MARTELLO

VANTAGE DX

PRODUCT OVERVIEW

REFERENCE GUIDE

RELEASE 3.15
DOCUMENT DATE: FEBRUARY 26, 2024

NOTICE

Trademarks

Product Overview
Release 3.15 - February 26, 2024

Contents

CHAPTER 1

Introduction

Document Purpose and Intended Audience

This document provides an overview of the Vantage DX solution and its features. It describes how Vantage DX works to monitor your Microsoft 365 services and Teams call quality.

This guide also provides an overview of the deployment process, and describes how to determine the placement of Vantage DX Monitoring robots and VDX Diagnostics probes. The availability of robots and probes depends on your license package; therefore, this guide may contain information about functionality that is not available in your deployment.

This guide is intended for use by system administrators and IT managers.

Revision History

Document Date	Description
February 26, 2024	Vantage DX3.15Product Overview

CHAPTER 2

About Vantage DX

Vantage DX is a powerful analytics tool that allows you to proactively monitor Teams call quality, as well as the status of Microsoft 365 services. The Vantage DX solution is made up of three modules, which work together to provide:

- Teams call quality data, in near-real time.
- Performance metrics based on synthetic transactions.
- Network path diagnostics.

The following sections provide an overview of the solution and its capabilities:

- "Modules" on page 2
- "Management Interfaces" on page 8

Modules

The Vantage DX solution is made up of the following three modules:

- "Vantage DX Analytics" on page 2
- "Vantage DX Diagnostics" on page 4
- "Vantage DX Monitoring" on page 6

Vantage DX Analytics

Vantage DX Analytics is a powerful IT analytics solution that consolidates information from your existing monitoring tools, cloud platforms and ITSM systems into a single system. It can retrieve alerts and health state information from a range of monitoring systems and unify them in one interface.

A key feature of VDX Analytics is its ability to integrate with your Microsoft Call Quality Dashboard (CQD). The CQD is a tool that is available in the Teams Admin Center. It monitors all voice and video calls made in Teams and provides call quality metrics within 30 minutes of the end of a call.

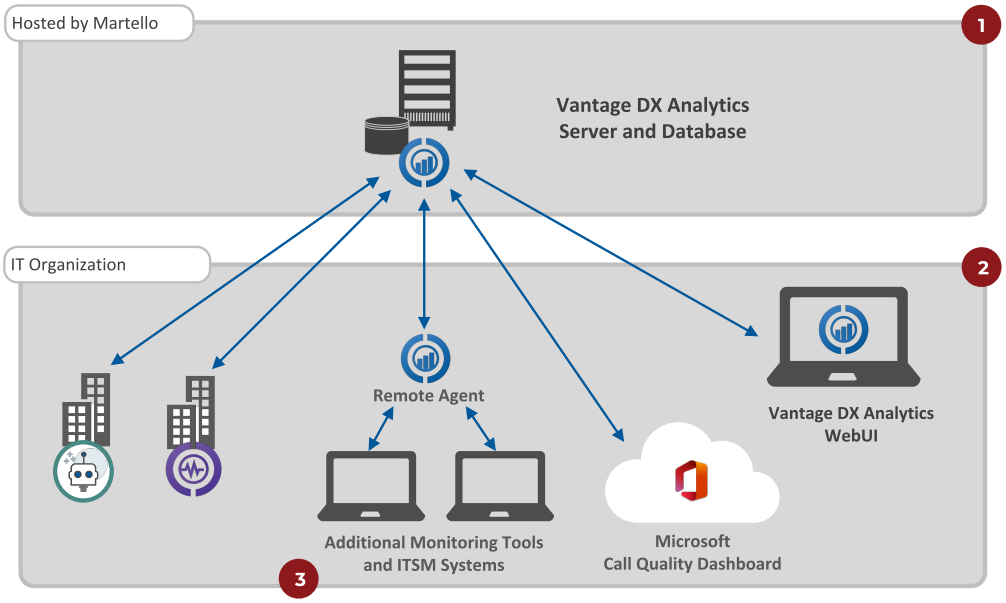
When you configure this integration, VDX Analytics retrieves data from your Microsoft CQD and organizes it in dashboards that make it easy for you to correlate call quality with the factors that impact it, such as the ISP, the connection type, or the location of the user. VDX Analytics also provides pre-defined searches so that

you can use to find call quality information quickly. In addition, data from the CQD is available as components that you can pin to custom boards and business services, which allow you to model the data in the way that best suits the needs of your organization.

Because VDX Analytics supports integrations with other monitoring tools, you can view the performance of your Teams service in the context of performance data from your other monitoring systems. This context is important to help you troubleshoot efficiently, because most call quality issues are caused by problems in the network infrastructure. For example, you can see the status of network infrastructure components that are monitored by PRTG or SolarWinds and understand immediately whether a failed switch is impacting the voice quality experienced by your users.

The following image shows an example of how VDX Analytics works to provide you with a consolidated view of your monitoring data. For a complete list of features, see "Vantage DX Analytics" on page 9.

Figure 1: Overview: VDX Analytics



1	Martello hosts VDX Analytics and its SQL and Elasticsearch databases.
2	Use the browser-based interface to view and organize data. You can also use the interface to manage incidents and alerts.

3	VDX Analytics retrieves information from your company's other monitoring tools and ITSM systems. It retrieves real-user data from your company's Microsoft Call Quality Dashboard (CQD), as well as data based on synthetic transactions performed by Vantage DX Monitoring. It retrieves network path data from an VDX Diagnostics installed at the business site. You can use the probe to monitor the network path between the business site and the Teams endpoint, or a custom endpoint.

Vantage DX Diagnostics

Vantage DX Diagnostics is an application that tests the network paths between physical office sites and target endpoints that you want to monitor, such as Microsoft Teams or SharePoint. It consists of a software probe and a web-based interface:

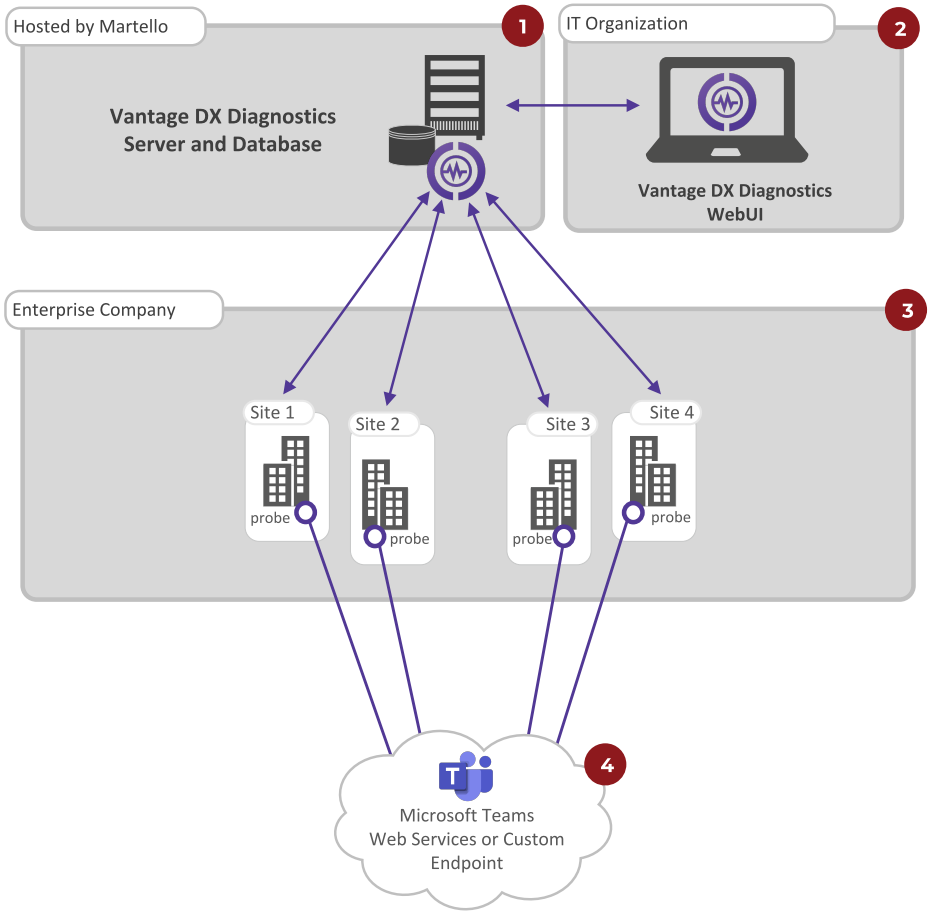
- **Probe:** The software probe installs on a Windows machine at each of your business sites, or on the machine of a remote user. The probe monitors and reports on the flow of data along the network path between the site where it is installed and the target endpoint. It uses My Traceroute (MTR)—which is a combination of traceroute and ping—to identify the segment of the network where errors occur. For example, if a user or a location is experiencing high round-trip time (RTT), jitter, or packet loss, you can deploy a probe to determine the source of the problem. The test results will show whether the issue is occurring in the corporate network, the user's home network, the ISP's network, or the Microsoft network.
- **Web-based interface:** The VDX Diagnostics interface provides a visual representation of the quality of the connection at each hop in a network path. This information is shown on network path diagrams to help you quickly understand where issues are occurring along the network path, how your end users' experiences are affected, and which networks are responsible for the issues. The interface also provides information about packet loss rate, round-trip latency, and jitter average for each network path.

Vantage DX Diagnostics deployments include the following concepts:

- **Support Organization**—The top level entity, which is the IT services organization. From the support organization, the target endpoints to monitor are configured. The endpoints are enabled and further configured for each site group.
- **Site Group**—Site groups function as theoretical containers for sites. An enterprise company will need only one site group to contain the sites that represent each office location.
- **Site**— A site represents a physical office location. Each site must have probe software installed on a computer at the physical location in order to test the connection to the target endpoints and collect data. VDX Diagnostics supports up to 400 sites (probes). Sites are created within a site group.

The following image shows an example of how you can deploy VDX Diagnostics probes at business sites. Refer to the accompanying table for information about each part of the deployment.

Figure 2: Overview: VDX Diagnostics



1	Martello hosts VDX Diagnostics and its database.
2	Use the browser-based interface to configure your sites, install probes, and configure the endpoints to monitor. You can also view network path information in the interface.
3	Software probes are installed on Windows computers at business sites. The probes monitor the path between the business site and the endpoint.
4	You can monitor endpoints that provide web services, such as Microsoft Teams, or you can monitor static endpoints, such as Salesforce. You can also monitor endpoints such as routers and gateways.

For more information about the features of VDX Diagnostics, see "Vantage DX Diagnostics" on page 13.

Vantage DX Monitoring

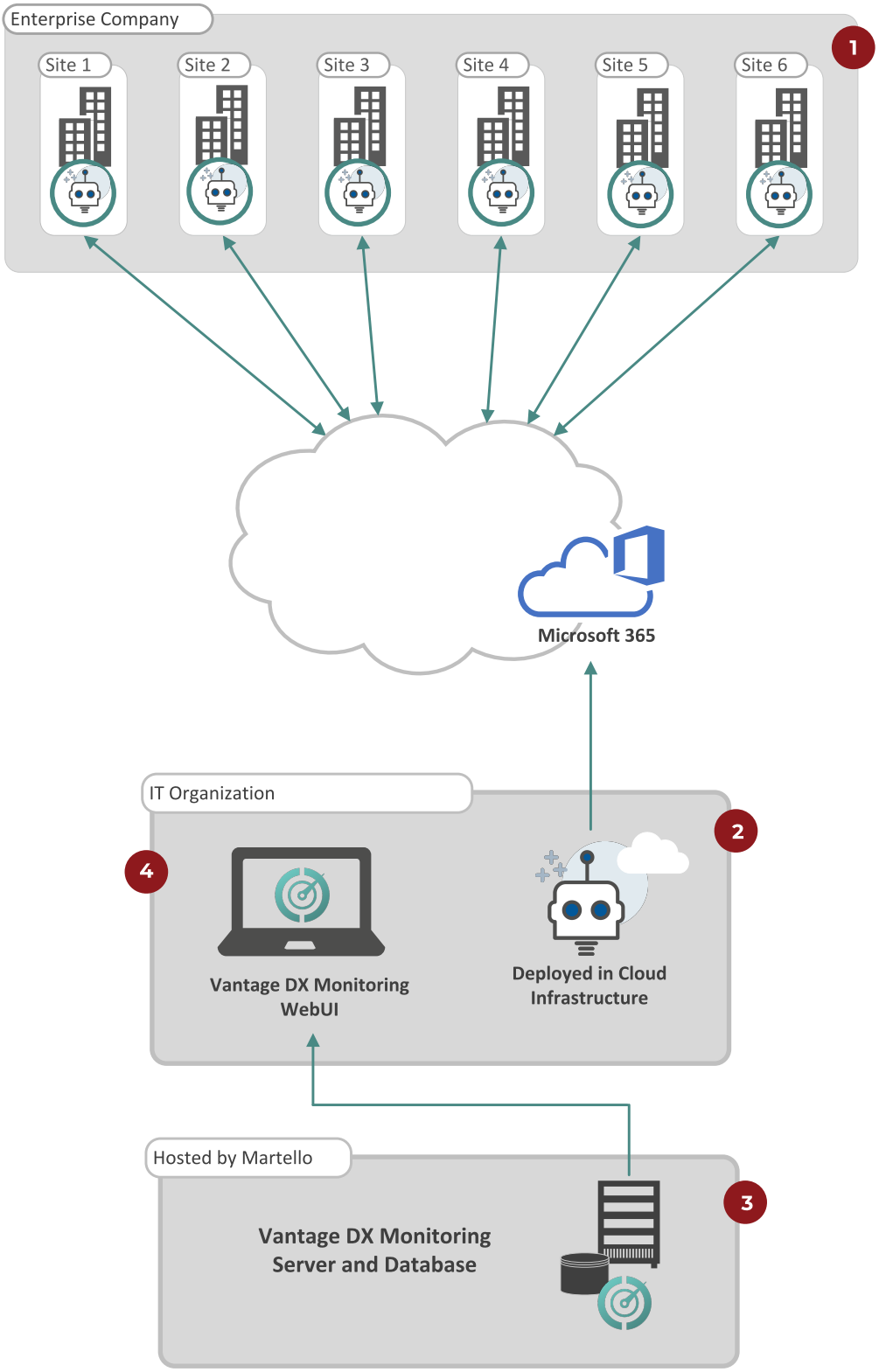
Vantage DX Monitoring is a monitoring tool that provides the data you need in order to understand the performance of Microsoft applications and resources. In Microsoft environments, these applications and resources are known collectively as workloads.

Vantage DX Monitoring deploys robots to perform synthetic transactions, which are tests that simulate the activities that your users typically do. Robots located at your critical business sites perform synthetic transactions on workloads—such as Microsoft Exchange, SharePoint, OneDrive, and Teams—while also testing network conditions. These robots continuously test the user experience from where your end users are located, to help you understand the service quality that you are delivering to your business sites. Based on these tests, Vantage DX Monitoring provides you with proactive alerts so that you can work directly on issues before they become a problem for your end users.

You can configure the activities and workloads that you want the robots to test. Vantage DX Monitoring can monitor a wide range of Microsoft workloads, including cloud-based Microsoft 365 applications and on-premises Exchange deployments.

The following image shows an example of how you can deploy Vantage DX Monitoring robots in the cloud and at business sites. Refer to the accompanying table for information about each part of the deployment.

Figure 3: Overview: Vantage DX Monitoring



1	The on-premises robots monitor the service that your business sites receive from the Microsoft datacenter. This type of deployment allows you to analyze the connectivity at remote offices and understand the experience of the users located there.
2	The cloud robots monitor the service that your business receives from the Microsoft datacenter. A robot deployed in this way allows you to understand the typical quality of service that your business receives. It also allows you to be aware of service degradation immediately, before you receive an alert from Microsoft.
3	The results of the synthetic transactions are transmitted to a SQL database on the Vantage DX Monitoring server, which is hosted by Martello.
4	Use the WebUI to view detailed performance metrics and alerts. You can also use the WebUI to customize how workloads are monitored. For example, you can choose which workloads to monitor, set thresholds for alerts, and configure how you receive notifications about alerts. You can also view and share performance metrics in Power BI reports.

For more information about the features of Vantage DX Monitoring, see "Vantage DX Monitoring" on page 15.

Management Interfaces

Each module in the Vantage DX solution has its own management interface. When you log into the Vantage DX solution, the VDX Analytics interface opens as the default management tool.

CHAPTER 3

Features

The following sections describe the features that are available in each of the Vantage DX modules:

Vantage DX Analytics

VDX Analytics is the main interface for the Vantage DX solution. The following table lists the features that are available in VDX Analytics.

Table 1: VDX Analytics Features

Feature	Description
Dashboards	Vantage DX Analytics automatically creates dashboards that provide comprehensive information about the call quality your users are experiencing. The following dashboards are available: • Teams Overview Dashboard • Users Dashboard • Locations Dashboard • Calls Dashboard • Meeting Rooms Dashboard • Meeting Room Devices Dashboard For detailed information about dashboards, see "Dashboards" in *Microsoft Performance Data in Vantage DX*. The guide is available on the Martello website at: https://martellotech.com/documentation/vantage-dx/#documentation

Feature	Description
Pre-defined searches	
Pre-defined searches	Pre-defined searches allow you to quickly find data that Vantage DX Analytics has retrieved from the Microsoft Teams CQD integration. The following searches are available: • Teams Users • User Devices • Teams Alerts • Teams Meetings • Meeting Rooms • Offices • ISPs • Microsoft Datacenters • Countries • Cities • PSTN Carriers • PSTN Trunks You can pin the search results to boards or business services.
Organize data	
Boards	Boards are a way to group components from one or more monitoring systems or cloud platforms. Boards are flexible and allow you to model your IT environment in the way that best fits your needs.
Business services	Use VDX Analytics to model, monitor, and report on business services. Business services are services that you deliver to your end users. Business services range from accounts receivable and email to VoIP calls and web sites. Business services are a way of mapping the devices and applications that work together to support specific business functions. When you map devices and applications to a business service, you can monitor IT resources in the context of the business workflow where those resources are used.

Feature	Description
Saved searches	Search the details or raw properties of each component, alert, and incident. The Saved Searches feature allows you to customize searches and save your preferences. You can set filters for the search and select the tab where you want the results to display. If you create saved searches for computers, groups, and services, you can pin the saved searches to a board or business service, to ensure that components update dynamically.
Rules and exclusions	Create membership rules to dynamically update dashboards so that they reflect changes to your IT infrastructure. For example, you can create a rule that searches for Microsoft System Center Operations Manager (SCOM) computers in the same IP address range and adds them to your board. You can configure exclusions to the rules.
Consolidated components	Link together components that have common properties. This feature is helpful if you have components that are monitored by multiple integrations. VDX Analytics can consolidate the components based on rules that you configure. It then displays them as a single component. For example, if you have a computer that is monitored by SCOM, it may also be inventoried in the ServiceNow CMDB and have security-log data that is monitored by Splunk. VDX Analytics models all of this data in a single object that you can monitor and manage.
Synched boards	When you use this feature, the components of a board are determined by the source system. The members of the board and the health state are determined by the source system and are not configurable in VDX Analytics. If members are added or deleted in the source system, or if the health state changes in the source system, the board in VDX Analytics automatically updates.
Manage health data and troubleshoot issues	

Feature	Description
Explorers	Explorers are topology diagrams that show components and relationships. There are three Explorers: a Boards Explorer, a Groups and Services Explorer, and a Component Explorer.
Critical issue locator	When you view an Explorer, you can click a button to expand the diagram and immediately view critical issues.
Health states	Configure how the health state of a board or business service is calculated.
Data views	Choose how you want to view status information on a board. You can view board data in pie charts or heat maps, and display the number of incidents, alerts, and the amount of uptime.
Searches and Filters	The VDX Analytics interface provides filters that allow you to sort data quickly. You can also search operators to efficiently search for data in the Elasticsearch database.
Manage and report on SLA	
Service Level Objectives	Configure the Service Level Objectives for each business service.
View SLA data	Monitor the SLA performance for each business service. In addition to uptime information, VDX Analytics provides a list of the components that have impacted the SLA during the selected period. You can select outages to exclude from the calculations.
Generate SLA reports	Generate PDF reports that provide a weekly or monthly view of SLA data.
Manage incidents	
Automate incident creation	If you have integrated your ITSM system with VDX Analytics, you can automatically create incidents based on alerts. You can also link an alert on a board or business service to an existing incident in your ITSM system.
Resolve alerts	You can resolve alerts raised by your monitoring tools from within VDX Analytics. You can also navigate to your ITSM from within iQ to close incidents quickly.

Feature	Description
Send notifications	You can configure a notification that is triggered when a board or business service is shared, when its state changes, or when there is a new alert or new incident. You can send notifications to email recipients or to a PowerShell script. The option to send notifications to a PowerShell script gives you the flexibility to configure a range of actions in response to the notification. For example, you can send notifications to a PowerShell script that generates an SMS message.
Manage access	
Role-based access	User permissions in VDX Analytics are based on roles. VDX Analytics includes two default roles: Administrators and Operators. Administrators can create additional roles, and can further refine permissions by scoping the extent of information that users can access.
Scope access	Use the scoping feature to further refine the permissions within a role. You can scope user access to boards, business services, or source systems. You can also scope access to saved searches.
Consolidate data from multiple systems	
Integrations	VDX Analytics integrates with a range of monitoring tools, cloud platforms, and ITSM systems. It consolidates data from all your tools so that you can see the overall health status of a system quickly.

Vantage DX Diagnostics

The following table lists the features that are available in VDX Diagnostics.

Table 2: VDX Diagnostics Features

Feature	Description
Custom endpoints	VDX Diagnostics is pre-configured to monitor the Microsoft Teams endpoint, but you can configure custom endpoints. Endpoints include web services, websites, gateways, and routers.
Network test summary	A bar graph illustrates the network path test results between the endpoint and each office location. Display data from the past 8 hours, 24 hours, 3 days, 7 days, 14 days, or 30 days. From the Network Testing Summary graph you can access more detailed data, such as the test results for each site.
Network path diagrams	View the network paths from each site to the endpoint. These diagrams identify each hop in the network path and use color-coding to indicate the health status of each hop. The diagrams also show the owner of each segment of the network.
Path analysis	A panel displays with the network path diagram to provide detailed information about each network path that appears in the diagram, such as the number of hops, the round-trip time (RTT), and the amount of jitter and packet loss.
Microsoft Teams access points	An interactive map shows the entry points that your sites are using to access the Microsoft data center, as well as the network paths that your sites are using to access those entry points. The geographical location of the entry point that you use to access the MS data center may affect the performance of MS Teams. The map highlights network paths that have an unexpected entry point, which may contribute to performance issues.
Probe	A software probe that monitors and reports on the flow of data along the network path between a site and the endpoint.

Vantage DX Monitoring

Vantage DX Monitoring performs continual tests of your Microsoft applications and resources, known as workloads Vantage DX Monitoring allows you to create monitoring configurations for the following workloads:

- AAD Connect (Azure AD Connect)
- ADFS (Active Directory Federation Services)
- Exchange DAG
- Exchange Edge Server
- Exchange Free/Busy
- Exchange Mailbox Server
- Exchange MAPI
- Exchange Online
- Exchange Online Network
- Exchange OWA
- Hybrid Mail Routing
- Internal Mail Routing
- Microsoft 365 Health, which includes the following applications (if enabled in your environment):
    - Azure Information Protection
    - Dynamics 365
    - Exchange Online
    - Identity Service
    - Microsoft Forms
    - Flow in Microsoft 365
    - Microsoft StaffHub
    - Microsoft Teams
    - Microsoft Intune
    - Office Client Applications
    - Office for the Web
    - Planner
    - PowerApps in Microsoft 365
    - Mobile Device Management for Office 365
    - Yammer Enterprise
    - Office 365 Portal
    - OneDrive for Business
    - Power BI
    - SharePoint Online
- Office 365 Web App, which includes the following applications (if enabled in your environment):
    - Azure AD Management

        - Azure Portal
        - Delve
        - Dynamics
        - Excel
        - Office 365 Admin Portal
        - OWA
        - Office365
        - Office Pro Plus Pages
        - OneDrive
        - OneNote
        - Planner
        - Power Apps
        - Power Automate
        - Power BI
        - SharePoint
        - Streams
    - OneDrive
    - Roundtrip Mail Routing
    - SharePoint Network
    - SharePoint Page
    - SMTP Gateways
    - Teams
    - Teams Advanced
    - Teams Network
    - Teams Video
    - URL

The following table lists the features that are available to help you monitor your workloads.

Table 3: Vantage DX Monitoring Features

Feature	Description
Vantage DX Monitoring WebUI	The Vantage DX Monitoring Web UI is an application that displays detailed dashboards, metrics, and alert notifications for the Microsoft workloads that you monitor. The data it provides helps you measure the experience of your end-users. You can use the Vantage DX Monitoring Web UI to customize how workloads are monitored. For example, you can choose which workloads to monitor, set performance thresholds, and configure how you receive alert notifications.
Robot Manager	Robot Manager is a Windows service that you install on machines located at critical business sites. It manages the robots that perform synthetic transactions at that site. The Robot Manager service sends the results of the synthetic transactions to the Vantage DX Monitoring server using encrypted communication.
Robots	Robots perform synthetic transactions, which are tests that simulate the activities that your users typically do. The robots perform these tests at the sites where your users are located, to provide you with insight into the user experience at each site. You can use the Vantage DX Monitoring Web UI to configure the activities and workloads that the robots test.
Dashboards	Vantage DX Monitoring provides pre-defined dashboards, as well as the ability to configure custom dashboards. Dashboards provide detailed information such as metrics in order to monitor the health of a specific workload or resource.

Feature	Description
Alerts	Alerts are based on the tests that the robots perform. Warnings and critical alerts are raised based on industry-standard thresholds for performance. Some thresholds are configurable so that you can adjust them to the needs of your business sites. For a full list of performance alerts and the thresholds that trigger them, see Vantage DX Monitoring Alerts in *Microsoft Performance Data in Vantage DX*.
Thresholds	Some performance metrics have configurable thresholds. These thresholds are set to default values that are based on industry standards, but you can configure them based on your needs.
Power BI Reports	You can view and share Vantage DX Monitoring data in a Power BI report.

CHAPTER 4

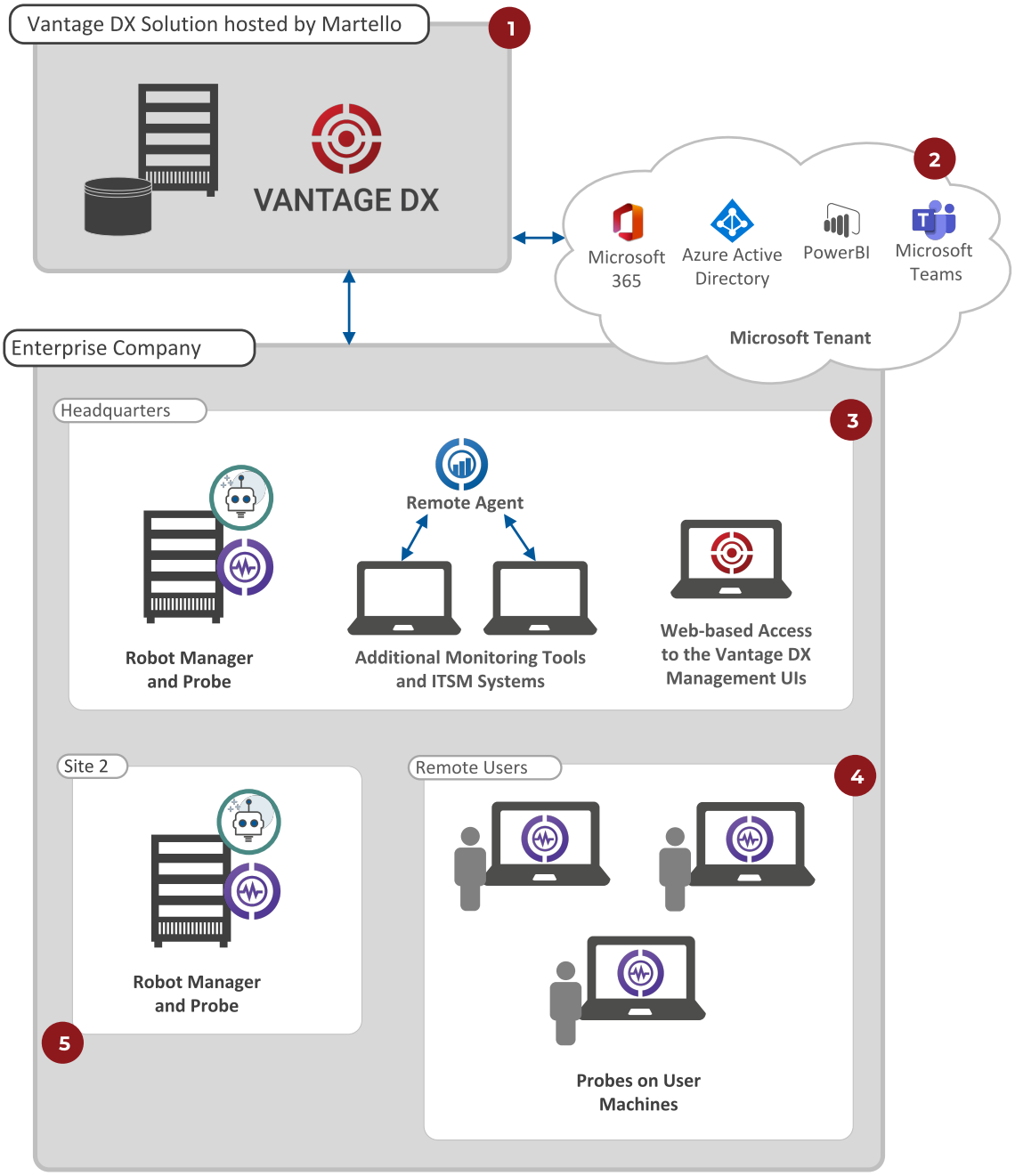
Vantage DX in your Environment

The following sections describe how the modules in the Vantage DX solution work together, and how they integrate with your IT environment.

Solution Overview

Vantage DX is a cloud-based solution that is hosted by Martello. The following image shows an example of the Vantage DX solution architecture. The table that accompanies the image describes how the components are deployed at each location.

Figure 4: Architecture for Enterprise Deployments



1	All of the modules of the Vantage DX solution are deployed in Martello's cloud environment.

2	VDX Analytics retrieves data from your company's Microsoft tenant, including call quality data from the Microsoft Call Quality Dashboard (CQD) and status information about your Microsoft 365 services.
3	In this example, a Vantage DX Monitoring Robot Manager and a VDX Diagnostics probe are deployed at the corporate headquarters. The Vantage DX Monitoring robots perform synthetic transactions that mimic the activities of the users at the site. It is optional to deploy a Robot Manager at business sites, but doing so provides you with proactive data about the user experience at your business-critical location. The VDX Diagnostics probe monitors the network path between the business site and the Microsoft Teams endpoint, or between the business site and a custom endpoint. This example also shows a VDX Analytics remote agent, which allows you to integrate other monitoring systems and ITSMs with the Vantage DX solution. You can configure this integration at any business site; it is shown at the headquarters only as an example. Similarly, this example shows that you can access the Vantage DX management UIs from the headquarters, but administrators and operators can connect from any site using a web browser. This data retrieved from the Microsoft CQD—along with the performance data collected by the Robot Manager and the network path data collected by the probe—is consolidated in the hosted environment, where you can access it using the Vantage DX management interfaces.
4	If you have remote users who experience call quality issues, you can deploy a VDX Diagnostics probe to monitor the network path between the user's site and the Microsoft Teams endpoint, or between the user's site and a custom endpoint.
5	Deploy a Vantage DX Monitoring Robot Manager and a VDX Diagnostics probe at any additional business sites.

Deployment Phases

The following sections provide an overview of the initial deployment process. We recommend that you deploy Vantage DX in stages:

- "Integrate your Microsoft Data" on page 22
- "Analyze Data and Identify Critical Locations" on page 22
- "Deploy Robots" on page 22
- "Deploy Probes" on page 23
- "Example" on page 23

Integrate your Microsoft Data

The first step in the deployment process is to integrate your Microsoft Call Quality Dashboard (CQD) and your Microsoft 365 subscription with Vantage DX. After you configure these two integrations, Vantage DX retrieves call quality data from your Microsoft CQD, as well as status information about your Microsoft 365 services.

After you configure these integrations, we recommend that you collect data for two weeks. This amount of data will help you analyze performance and identify trends. You can use this information to quickly identify problem areas, and to plan the most effective locations to deploy VDX Diagnostics probes and Vantage DX Monitoring robots.

For information about how to configure these integrations, see "Integrate Data from your Microsoft Tenant" on page 1.

Analyze Data and Identify Critical Locations

The next step in the process is to identify critical locations using the data in the dashboards.

We recommend that you identify two types of locations to deploy Vantage DX Monitoring robots and VDX Diagnostics probes:

- **Sites to monitor proactively**—Choose at least one business-critical site, such as your corporate headquarters, or sites where you have VIP users.
- **Sites or users who experience problems**—Select sites where you have known issues, or where you have identified problems based on your analysis of the data available in Vantage DX dashboards.

The dashboards provide comprehensive information about the call quality that your users are experiencing. You can use them to understand:

- The locations where problems are impacting users.
- The specific users who are experiencing problems with voice quality.
- The percentage of calls that are good, poor, or failed; this information is displayed for the total number of peer-to-peer calls, as well as conference calls and PSTN calls.
- The network issues that impact call quality, such as round-trip time (RTT), packet loss, jitter, and frame rate.
- Connectivity data, such as the connection type, the ISP, and the connected device.
- Teams Meeting room data, including the usage of meeting rooms and the health state of devices associated with meeting rooms.

Deploy Robots

The number of Vantage DX Monitoring robots that you can deploy depends on your license package.

We recommend that you start by deploying up to 10 robots, distributed in the following way:

- Deploy up to 8 robots at sites where you have known issues, or where you have identified problems based on your analysis of the dashboard data. You can install the robot on a machine that is connected to your LAN or that is connected by WiFi; you can determine which type of connection is most important to monitor based on the dashboard data.
- Deploy a minimum of 2 robots at each business-critical site. For each business-critical site, we recommend one robot on a machine connected to the LAN, and one robot on a machine that connects to the network through WiFi.
- If you have not deployed all 10 robots based on this criteria, select other important business sites that you want to monitor proactively, or install robots on different floors at the same site.

Tip:
We recommend that you install the robots on machines that are located close to large numbers of users, and that are similar as possible to your users' machines. Plan to install each robot on a dedicated machine.

For information about how to deploy robots, see "Configure Synthetic Transactions" on page 1.

Deploy Probes

The number of VDX Diagnostics probes that you can deploy depends on your license package.

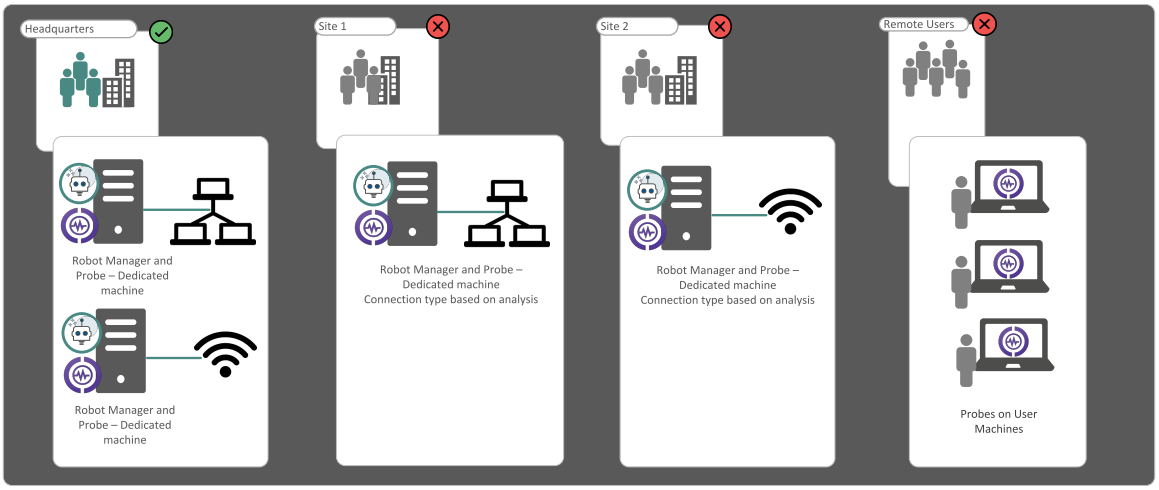
We recommend that you start by deploying up to 10 VDX Diagnostics probes, distributed in the following way:

- Deploy one probe at each business-critical site. We recommend that you install a probe at any location where you have installed a robot manager. You can install the probe on the same machine that hosts the robot manager.
- Deploy one probe at each site where you have known issues, or where you have identified problems based on your analysis of the dashboard data.
- Deploy one probe on the machine of a user who is affected by poor call quality, based on your analysis of the dashboard data. We recommend this approach for VIP users who work remotely.

Example

The following image shows an example of how Vantage DX Monitoring robots and VDX Diagnostics probes work together to proactively monitor business-critical sites, sites with known issues, and VIP users who work remotely.

Figure 5: Example of a Vantage DX Deployment



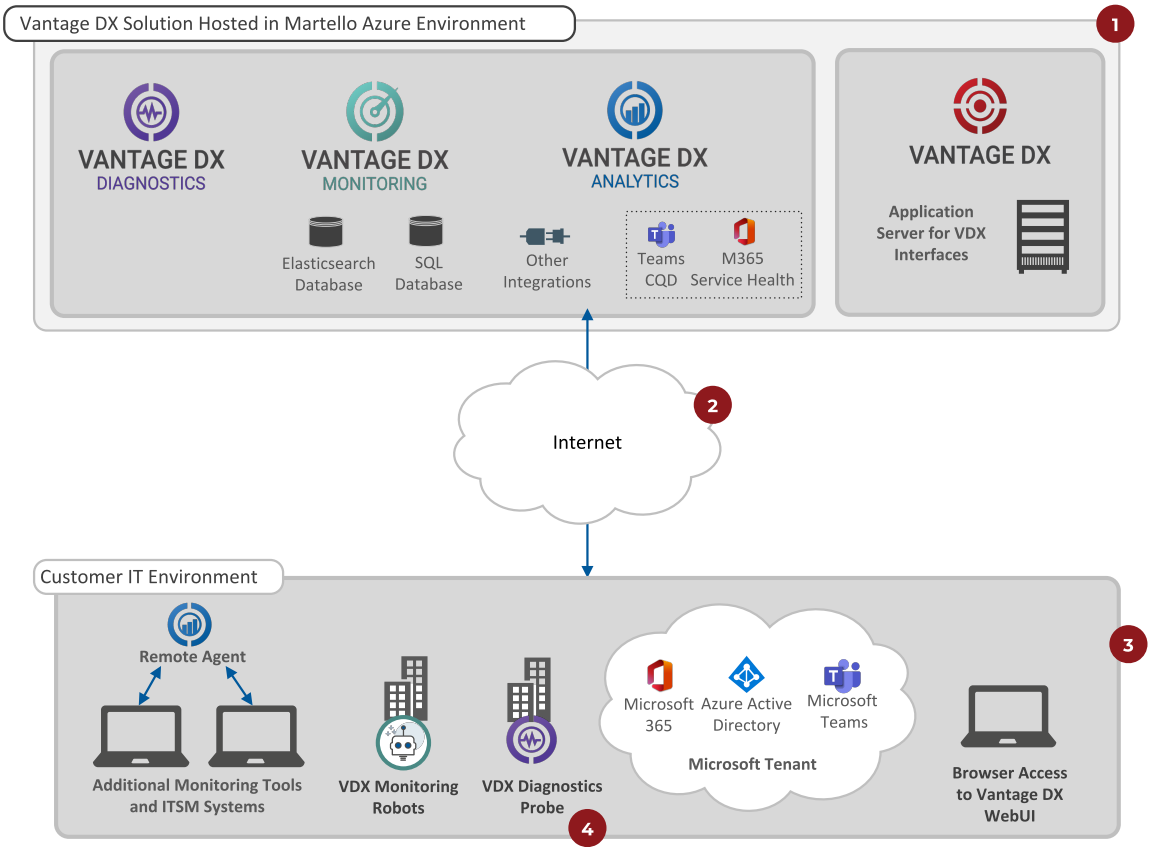
CHAPTER 5

Security

The following sections describe theVantage DX security infrastructure and the security policies that protect your data.

Security Overview

The following diagram and its corresponding table provide an overview of the security policies and technologies that are used in Vantage DX.



Number	Description
1	The Vantage DX cloud infrastructure is hosted in Microsoft Azure data centers. The data for each customer instance is stored in a virtual private network. We use Microsoft Azure volume encryption to protect data at rest.
2	Communication between the sites and the Vantage DX environment is through the WAN. Vantage DX uses HTTPS for all connections and uses digital certificates for encryption.
3	Vantage DXuses single sign-on to authenticate users against your Azure Active Directory.
4	Each Vantage DX module retrieves different information from your IT environment and transmits it to the Vantage DX servers and databases in Martello's Azure environment.

Authentication and Access

Vantage DX uses SSO to authenticate users against your Azure Active Directory (AAD). Permissions within Vantage DX are role-based. Two default roles are provided:

- **Service Administrators**—Users assigned to this group have read-write access to everything in Vantage DX.
- **Service Operators**—Users assigned to this group have:
  - Administrative permissions in Vantage DX Monitoring.
  - Read-write access to any integrations, boards, and business services that the administrator provisions for this role in VDX Analytics.
  - The ability to create sites and install probes in VDX Diagnostics.

VDX Analytics is the main management interface, and within this interface, administrators can create and assign roles that determine:

- The actions that users in each role can perform.
- The data that users in each role can see.

Data Collection

Vantage DX collects a range of data. The following sections describes the data that Vantage DX collects from standard integrations:

- "Microsoft Call Quality Dashboard" on page 27
- "Microsoft 365" on page 27
- "Vantage DX Analytics" on page 28
- "Vantage DX Monitoring" on page 28
- "Vantage DX Diagnostics" on page 28

Microsoft Call Quality Dashboard

The following user data is collected from the Microsoft Call Quality Dashboard:

- Full IP address
- Session initiation protocol (SIP) URI (Skype for Business only)
- User principal name (UPN)
- User verbatim feedback (provided when users rate the call experience)
- Object ID (the Active Directory object ID of the endpoint's user)
- User name
- User email address
- User department
- User office location

Microsoft 365

The following data is collected about your Microsoft 365 service:

- Organization name and domains
- Office subscription details
- Active and inactive user counts
- Service Plans—health states
- Service incidents
- Service features

Vantage DX Analytics

If you are integrating other monitoring tools or ITSM systems with VDX Analytics, VDX Analytics polls and persists health state and alert data using the APIs of the source system.

Vantage DX Monitoring

Vantage DX Monitoring stores the following information:

- The hostname of the machine where the Robot Manager is installed.
- The credentials of the Microsoft 365 accounts used by the robots to test the workloads.
- The configuration settings that you enter when you configure monitoring for a workload. These settings vary, depending on the workload. For example:
  - If you are monitoring the SharePoint workload, the URL of your SharePoint page is stored.
  - Some workloads allow you to use a static proxy; if you choose this option, the proxy address and credentials are stored.

Vantage DX Diagnostics

This module records the IP addresses of the hops between the host machine and the endpoint. For example, it records the IP addresses of the hops between the VDX Diagnostics probe installed on the host machine and the network path to world.tr.teams.microsoft.com.

The addresses of the gateway and router hops traversed to reach the endpoint are recorded. Vantage DX does not record the IP address of the machine where the probe is installed.

Data Transmission

Communication between all sites and the Vantage DX environment is through the WAN.

Vantage DX uses HTTPS for all connections and uses digital certificates with ACME v2 for encryption.

Data Storage

The following sections describe how Vantage DX stores and secures your data:

Infrastructure

The data collected by the Vantage DX modules is transmitted to the Vantage DX servers and databases, which are hosted in Microsoft Azure data centers. Multiple data center locations are available to choose from:

- Western Europe
- Eastern United States
- Australia

The following security measures are implemented in this infrastructure:

- **Virtual Private Networks**—Each Vantage DX instance securely stores data in a virtual private network. Each endpoint accepts only secure connections from within same private virtual network. Access to the virtual private network is protected by secure web application firewall (WAF).
- **Encryption**—Vantage DX uses Microsoft Azure volume encryption to protect data at rest.

Data Access

Administration of the environment is restricted to Martello senior cloud platform administrators.

Authentication with the Azure portal and PowerShell management is protected by secure passwords and Azure AD Multi Factor Authentication (MFA).

Data Removal

In the event that a customer cancels their service with Martello, all data is removed from our production databases within 7 business days. Customer data may still exist within the backups for up to 30 days. Data destruction certificates can be provided upon request.

Backups

Backups are performed daily using the Azure Backup service and are encrypted using Microsoft platform-managed keys. This allows us to perform point-in-time restores of the data in the event of data corruption or database failure. We retain these snapshots for a period of 30 days after which they are automatically purged. The backups are stored within the Azure environment and are only accessible by Martello senior cloud platform administrators. All data is encrypted using the Microsoft platform-managed keys. This encrypt applies to all volumes backed up to the Recovery Services vault.

Logging

The following sections describe logging in Vantage DX:

Error Logs

Vantage DX collects and stores error logs required to troubleshoot issues and monitor the health of your instance. Error logs are aggregated into an Elasticsearch logging infrastructure. No user identifiable data other than the company name is ever recorded into this platform. Log data is retained for 6 months and we have several automatic anomaly detection processes in place to identify potential security incidents and unauthorized access attempts. Any security incidents are logged in our Support queue where they are tracked and moved through a workflow process to resolution.

User Event Logs

Vantage DX records user login events. Login events occur when:

- A user logs in successfully.
- A user enters an incorrect password.
- A user account is updated.
- User audit logs are persisted using Global Unique Identifiers, not user names.

Security Testing and Analysis

The following sections describe how Vantage DX is assessed for security vulnerabilities:

Vulnerability Tests

We perform continuous scans of source code in development repositories and release repositories for known vulnerabilities.

Penetration Scans and Assessments

All product releases must pass penetration scans performed by our security team. Once each year, we have an external cyber-security analyst perform penetration tests. We can provide a copy of a security assessment prepared by the cyber-security analyst on request.

CHAPTER 6

Licensing Options

The Vantage DX modules that are available to you depend on your package. The following table lists the modules and features that are available for each package.

Table 4: Vantage DX Packages

	Essentials	Professional	Enterprise
Robot Managers	—	Up to 10 (with option to purchase additional)	Unlimited
Probes	—	Up to 10 (with option to purchase additional)	Unlimited
Integrations			
AWS		✓	✓
AppDynamics		✓	✓
AudioCodes			✓
Broadcom DX Performance Management		✓	✓
Cherwell			✓
Derdack		✓	✓

	Essentials	Professional	Enterprise
Email	✓	✓	✓
Microsoft 365	✓	✓	✓
Microsoft Azure		✓	✓
Microsoft Azure Insights		✓	✓
Microsoft Call Quality Dashboard (CQD)	✓	✓	✓
Microsoft Teams Notifications	✓	✓	✓
Microsoft System Center Operations Manager (SCOM)		✓	✓
Mitel Performance Analytics (MPA)		✓	✓
Nagios		✓	✓
PowerShell	✓	✓	✓
PRTG Network Monitor		✓	✓
ServiceNow			✓
SolarWinds		✓	✓
Splunk		✓	✓
Vantage DX Diagnostics		✓	✓

Essentials	Professional	Enterprise
Vantage DX Monitoring	✓	✓
VMware vCenter	✓	✓
WhatsUp Gold	✓	✓
Zabbix	✓	✓

CHAPTER 7

Resources

Refer to the following resources to learn how to use Vantage DX to monitor your Microsoft 365 services, and how you can integrate data from your existing monitoring tools to provide end-to-end monitoring of your IT environment.

Documentation

For complete information about using the components of the Vantage DX solution, refer to the following documentation, available in the Martello Help Center at:

https://helpcenter.martellotech.com/s/documentation/vantage-dxcloud

Application Notes

- Understanding Vantage DX
- Monitor and Troubleshoot Microsoft Teams Call Quality
- Monitor a Hybrid Exchange Environment
- Monitor Co-Authoring Platforms
- Manage Alerts and Incidents
- Manage Complex Data in VDX Analytics
- Business Services and SLA Performance Data on VDX Analytics
- Customize Monitored Sites in Vantage DX Monitoring

Vantage DX Solution-Level Documentation

- Vantage DX Release Notes
- Microsoft Performance Data in Vantage DX

VDX Analytics

- VDX Analytics Integration Guide
- VDX Analytics User Guide

Vantage DX Monitoring

- Vantage DX Monitoring User Guide

VDX Diagnostics

- VDX Diagnostics Administration Guide for Service Providers
- VDX Diagnostics Administration Guide for Enterprises

.

Training

Self-guided training modules are available to help you learn about key features in Vantage DXTo. You can access the training modules at the following website:

https://helpcenter.martellotech.com/s/training/self-guided-training

In-person training is also available for your organization. You can learn more about in-person training at:

https://helpcenter.martellotech.com/s/training/in-person-training