DATASHEET

VMware NSX – Privacy Datasheet

ABOUT VMWARE NSX

The VMware NSX platform delivers extensive networking and security capabilities across multiple workload types, and locations. Learn more at: *VMware NSX*

ABOUT VMWARE'S PRIVACY PROGRAM

- Trust Center – At VMware, we want to bring transparency that underlies trust. *The VMware Trust Center* is the primary vehicle to bring you that information.
- Data Privacy Officer - Please contact VMware's Privacy Team via the *Privacy Contact Form* or by mail at Office of the General Counsel of VMware, Inc., 3401 Hillview Ave, Palo Alto, California, 94304, USA.

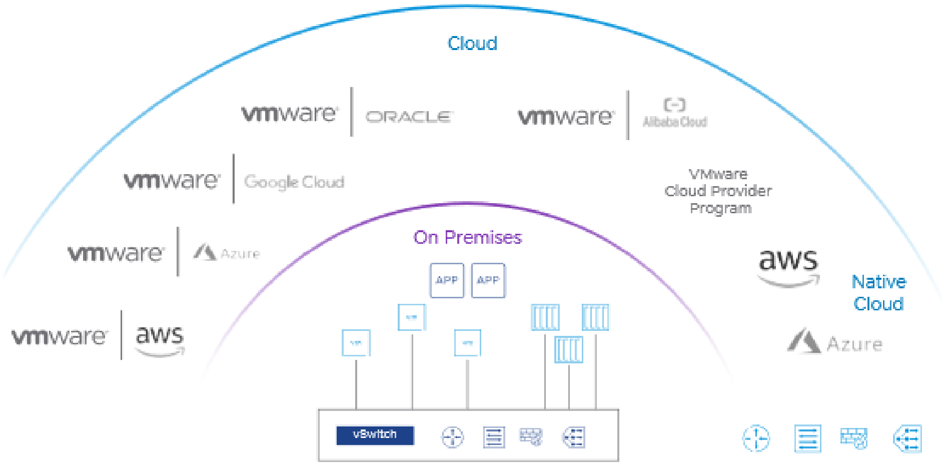
How VMware NSX brings value to you!

VMware NSX enables customers to manage their network as a single entity, and protect applications across data centers, clouds, and applications by reproducing the entire network model in software so the customer can create and provision any network topology in seconds and deliver critical apps and services faster and easier. Customers can leverage a combination of the services offered via NSX or from a broad ecosystem of third-party integrations—ranging from next-generation firewalls to performance management solutions—to build inherently more agile and secure environments. This datasheet covers the following cloud-based services which the customer can deploy to extend security capabilities for their on-premises deployments.

The NSX Threat Intelligence Cloud Service (NTICS) is a cloud-based service, which provides threat feeds and intelligence for on-premises NSX deployments to connect with and pull data to update NSX security features. When enabled via an on-premises NSX environment, NTICS can be used by a customer to authenticate NSX deployments and provide information used to detect a potential security threat.

The NSX Defender and Detonator Services are cloud-backed standalone services. They provide customers with the ability to analyze network traffic, intrusion detection, anomaly detection and correlation along with deep packet inspection (sandboxing).

The NSX Sandbox Service provides a complete malware analysis system for your threat analysts and incident response teams. It safely executes malware samples, analyzes URLs, and provides complete visibility into malicious behavior.



For more information, see the VMware NSX Service Description available *here*.

LAST UPDATED: JULY 2022

VMware and Privacy

In a complex world of data and the digital era our goal is simple: At VMware, you, our customers, and your data are our primary concern. VMware takes privacy and data protection very seriously and is committed to providing clear information about how we collect, use, and process your personal data. We have established policies and practices designed to protect the personal data we process on behalf of our customers (as a processor), and as a controller. We are also committed to privacy-by-design when developing products and services. VMware's Privacy Team actively works with the development teams to identify and embed privacy controls for customers.

The personal data collected and processed by VMware are largely dependent on the type of offering you purchase. This Privacy Datasheet provides you with information about how VMware processes and protects your personal data in connection with VMware NSX.

Types of Data Collected by VMware NSX

VMware NSX allows customers to connect to cloud-based services to extend security capabilities for their on-premises deployments. VMware NSX has features which customers can connect with: NSX Threat Intelligence Cloud Service (NTICS) and NSX Defender and Detonator Service (formerly Lastline Cloud Platform), and NSX Sandbox.

In connection with the customer's use and VMware's provision of NSX Threat Intelligence Cloud Service, NSX Defender and Detonator Service, or NSX Sandbox VMware collects, and further processes data as classified in the table below. In some instances, personal data may be included in such data. The types of personal data will depend on the file artifacts the customer chooses to inspect. Personal data of customers IT administrator will also be processed in connection with their use of the Service.

The NSX Threat Intelligence Cloud Service (NTICS) provides threat feeds and intelligence for on-premises NSX deployments such as categories and reputations of URLs and IPs, or information whether a file with a specified MD5 hash is harmful or not. The customer's NSX on-premises environment does not push any content to NTICS. The data processed by NTICS includes:

- Log Files generated in connection with the use of the NTICS service. These logs include capacity and performance information for improving the NTICS service.
- Customer external IP address to enable customer connection to NTICS service. This is standard IP information collected to log which IP address connected.

The NSX Defender and Detonator Service allows customers to send network traffic, URLS, and files for inspection to the NSX Defender and Detonator Service if they want to leverage the capabilities offered by the Services rather than only rely on the functionality offered by the on-premises offering to inspect files for malicious intent. The customer can choose to send the following information to the cloud for additional processing:

- Detection information related to malicious or anomalous activity detected in the network. This includes metadata identifying the endpoints involved in the activity (such as source and destination IP addresses); characteristics of the detected traffic (e.g., network protocol and port, volume of data exchanged, URLs and DNS names involved in the activity); and metadata about malicious or suspicious file artifacts (e.g., their transfer location and protocol, fingerprint (hash), and size). Actual files are not sent to the cloud service.

- Customer Sensor Data, such as IP addresses, Port and Protocol information, and packet headers.
- Information related to VMs/Physical machines observed in the monitored network, specifically the IP addresses of monitored VMs.
- Configuration information, specifically the license and the private IP ranges as configured by the NSX admin.
- Log Files used to gather analytics around usage, number of customers requests

The NSX Sandbox Service allows customers to send files to the cloud-based service for inspection. The customer has the choice of the file types to send for inspection. The data which may be processed by NSX Sandbox includes:

- File artifacts (i.e., the full contents of a file, file name, HTTP Headers for file download, email headers, subjects, and attachments) if a file requires in-depth analysis in the sandbox.
- User IP address and Server IP address

NSX Services

VMware Data Classification	Description and Purpose of processing	Categories of Personal Data
Customer Content	Content uploaded by customer or its users to the Cloud Service (as set forth in VMware's General Terms). To the extent the Cloud Service processes Customer Content, VMware processes such Content to provide the Service.	The customer controls and determines which type of personal data it submits to the Cloud Service. The specific personal data processed will depend on the customer's specific configurations and deployment. **NSX Threat Intelligence Cloud Service (NTICS)** Customers pull data from NTICS and do not upload any personal data to NTICS. **NSX Defender and NSX Detonator** Only potentially malicious files are submitted to the cloud service, by customer choice Online Identifiers such as, IP addresses File Identifying Metadata such as, File Hashes, URL, sender metadata Communication Metadata such as, IP addresses, Port and Protocol information, and packet headers Customer User Device Information such as type, operating system, and model

		NSX Sandbox Customers choose what files are submitted to the Cloud Service for inspection.
Support Request Content	Content uploaded or otherwise provided by customer to VMware to address a technical support issue (a "Support Service" under the VMware General Terms).	**NSX Threat Intelligence Cloud Service (NTICS), NSX Defender and NSX Detonator, and NSX Sandbox** Any personal data customer shares with VMware in connection with a support request (as controlled and determined by Customer).
Account Data	Data collected and used by VMware to manage the customer account and maintain the relationship with customer, such as to bill the customer or deliver notifications and alerts.	**NSX Threat Intelligence Cloud Service (NTICS), NSX Defender and NSX Detonator, and NSX Sandbox** Contact Information, such as customer administrator name, email address, address, and phone number. Online Identifiers such as customer administrator's IP address or login credentials.
Service Operations Data	Data used by VMware to facilitate the delivery of the Service. This may include (i) tracking entitlements, (ii) providing support, (iii) monitoring the performance, integrity, and stability of the Service's infrastructure, and (iv) preventing or addressing Service or technical issues. For example: • Configuration, usage, and performance data • Authentication Data • Service logs, security logs, and diagnostic data • Survey and feedback data	**NSX Threat Intelligence Cloud Service (NTICS), NSX Defender and NSX Detonator, and NSX Sandbox** Contact Information, such as administrators' email address. Online Identifiers such as administrators' and developers' IP address, login credentials or login time stamps.

SECURITY, CERTIFICATIONS AND THIRD-PARTY ATTESTATIONS

- All compliance certifications are available in the *VMware Trust Center's Compliance Page.*

Service Usage Data	Information used by VMware for analytics, product improvement purposes, and proactive support. See *VMware Trust & Assurance Center* for additional details regarding VMware's Service Usage Data Program (SUDP). For example: Configuration, usage, and performance data.	**NSX Threat Intelligence Cloud Service (NTICS), NSX Defender and NSX Detonator, and NSX Sandbox** Contact Information, such as administrators' email address (e.g., to provide proactive support). Online Identifiers such as administrators' IP address.

How We Process and Protect Data as a Controller

To the extent VMware processes personal data as part of Account Data, Service Operations Data and Service Usage Data, VMware acts as the Controller in respect to such personal data. The following privacy notices explain how VMware collects, uses, and protects any personal data in its capacity as a Controller:

VMware Privacy Notice: This notice addresses the personal data we collect when you purchase VMware products and services and provide account-related personal data.

VMware Products and Services Privacy Notice: This notice applies only to the limited personal data we collect and use for our own purposes in connection with our provision of VMware products and services, including (i) any cookies and similar tracking technologies we may use when providing the products or services; (ii) any information we use to facilitate the delivery of VMware services; and (iii) any data we collect to improve our products and services and our customer's experience.

How We Process and Protect Data as a Processor

Where VMware processes personal data contained in Customer Content in connection with the provisioning of the Service Offering, VMware will process such personal data on behalf of the customer as a "processor" (acts on the instruction of the controller). The customer is the "controller" of any personal data contained in Customer Content and determines the purposes of the processing.

Data Protection Addendum

VMware's obligations and commitments as a data processor are set forth in VMware's *Data Processing Addendum* ("DPA"). VMware will process personal data contained within Customer Content in accordance with the applicable agreement and the DPA. The applicable agreements for VMware NSX, including the VMware Terms of Service, the relevant Service Description, and other relevant legal documents can be found *here*.

Data Storage and Cross-Border Data Transfers

NSX Threat Intelligence Cloud Service currently has data centers located in The United States, Germany, Ireland, Australia, and South Korea. Hosting location options may be added from time to time so please visit the *Sub-Processors list* for up-to-date primary and disaster recovery location details.

NSX Defender and Detonator and NSX Sandbox currently have data centers located in the United States, Belgium, and Netherlands. When configuring the associated services that utilize the NSX Defender and Detonator and NSX Sandbox, customers are presented with the location to connect. Hosting location options may be added from time to time so please visit the *Sub-Processors list* for up-to-date primary and disaster recovery location details.

For cross-border personal data transfers from the EEA, Switzerland and the UK, VMware relies on Binding Corporate Rules ("BCR") as a processor. You can view VMware's BCR's in the *VMware Trust Center.*

DATA PRIVACY REQUESTS

If you wish to exercise any of your rights under applicable data privacy laws for personal data processed by your organization while using the Service Offering, please contact your organization. See *VMware's Privacy Notice* for information about how to exercise your rights where VMware is processing personal data in connection with its business operations.

FOR MORE INFORMATION OR TO PURCHASE VMWARE PRODUCTS

Contact your VMware account representative or call 877-4-VMWARE (outside North America, +1-650-427-5000), visit *vmware.com/products*, or search online for an authorized reseller.

UPDATES

Reading from a PDF? Do not be outdated, be informed! Find the latest information in the current version of this document from the *VMware Trust Center's Privacy Page*.

Sharing with Sub-Processors

VMware may utilize third-party companies to provide certain services on its behalf in connection with the provision of NSX Threat Intelligence, NSX Defender and NSX Detonator and NSX Sandbox Services. As set forth in the *Data Processing Addendum*, VMware has agreements and data transfer mechanisms in place with each sub-processor. A list of these sub-processors is available *here*

Additional sub-processors providing technical support functionality for the Service Offering is available in the *Support Services Sub-Processer List*.

VMware also provides customers with an easy mechanism to monitor changes to our list of sub-processors. If you would like to receive notifications, please visit this page *here*.

Data Retention and Deletion Practices

VMware retains personal data that we may collect in connection with the customer's use of the Service Offering for as long as it is needed to fulfill the obligations of the VMware Terms of Service.

The *VMware Data Processing Addendum* and the Service Guide set forth how personal data contained in Customer Content is deleted after contract expiration or termination. Upon termination of your account, Customer Content will be retained by backup systems for up to 90 days. VMware advises you to retrieve any data you wish to retain before the account termination takes place. VMware has no obligation to retain data beyond 30 days of the effective termination date.

NSX Threat Intelligence Cloud Service does not store customer data. Any access to the NTICS service is disabled when the customer subscription terminates.

NSX Defender and Detonator customer file data and any logs generated that are processed by the service will be retained for 12 months and deleted 180 days after license expiration. Data can be immediately deleted upon customer request. Any files the service finds that are malicious, are kept indefinitely for research purposes.

NSX Sandbox file uploads and associated metadata and logs are retained for up to 12 months and deleted 180 days after license expiration. Any files the service finds that are malicious, are kept indefinitely for research purposes.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.

Copyright © 2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: vmw-ds-temp-word 1/20