Virtual Firewall: The 5nine Cloud Security vFirewall allows organizations to control all inbound, outbound, and VM-to-VM traffic by inspecting network packets before they reach their virtual machines and virtual networks.

Deep Packet Inspection (DPI): Deep packet inspection of both HTTP and DNS packets allows the data portion of these packets to be inspected for specific strings or URLs, as determined by the administrator.

Agentless Antivirus: 5nine delivers built-in AV so that organizations do not need to separately acquire and deploy third-party antivirus solutions. 5nine Cloud Security protects VMs at the networking layer through its virtual router, so it does not require any antivirus agents to be installed. 5nine uses its patented Change Block Tracking (CBT) technology, which only analyzes files that have been created, accessed or changed since the last scan, allowing scans that are up to 70X faster than comparable AV solutions.

5NINE | Mission Control for the Microsoft Cloud

Technical Differentiators:

- Unified Security Suite
- Automatic and Immediate Protection
- Intuitive Interface
- Easy Network Logging
- Intuitive Interface
- Supports Any Guest OS
- Prevents Antivirus Storms
- Agentless Introspection
- Tenant Isolation
- No Hardware Required

"The right fit for your business may require a well-balanced blend of private and public cloud environments. Until now, each required its own unique tools for configuration, maintenance, monitoring and security-compounding complexity and overhead. Instead, the 5nine platform empowers you to approach your hybrid cloud as a single enterprise that is scalable, extensible and agile."

— William Fellows, 451 Research

451 Research

Awards

NETWORK PRODUCTS GUIDE
IT World Awards 2018 SILVER

INFOSEC AWARDS WINNERS
Cyber Defense Magazine 2018

SC 2017 awards
finalist

EDITOR'S CHOICE
VIRTUALIZATION
2016

Intrusion Detection System (IDS): Cisco Snort IDS rules are integrated into 5nine Cloud Security to identify different types of network attacks, including DoS/DDoS, direct access attacks, cross-site scripting, brute force, buffer overflows, CGI attacks, stealth port scans, and much more.

Automatic Protection: 5nine Cloud Security delivers the ability to automatically and immediately protect a newly created VM in an Azure Resource Group. Any newly created VM can have virtual firewall, antivirus or intrusion detection (IDS) automatically enabled for instant protection.

Quality of Service (QoS): Network bandwidth management can be configured on each VM, which prevents any VM from consuming too much of the network and negatively impacting the performance of other VMs, services or users.

Network Statistics & Analytics: Administrators can view all inbound and outbound network traffic statistics and connections, which provides complete visibility into the virtual network's usage.

Network Logging: 5nine Cloud Security for Azure logs all network traffic within the user's Azure Resource Groups, enabling administrators to filter the data or perform advanced analytics for testing, optimization or incident triage.

Internal Events Logging: Any time that 5nine Cloud Security performs a change to its security management system, services, or any other virtual infrastructure component which it manages, these changes are logged. This allows administrators to understand the health and state changes of the security system itself, as required by most compliance standards.

User Actions Logging: Many compliance standards require internal user action logging, to ensure that malicious admins do not attempt to hide mistakes or otherwise cover up a security vulnerability. 5nine Cloud Security logs all user actions and the results of the corresponding changes, enabling easy and simple audit.

Granular User and Tenant Management: 5nine offers role-based access control for each administrator and tenant. By separating users and their resources, 5nine reduces the risk of threats being passed between them, and this enables service providers to offer Security as a Service (SECaaS) as a new revenue channel.

Alerts and Email Notifications: 5nine Cloud Security provides a variety of email alerting options so that administrators can be notified immediately when an issue is detected. Communication frequency can be configured by different threat categories.

Centralized Security Management: 5nine Cloud Security for Azure is managed from a centralized GUI console, removing the need for administrators to log into the Azure Portal to manage their security.

Try 5nine Cloud Security

Download a free 14-day trial of 5nine Cloud Security at 5nine.com/security

For more information, visit 5nine.com

CONTACT US

Sales:

Phone US: + 1 561-898-1100

Phone EU: + 44 (20) 7048-2021

Email: sales@5nine.com

Technical Support:

Phone US/Canada: + 1 561 898-0076

Phone EMEA: + 44 131 357 6300

Email: support@5nine.com

Microsoft Partner
Gold Datacenter
Silver Cloud Platform
Microsoft

5NINE