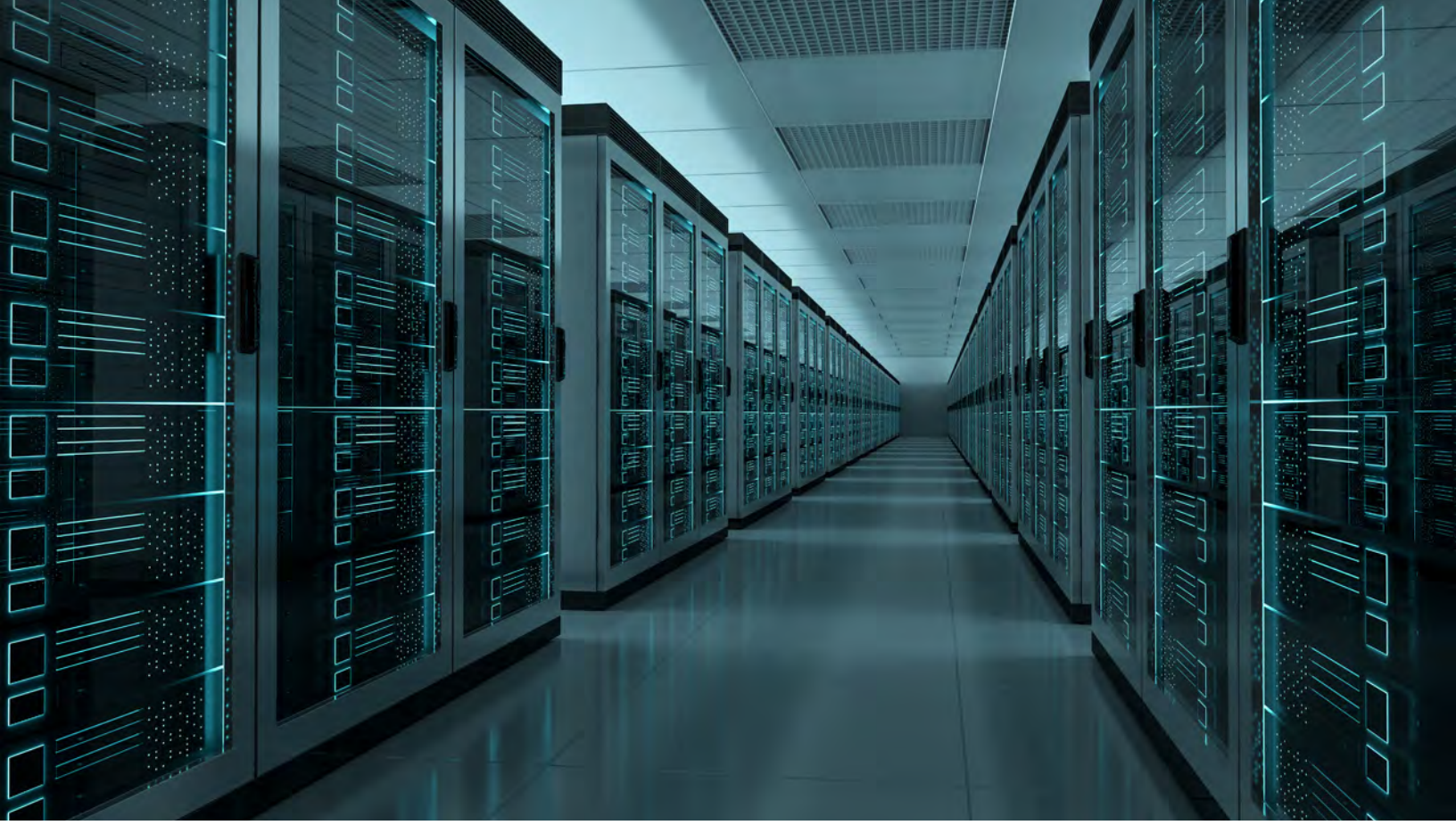

Verizon Hosted Network Services (HNS)

Security Posture and Overview

verizon

HNS Security Responsibilities

Verizon is responsible for protecting the global infrastructure for HNS. This infrastructure is comprised of the hardware, software, networking and facilities that run HNS. Verizon routinely audits our infrastructure internally to determine whether our systems are deployed with industry approved security best practices applied. Details on our auditing practices are covered later in this document.

Customer Security Responsibilities

Verizon provides cloud services using the Infrastructure as a Service model. Verizon is responsible for the installation, configuration, management, maintenance and security of HNS.

HNS Security

A five-pronged approach to security is used for platform and infrastructure security. The five areas are as follows:

Penetration Testing and Automation – the practice of using external, third party vendors to simulate a malicious attack on the HNS infrastructure to determine potential attack vectors and vulnerable services or applications both from an external and internal perspective. Internal penetration tests are also conducted randomly, where appropriate, to validate ongoing security remediation efforts.

Zone 3 Security – a broad set of policies, technologies, and controls deployed to protect data, applications, and HNS infrastructure ranging from the use of OpenStack Security Groups for network protection to the application of endpoint security tools to detect potential virus or malware infections onvirtual systems.

Infrastructure Hardening, Auditing and Compliance – checking that the HNS infrastructure elements (Servers, Routing and Switching Elements, and Hypervisor Resources) are compliant with industry standard security practices and that systems have security updates applied to reduce the risk of malicious access via known vulnerabilities.

IP Routing and Perimeter Hardening – the protection of the HNS infrastructure and associated Zone 3 spaces by way of IP
networking, virtual Layer 2 networks and ACLs, only allowing IP communications between systems or elements that fall within accepted Verizon business policies.

DDoS, IDP/IPS – software and hardware elements that are deployed to constantly monitor HNS network traffic, comparing that traffic against signatures which define malicious or abusive activity and which protect the HNS infrastructure from volumetric attacks designed to consume all network or computing resources and impact HNS's resource availability to customers.

Penetration Testing

In an effort to stay current with mainline Openstack code deployments, the HNS engineering and deployment teams are constantly vetting and testing new features as they become available with each Openstack software release. Since Verizon works closely with Red Hat for our deployment software and methodologies, Verizon determines whether each OSP version that we deploy to production sites has been fully vetted from a security perspective.

To that end, Verizon employs several external third party vendors who specialize in Penetration Testing or "white hat" hacking to access our deployments in a controlled environment. These vendors attempt to compromise the security controls that inherently exist in the Openstack APIs and services running on our infrastructure.

Reports of findings are generated after each penetration test, and vulnerabilities are tracked and remediated before any given OSP version is approved for production deployment.

Network Security / Security Groups
Verizon is responsible for managing and maintaining network security policies through the use of Security Groups. NNO Data Services Engineering resources will monitor these rules for Verizon to determine whether a high level of security is applied while still allowing the applications behind them to remain functional.

Infrastructure Hardening and Auditing

The goal of Infrastructure Hardening and Auditing is to determine whether the HNS Infrastructure has a high level of security applied to it, while allowing it to remain a functional cloud platform. System level audits are conducted and security best practices are applied to harden our systems before being considered a production element and mechanisms are constantly being developed to automate the application of these standards and the reporting of the audit results.

Each production HNS node is regularly scanned with Symantec's ESM and the open-source security product, OpenSCAP.

Results of the ongoing scans are archived for future reference.

IP Routing and Perimeter Security

By selectively allowing or restricting what IPs and networks Verizon advertises throughout the business and to other companies or the Internet, Verizon controls who can or cannot access certain network resources. As part of a "defense in depth" strategy, Verizon uses this methodology to reduce risk and attack vectors available to external parties or internal groups who do not need access.

VRF/VLAN Isolation

VRFs and VLANs are used as a means to logically isolate networks or network resources from each other. The use of these technologies is yet another way that Verizon limits application visibility and the HNS Engineering and Security Teams work to provide HNS access to only authorized parties.

ACL Enforcement

IP Routing goes hand in hand with the use of ACLs as a means to restrict or permit what network resources a remote user can access. ACLs controls access based on whether the customers IP or IP Network appear on an ordered list that grants or restricts access to specific network resources.

Network Security Monitoring

Network Security Monitoring is the function which allows the Verizon security and incident response teams to see what traffic is traversing the network and what that traffic is attempting to do.

DDoS Monitoring

Radware Anti-DDoS appliances will be used to help protect HNS from these types of attack in addition to a subscription based, chargeable online traffic scrubbing solution currently offered by Verizon. Both of these solutions have the ability to detect 'bad' traffic and clean it off the wire, only passing legitimate traffic on to the intended endpoint. Malicious traffic is absorbed by the Anti-DDoS solution, keeping the HNS infrastructure available to handle legitimate customer traffic.

IDS/IPS Strategy

Intrusion Detection Systems and Intrusion Prevention Systems detect and prevent unauthorized or malicious traffic from entering the network, typically through some sort of gateway or choke point through which all traffic must flow. These devices are deployed in all HNS locations and will mark bad traffic and generate alerts based on known bad source IP addresses, known bad network behavior characteristics and by matching signatures.

- Intrusion Detection System – A device or application that analyzes whole packets, both header and payload, looking for known events. When a known event is detected a log message is generated detailing the event.
- Intrusion Prevention System – A device or application that analyzes whole packets, both header and payload, looking for known events. When a known event is detected the packet is rejected.

Vulnerability Scanning

Routine vulnerability scanning is conducted on the HNS infrastructure.

Infrastructure and Openstack Services Logging.

HNS retains and monitors logs to determine whether the platform is operating as expected and anomalies are discovered and investigated. Platform specific logs that may contain security events are forwarded to Verizon's Network Intelligence Team for review and event correlation purposes. Transport of these logs is performed over a TLS encrypted connection to the internal/external endpoints.

Glossary

ACL	Access Control List
DDoS	Distributed Denial of Service
ESM	Enterprise Security Manager
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
NNO	Network to Network Operations
OSP	OpenStack Platform
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VRP	Virtual Routing and Forwarding

Questions?

For more information, contact your Verizon sales representative.

verizon