

TECHNICAL BRIEF

OnelQ Security



The purpose of this document is to define the OnelQ platform components, explain the data flow among them and outline security measures used by OnelQ for data collection, transport, storage, access and removal.



Introduction

OneIQ is an **ISO/IEC 27001** certified software-as-a-service provider of edge-to-cloud, Fullstack Intelligence[®] for continuously optimizing application performance, modernizing IT infrastructure and reducing operating costs. We use patented secure workspaces to give teams a shared context of application workloads and the underlying Hybrid IT infrastructure, while allowing ITOps teams to have total control over their data. Customer trust and information security are at the heart of everything we do at OneIQ.



3 core components in the OneIQ platform



ONEIQ PULSE

Agentless connector for capturing configuration, billing, performance and network data across cloud-native, cloud and datacenter platforms.



ONEIQ CENTRAL

Data warehouse for storing data collected by OneIQ Pulse in an IT environment hosted on Azure cloud storage with encryption-at-rest.



ONEIQ PORTAL

Web-based interface with secure workspaces for collaborative analysis of connected Hybrid IT environments using data from the OneIQ Central.

Data Flow

IT infrastructure and operations teams can download the OnelQ Pulse from the OnelQ Portal and deploy it in cloud-native, cloud and datacenter environments. For multiple sites or network segments, additional OnelQ Pulse instances can be deployed. Here is the data flow from discovery to analysis of the IT environment.

1

Specify data visibility

When an IT environment is connected to a workspace, machine-identifiable information such as IPs and hostnames can be scrambled.

2

Discover target systems

OnelQ Pulse can discover multiple target systems in each IT environment using read-only credentials and standard platform instrumentation.

3

Profile target systems

Billing, configuration, performance and network metrics are captured to characterize application workloads and the underlying IT infrastructure.

4

Upload data

OnelQ Pulse encrypts data using asymmetric cryptographic protocol and uploads it over HTTPS to the OnelQ Central data warehouse.

5

Store data

Data is securely synchronized with the OnelQ Central, where private keys are located, and stored on encrypted cloud storage in Microsoft Azure.

6

Data analysis

The IT environment, and the workspaces its connected to, are accessible in the OnelQ Portal to authorized, authenticated users.

7

Remove data

Access to the IT environment can be disabled by removing it from the workspace or deleting it altogether.

OnelQ Pulse

OnelQ profiles application workloads, underlying IT infrastructure and network in your environment using the agentless OnelQ Pulse connector.

System Requirements

OnelQ Pulse should be deployed according to the following system requirements:



CONTAINERS



CLOUD



DATACENTER



NETWORK

SECURITY FEATURES

AGENTLESS ARCHITECTURE

OnelQ does not deploy agents to avoid increasing the attack surface on target systems.

DIGITAL SIGNATURES

OnelQ Pulse is digitally signed to prevent tampering with embedded scripts and software assemblies.



SECURED CREDENTIALS

Passwords for target systems are encrypted using AES-256 and are never displayed in plain text or transmitted externally.

ZERO TRUST

SSL/TLS certificates and SSH host keys must be valid or manually trusted for all discovered target systems.



RUNTIME DATA ENCRYPTION

Collected data is encrypted using a unique key for the IT environment to prevent unauthorized data extraction.

SECURE COMMUNICATION

OnelQ Pulse uploads data to the OnelQ Central over a secure HTTPS channel.



SOFTWARE UPDATES

Security patches and new security features are automatically downloaded and installed.

IT Environments

The IT environment acts as a security boundary for the following data within a OneIQ account:

- Application metrics, traces and logs
- Billing data from AWS, Azure and GCP
- Configuration, performance and network data from container, cloud and datacenter platforms profiled by OneIQ Pulse connectors

Cloud-Native Applications

Kubernetes,
Red Hat OpenShift



Datacenter Platforms

VMware, Microsoft
Hyper-V and
Windows, Linux

vmware®



Cloud Platforms

Amazon Web
Services, Microsoft
Azure, GCP



HCI Platforms

Azure Stack HCI,
Nutanix, VMware vSAN



vmware®

Collected Data

OneIQ Pulse collects configuration, performance and network data in real-time.



Configuration Data

Clusters, hosts, nodes,
cloud instances, VMs,
network and storage.



Performance Data

CPU, memory, storage,
network consumption
and utilization.



Network Flows

Cloud and datacenter
platforms: IPFIX, JFlow
and NetFlow

OnelQ Central and Portal

Billing, configuration, performance and network metrics are uploaded by OnelQ Pulse over HTTPS to the OnelQ Central data warehouse, which is hosted in the Canada Central (Toronto) region of Microsoft Azure. OnelQ employs the following Microsoft Azure security features:

- **Azure Firewall** to protect OnelQ network resources and services.
- Secure cloud storage with **encryption-at-rest**.

A security boundary is implemented around each IT environment and all secure workspaces it is connected to. Application workload and IT infrastructure data is only visible to authenticated, authorized users through the web-based OnelQ Portal.

ISO/IEC 27001

OnelQ maintains the ISO/IEC 27001 Information Security Management certification through the British Standards Institution (BSI), one of the leading certification bodies and original contributors to the ISO/IEC 27001 standard. OnelQ regularly performs:



Surveillance Audits

OnelQ undergoes annual ISO/IEC 27001 surveillance audits with BSI to ensure continuous improvements to our information security management system (ISMS).



Penetration Testing

OnelQ conducts application and infrastructure testing annually through a leading security firm, which also works with clients in defense, financial services and public sectors.

Organizational Policies

Information Security Officer

OnelQ has an Information Security Officer, who is responsible for compliance with the ISO/IEC 27001 standard, continuous improvement to our information security policies and procedures, and incident management.

Security Screening

New staff must undergo criminal record and employment verification checks before joining OnelQ. All contracts include a confidentiality agreement.

2FA and SSO

All OnelQ systems have rigorous access controls and require single-sign-on (SSO) with two-factor authentication (2FA).

Incident Management

OnelQ has rigorous information security incident management procedures for mitigating security incidents and communicating security events.

Security Training

All staff must go through security training when they join OnelQ and at least once annually.

Infrastructure Security

Supplier Security

OnelQ has a rigorous onboarding process for new suppliers and conducts annual reviews for existing suppliers to ensure that they have sound privacy and security policies in place.

Extensive Logging

OnelQ performs extensive logging to identify and mitigate security risks and vulnerabilities.

Endpoint Security

All endpoints used by staff have BitLocker encryption and security scanning software. Staff must use single-sign-on and follow clear-screen policies.

For further information, please contact the OnelQ information security team at security@oneiq.com

Copyright © 2024. OnelQ Corp.
All Rights Reserved.