Quest

Quest® Security Guardian

Security Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

20 Enterprise, Suite 100

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

Security Guardian Security Guide
Updated -December 19, 2024

Contents

Introduction

Managing information system security is a priority for every organization. In fact, the level of security provided by software vendors has become a differentiating factor for IT purchase decisions. Quest strives to meet standards designed to provide its customers with their desired level of security as it relates to privacy, confidentiality, integrity and availability.

This document describes the security features of Quest® Security Guardian. This includes access control, protection of customer data, secure network communication, and cryptographic standards.

About Security Guardian

Quest® Security Guardian is an integrated On Demand solution that helps you keep the Active Directory domain(s) and Entra ID tenant(s) in your organization secure.

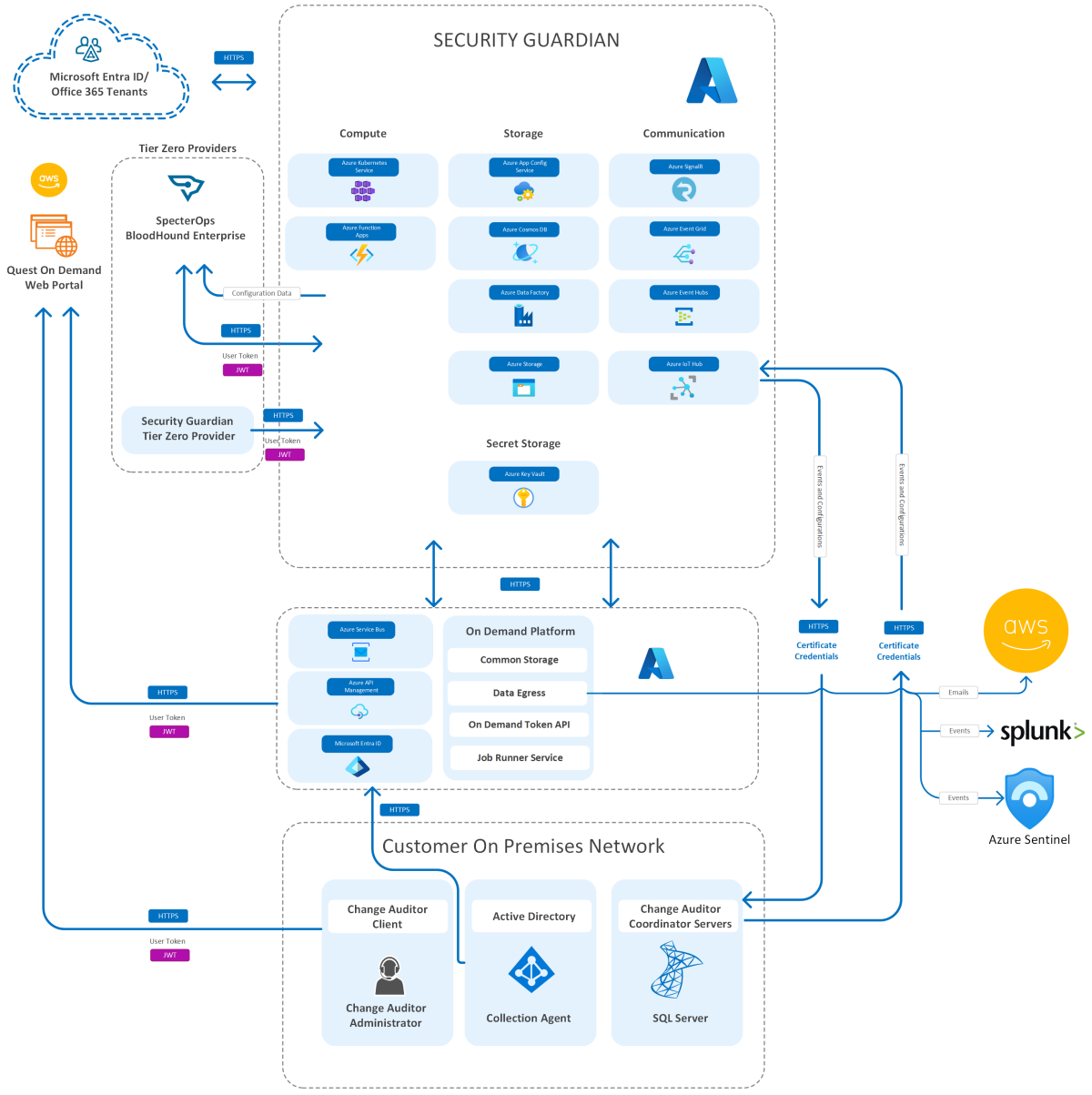
You can:

- Identify Tier Zero objects in Active Directory.
- Identify Privileged objects in Entra ID.
- Certify that objects are indeed Tier Zero or Privileged and, when Quest Change Auditor version 7.4 is integrated, protect Active Directory Tier Zero objects against unauthorized or accidental modification or deletion.
- Run pre-defined Security Assessments to identify vulnerabilities in Active Directory and Entra ID and create your own Assessments.
- Investigate Findings for Tier Zero and Privileged objects, vulnerabilities identified through Assessments, and Critical Activity from On Demand Audit.
- Have Findings forwarded to a SIEM tool and alerts sent to selected email recipients.

Architecture Overview

The following scheme shows the key components of the Security Guardian configuration.

Figure 1: High-Level Architecture



Azure Datacenter Security

Microsoft Azure datacenters have the highest possible physical security and are considered among the most secure and well protected datacenters in the world. They are subject to regular audits and certifications including Service Organization Controls (SOC) 1, SOC 2, and ISO/IEC 27001:2005.

Relevant references with additional information about the Windows Azure datacenter security can be found here:

- Microsoft Azure Trust Center: https://azure.microsoft.com/en-us/overview/trusted-cloud/
- Microsoft Trust Center Compliance: https://www.microsoft.com/en-us/trust-center/compliance/complianceoverview?service=Azure#Icons
- Microsoft's submission to the Cloud Security Alliance STAR registry: https://cloudsecurityalliance.org/star/registry/microsoft/
- Whitepaper: Standard Response to Request for Information – Security and Privacy: http://www.microsoft.com/en-us/download/details.aspx?id=26647
- Microsoft Global Datacenters: Security & Compliance: https://azure.microsoft.com/en-us/explore/global-infrastructure/
- Azure data security and encryption best practices: https://learn.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices

Overview of Data Handled by Security Guardian

Security Guardian manages the following type of customer data:

- Active Directory objects such as users, groups, computers and domains are provided by the On Demand Hybrid Agent via Event Hubs and stored in the Azure Data Explorer product database and in Azure Storage BLOBs.
- Entra ID objects such as users, groups, roles, service principals and tenants are provided by the On Demand Entra ID collector via Event Hubs and stored in the Azure Data Explorer product database and in Azure Storage BLOBs.
- Active Directory and Entra ID object content is persistently stored by the product. Data collected is stored in Azure Event Hubs and then in Azure Data Explorer and Azure Storage BLOBs and is encrypted at rest.
- The application does not collect or store Active Directory object passwords.

Admin Consent and Service Principals

Security Guardian requires Admin Consent for Entra ID collections.

Location of Customer Data

When a customer signs up for On Demand, they select the region in which to run their On Demand organization. All computation is performed, and all data is stored in the selected region. The currently supported regions can be found here https://regions.quest-on-demand.com

Azure Storage, including the Blobs, Tables, and Queues storage structures, are replicated three times in the same datacenter for resiliency against hardware failure. The data is replicated across different fault domains to increase availability. All replication datacenters reside within the geographic boundaries of the selected region.

See this Microsoft reference for more details: https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy

Privacy and Protection of Customer Data

A common concern related to cloud-based services is the prevention of commingling of data that belongs to different customers. Security Guardian has architected its solution to specifically prevent such data commingling by logically separating customer data stores. Information such as Active Directory and Entra ID objects are all stored in Azure Data Explorer with each customer having their own database. However, items such as Assessments and Assessment results are stored within the same Azure Storage Account and partitioned by the Customer Organization ID and the Azure Tenant ID.

Customer data is differentiated using a Customer Organization Identifier. The Customer Organization Identifier is a unique identifier obtained from the Quest On Demand Platform that is created when the customer signs up with the application. This identifier is used throughout the solution to ensure strict data separation of customers' data in the Azure Data Explorer database and during processing.

Network Communications

Internal network communication within Azure includes inter-service communication between Security Guardian components and the On Demand Platform.

Inter-service communication uses OAuth authentication using a Quest Entra ID service account with the rights to access the services. No backend services of Security Guardian can be used by end users.

On Demand Services accepts access to Security Guardian from the On Demand web user interface.

All external communication is secured with HTTPS TLS 1.2.

The Security Guardian user interface uses OAuth authentication with a JWT token, issued to a logged in user.

Authentication of Users

The customer logs in to the application by providing On Demand user account credentials.

For more information about user authentication, please refer to the Quest On Demand Global Settings Security Guide.

Role Based Access Control

Quest On Demand is configured with default roles that cannot be edited or deleted and allows you to add custom roles to make permissions more granular. Each access control role has a specific set of permissions that determines what tasks a user assigned to the role can perform. For more information on role-based access control, please refer to the Quest On Demand product documentation.

FIPS 140-2 Compliance

Security Guardian cryptographic usage is based on Azure FIPS 140-2 compliant cryptographic functions. For more information, see Microsoft-us/azure/storage/blobs/security-recommendations.

SDLC and SDL

The On Demand team follows a strict Quality Assurance cycle.

- Access to source control and build systems is protected by domain security, meaning that only employees on Quest's corporate network have access to these systems. Therefore, should an On Demand developer leave the company, this individual will no longer be able to access On Demand systems.
- All code is versioned in source control.
- All product code is reviewed by another developer before check in.
- Regularly scheduled static code analysis is performed on regular basis.
- Regularly scheduled vulnerability scanning is performed on regular basis.
- Segregated Development, Pre-Production, and Production environments. Customer data is not used in Development and Pre-Production environments.
- In addition, the On Demand development team follows a managed Security Development Lifecycle (SDL) which includes:
    - MS-SDL best practices
    - Threat modelling
    - OWASP guidelines

On Demand developers go through the same set of hiring processes and background checks as other Quest employees.

Third Party Assessments and Certifications

Penetration Testing

On Demand has undergone a third-party security assessment and penetration testing yearly since 2017. The assessment includes but is not limited to:

- Manual penetration testing
- Static code analysis with Third Party tools to identify security flaws

A summary of the results is available upon request. No OWASP Top 10 critical or high-risk issues have been identified.

Certification

On Demand is included in the scope of the Platform Management ISO/IEC 27001, 27017 and 27018 certifications:

- ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements: **C710-ISMS222-07-19**, valid until **2025-07-28**.
- ISO/IEC 27017 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services: **C711-ITCS2-07-19**, valid until **2025-07-28**.
- ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors: **C712-ITPII2-07-19**, valid until **2025-07-28**.

Quest Software, Inc. has successfully completed a SOC 2 examination of its On Demand solution. The examination was performed by an independent CPA firm for the scope of service described below.

Examination Scope: **Quest On Demand Platform**

Selected SOC 2 Categories: **Security**

Examination Type: **Type 2**

Review Period: **August 1, 2022 to July 31, 2023**

Service Auditor: **Schellman & Company, LLC**

Operational Security

Source control and build systems can only be accessed by Quest employees on Quest's corporate network (domain security). If a developer (or any other employee with access to Security Guardian) leaves the company, the individual immediately loses access to the systems.

All code is versioned in source control

Access to Data

Access to Security Guardian data is restricted to:

- Quest Operations team members
- Specific Quest Support team members working closely with Security Guardian product issues
- The Security Guardian development team, providing support for the product

Access to Security Guardian data is restricted through the dedicated Quest Entra ID security groups. For different types of data (e.g., product logs, customer data, and sensitive data), different access levels, and lists of allowed people are assigned.

Permissions Required to Configure and Operate Security Guardian

Quest Operations team members have access to Quest's production Azure Subscription and monitor this as part of normal day to day operations. Security Guardian developers have no access to Quest's production Azure Subscription.

To access Security Guardian, a customer representative opens the On Demand website and signs up for an On Demand account. The account is verified via email; thus, a valid email address must be provided during registration.

An organization is automatically created once the new account is created.

Operational Monitoring

Security Guardian internal logging is available to Quest Operations and Security Guardian development teams during the normal operation of the platform. Some customer or Personally Identifiable Information (PII) data can become a part of internal logging for troubleshooting purposes.

Production Incident Response Management

Quest Operations and Quest Support have procedures in place to monitor the health of the system and ensure any degradation of the service is promptly identified and resolved. Security Guardian relies on Azure infrastructure, and as such, is subject to the possible disruption of these services.

- Quest On Demand services status page is available at https://status.quest-on-demand.com/.
- Azure services status page is available at https://azure.microsoft.com/en-ca/status/.

Customer Measures

Security Guardian security features are only one part of a secure environment. Customers must implement their own security practices when proceeding with data handling. Special care needs to be given to protecting the credentials of the Active Directory administrator accounts.

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product