Quest®

Quest® Change Auditor Threat Detection 7.0
Deployment Guide

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

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (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, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Change Auditor Threat Detection Deployment Guide
Updated - March 2018
Software Version - 7.0

Contents

1

Deploying Threat Detection

Introduction to Change Auditor Threat Detection

To protect your data and your business, Change Auditor Threat Detection uses advanced machine learning, user and entity behavioral analytics (UEBA), and SMART correlation technology to spot anomalous activity and identify the highest risk users in your environment. The users with the highest risk scores are then highlighted in the Threat Detection dashboard, enabling you to prioritize your response and adjust policies to strengthen your organization's security and regulatory enforcement.

For details about using the Threat Detection dashboard see the Change Auditor Threat Detection User Guide.

This guide gives information about how Change Auditor integrates with the Threat Detection server to process event data. It is intended for administrators who are responsible for the implementation, deployment, and monitoring of the Change Auditor Threat Detection deployment and configuration.

Who should have input on the deployment plan?

A complete deployment plan requires the combined effort of the resources within your organization who are responsible for information security, such as:

- Chief Information Security Officers who understand the complexities of the enterprise's IT infrastructure and are responsible for the overall handling of key vulnerabilities. Change Auditor provides data to help them deliver security updates and communications.
- Security architects who are responsible for building and overseeing the implementation of the network's security measures. They need to define the threat priorities for their environment.
- Database and network administrators who are responsible for the implementation, deployment, and monitoring of the Change Auditor Threat Detection configuration.
- Auditors and network administrators who are responsible for reviewing the potential threats, optimizing the system by inputting feedback, and prioritizing and investigate the most serious threats.

Components and workflow

Change Auditor sends events in real time to the Threat Detection server to be used for analysis based on calculated user behavior baselines.

See the Change Auditor Threat Detection User Guide for details on Threat Detection concepts and terms.

The following must be performed to enable Threat Detection:

1. Apply the required licenses. (Change Auditor Threat Detection and any required Change Auditor auditing modules.) If you are using more than one coordinator, apply the license to all of them. To verify that a license is applied, right-click the coordinator icon in the system tray and select Licensing.
2. Configure required events for Threat Detection. See Events to configure.
3. Deploy the Threat Detection server on a virtual computer. See Deploying the Threat Detection server.
4. Configure Change Auditor to send collected event data to the Threat Detection server. See Creating a Threat Detection configuration.
5. Login to the Threat Detection dashboard to see the alerts and data. See the Threat Detection User Guide for information about navigating the dashboard and using the data to secure your environment.

Requirements and prerequisites

For a successful deployment, ensure that your environment meets the minimum system requirements.

NOTE: The Threat Detection server is available in both 8 and 16 cores versions. The number of cores impact the length of time it takes to process historical audit data and build baseline.

Minimum system requirements for the Threat Detection server:

- VMWare ESX version 5.5 and above
- Small and medium sized enterprise edition OVA:

  NOTE: The 8 core edition is most appropriate if Change Auditor is sending and the Threat Detection server is processing less than 5 Million events per day.

  - OVA file size: ~10GB
  - CPU: 8 cores, Minimal 2.3 GHz, Recommended 2.4 GHz
  - RAM: 64 GB
  - I/O: 500 MB/sec
  - Disk: SAS 320 GB, SAS 930 GB
- Large sized enterprise edition OVA:
  - OVA file size: ~10GB
  - CPU: 16 cores, Minimal 2.3 GHz, Recommended 2.4 GHz
  - RAM: 64 GB
  - I/O: 500 MB/sec
  - Disk: SAS 320 GB, SAS 930 GB
- Obtain a static IP address for Threat Detection server and add DNS (A) record for it.
- Determine the number of historical days to use for your activity baseline. For information on how to determine the best amount for you, see Historical events and your baseline calculations.

Events to configure

NOTE: Consider Maintaining the Change Auditor database size when adding events for Threat Detection auditing.

Events from the following modules are used to build models and generate alerts:

Table 1. Events used for modeling and alerts

Module	Events
Change Auditor for Logon Activity	Authentication Activity events – these are the successful and failed interactive and remote interactive events (all enabled by default). Domain Controller Authentication events – Ensure that you enable the ‘User authenticated through Kerberos” event. By default, it is disabled.

Table 1. Events used for modeling and alerts

Module	Events
Change Auditor for Active Directory	User and group events (all enabled by default)
Change Auditor for Windows File Servers Change Auditor for EMC Change Auditor for FluidFS Change Auditor for NetApp	For optimal Threat Detection results, Quest recommends that you select file, folder, and share events that audit permission changes, create, delete, rename, and open actions during the template creation.

Maintaining the Change Auditor database size

Some of the events required for Threat Detection can be very noisy and take up space in the Change Auditor database. Once the events are sent to the Threat Detection server for analysis storage in the Change Auditor database is no longer needed.

To ensure the database maintains a manageable size, Quest recommends that you purge events older than 30 days.

Particularly noisy events are:

- User authenticated through Kerberos
- File and folder open

Deploying the Threat Detection server

To download the Threat Detection server go to https://support.quest.com/change-auditor/download-new-releases.

The Threat Detection server, which is a a version of Red Hat Enterprise Linux 6 (64 bit), is available as Open Virtual Appliance (OVA) file that needs to be deployed on VMWare ESXi using VMWare VSphere Client.

NOTE: Depending on the version of the ESXi, the deployment steps may be different. The below steps outline the process for vSphere Client version 6.5.

To deploy the Threat Detection server

1. Open vSphere Web Client (Flash) version.

   NOTE: VMWare VSphere Client should be connected to VMWare vCenter not an individual ESXi host.

2. Select **Actions | Deploy OVF Template**.
3. Under **Select template**, choose **Local file**, browse for the OVA template, and click **Next**.

   NOTE: The file should be located on the computer where the VSphere client is being used.

4. Under **Select name and location**, specify the name and inventory location for the deployed template and click **Next**.
5. On **Select a resource**, choose the destination computer for the OVA and click **Next**.
6. Under **Review details**, verify the OVF template details and click **Next**.

7 Under **Select Storage**, select the datastore for the configuration and the disk files and click **Next**. The **Thin Provision** option is recommended.

8 Under **Select networks**, choose a destination network for the virtual computer and select **Next.**

9 Under **Customize template**, enter the deployment properties for the Threat Detection sever.

Property	Description
Hostname	Fully qualified domain name of the Threat Detection server that has been registered in DNS For example: hostname.yourcompamy.com
IP Address	Static IPv4 address of the Threat Detection server
Subnet Netmask	Subnet mask For example: 255.255.255.0
Default Gateway	Default gateway IP address
DNS	DNS server IP address
Password	Password required for the integration between Change Auditor and the Threat Detection server. The integration password is used during the Threat Detection configuration and accessing the Tread Detection dashboard from a Chrome browser. The password must be 8-24 characters and can only include the following supported values: a-z, A-Z, 1-0, @,$. Maintain this password for creating the Threat Detection configuration.

10 Click **Next**.

11 Under **Ready to complete**, verify the information and click **Finish.**

12 Once the deployment in complete, power on the Threat Detection server.

13 Quest recommends that you take a snapshot of the newly deployed virtual server. This allows you to revert to a clean state without redeploying the server if you need to start over or re-create a configuration.

You are now ready to create a Threat Detection configuration in Change Auditor.

Creating a Threat Detection configuration

A Threat Detection configuration must be created before you can view activity, receive alerts, and analyze anomalies on the dashboard.

The status of the Threat Detection configuration is displayed on the configuration page. The configuration is either:

- Configured - All Change Auditor settings are properly applied.
- Not Configured - Change Auditor does not have an existing Threat Detection configuration. If you see this status after removing a configuration and want to configure Threat Detection again, see Removing a configuration for details.
- A valid Change Auditor Threat Detection license is required - Information is provided on how to obtain a license.

To create a Threat Detection configuration

NOTE: Selecting the Refresh button, will provide an accurate state of the configuration - that is to say, whether it is currently configured, unconfigured, or a license update is required.

1. From Change Auditor select **Administration Tasks | Configuration | Threat Detection**.
2. Enter the Threat Detection server fully qualified domain name and integration password you created when deploying the Threat Detection server.
3. Select how many days of historical events should be sent to Threat Detection server. For information on how to determine the best amount for you, see Historical events and your baseline calculations.
4. Select **Apply Changes**.

Reviewing configuration status

To see Threat Detection configuration status

1. Select **Administration Tasks | Configuration | Threat Detection**.
2. Click **Refresh** to update the Threat Detection configuration from Change Auditor.

   The following deployment details are displayed:

   - State of the configuration
   - How many historical events have been sent to Threat Detection server.
   - Status of the Threat Detection server.
   - Status of the data processing. For example, building baseline.
   - Threat Detection server version.
   - Threat Detection subscription ID.
   - Starting point in time for events to send.
   - Subsystems that contain the event data that is being sent.
   - Whether the Threat Detection subscription is enabled.
   - How often how often (in milliseconds) events are sent.
   - Interval (in milliseconds) that a heartbeat check is made for the configuration.
   - Batch size. (The maximum number of events to include in a single notification message.)
   - Url for notifications.
   - Url for heartbeat notifications.
   - When the last event was sent.
   - Last event response (For example OK, HTTP 429 - Too many events being sent, and HTTP 401 - Unauthorized access.)
   - When the last heartbeat was sent.
   - When the last heartbeat response. (For example OK, HTTP 429 - Too many events being sent, and HTTP 401 - Unauthorized access.)
   - Number of events sent.
   - Number of batches sent.
   - Number of heartbeats sent.
   - Time of the event that was last sent.

- List of coordinators permitted to send events.
- The coordinator that is sending events. If the subscription is disabled, this is the last coordinator sending the events.

Removing a configuration

In the current version of Change Auditor, deleting the configuration only removes configuration information from Change Auditor. It does not remove data or configuration on the Threat Detection server.

If you are removing the configuration as a part of a clean up process, you can delete the Threat Detection server after removing configuration.

If you are removing the configuration and plan to start over with the same Threat Detection server, you can either revert to a snapshot of the server taken right after it was deployed or replace the existing Threat Detection server with a new server.

To remove a Threat Detection configuration

1. Select **Administration Tasks | Configuration | Threat Detection**.
2. Click **Remove Configuration**.

   This removes the Threat Detection configuration from Change Auditor.

Historical events and your baseline calculations

Before the Threat Detection server can generate alerts, it needs to establish user behavior baseline. The baseline is built by processing 30 days of historical or real time events. Refer to the Change Auditor Threat Detection User Guide for information about baseline modeling.

When you create the Threat Detection configuration, you can specify how many days of historical events should be sent to the Threat Detection server to create the baseline.

NOTE: The baseline is more accurate if it is built using the exact configuration of events that you plan to analyze on an ongoing basis. If a new event is enabled after the initial baseline has been built (for instance, the User authenticated through Kerberos event) it may initially be treated as an anomaly as there is no history of it in the baseline.

Table 2. How to determine which type of events to use for a baseline

Type of events to use	When to use...
Real-time events (0 days) **NOTE:** It will take at least 30 days before you start seeing alerts in the Threat Detection dashboard.	• For a new installation of Change Auditor where no events have been collected. • If you just enabled events that need to be analyzed by Change Auditor Threat Detection.
Historical events (more than 0 days)	• If you have been collecting all events supported by Change Auditor Threat Detection. • If you are not purging any of the events supported by Change Auditor Threat Detection.

Use the following as guidance on the number of days to specify when you create your Threat Detection configuration:

- You should not specify more days than the number of days of events that exist in the Change Auditor database.

- You can enter between 1 and 90 days.
- If you specify less than 30 days, Threat Detection uses real time events to continue to build a baseline until 30 days of event have been analyzed.
- If you specify more than 30 days, the Threat Detection server starts generating alerts for any abnormal activity that happened after 30 days.

2

Threat Detection configuration commands

- Adding the PowerShell module
- Viewing available commands and help
- Connecting to Change Auditor
- Managing a Threat Detection configuration

Adding the PowerShell module

Change Auditor comes with a PowerShell module for you to use to manage your Threat Detection deployment. It is installed when you install the Windows client or a coordinator.

NOTE: Windows PowerShell version 3.0 or higher is required.

To import the Change Auditor PowerShell module:

1. Open a Windows PowerShell window and type the following at the Windows PowerShell command prompt:

   ```
   Import-Module <path>
   ```

   Where "<path>" is the file path for the ChangeAuditor.PowerShell.dll assembly found in the Change Auditor Windows client or Change Auditor coordinator folder.

2. To ensure that the module was added, type the following at the Windows PowerShell command prompt:

   ```
   Get-Module -All
   ```

   The registered PowerShell modules are listed.

Viewing available commands and help

- To view all available Change Auditor commands, enter:

  ```
  Get-Command -Module ChangeAuditor.PowerShell
  ```

- To view help on each command including the syntax, enter:

  ```
  Get-Help cmdletName
  ```

- To view an interactive command browser that shows you the layout of commands and the help for the commands, enter:

  ```
  Show-Command cmdletName
  ```

Threat Detection sample scripts

Change Auditor includes the following sample scripts to help you configure and manage Threat Detection:

- CreateThreatDetectionConfiguration.ps1
- GetThreatDetectionConfiguration.ps1
- ModifyThreatDetectionConfiguration.ps1
- RemoveThreatDetectionConfiguration.ps1

NOTE: By default they are located here: C:\Program Files\Quest\ChangeAuditor\Client\PowerShell Sample Scripts

Connecting to Change Auditor

- Connect-CAClient

Connect-CAClient

Most Change Auditor commands require a connection to a coordinator. You can make multiple connections to different coordinators or deployments in the same script as long as the version of Change Auditor is the same.

This connection can be assigned to a variable and used for any command that requires it. Use this command to search for a suitable coordinator in a Change Auditor installation and create a connection. Suitable coordinators are those which you have access to and can be located by searching through Active Directory service connection points.

NOTE: Connections are closed when the PowerShell session is ended or disconnected.

Table 1. Available parameters

Parameter	Description
-Credential (Optional)	Windows credentials specifying the user to connect to the Change Auditor installation. All operations using this connection will be authorized as this user. When not specified, the current client running PowerShell is used.
-CoordinatorConnectionPoint (Optional)	Specify to use a specific coordinator found from a previous call to Find-CACoordinators.
-SelectLocalCoordinator (Optional)	Create a connection to the local coordinator.
-InstallationName (Optional)	The installation name to connect to. If an installation cannot be found with this name, no connection is made. If more than one Change Auditor installation exists in the current forest, this parameter is mandatory. Omitting it results in a connection failure due to ambiguity.
-DomainName (Optional)	The name of the domain where the Change Auditor installation exists.
-ComputerName (Optional)	The computer to connect to.
-Port (Optional)	The port to connect to.
-WaitForServiceReady (Optional)	The number of seconds to wait for the connected coordinator service to be ready. **NOTE:** If not specified, when the Change Auditor coordinator is not ready for connections due to an in-progress install or upgrade, an error is returned. The maximum is 144,000 seconds, or 10 hours.

Example: Connect to the installation “XYZ” in the specified domain

```
Connect-CAClient –InstallationName ‘XYZ’ -DomainName 'DomainName.com'
```

Managing a Threat Detection configuration

- New-CAThreatDetectionConfiguration
- Get-CAThreatDetectionConfiguration
- Set-CAThreatDetectionConfiguration
- Remove-CAThreatDetectionConfiguration

New-CAThreatDetectionConfiguration

Use this command to create a Threat Detection configuration.

NOTE: Quest recommends that you use the sample script CreateThreatDetectionConfiguration.ps from Program Files\Quest\ChangeAuditor\Client\PowerShell Sample Scripts.

NOTE: When you create a new configuration, the underlying webhook subscription that is generated is marked as internal. This ensures that the required subscription cannot be removed from an existing configuration.

Table 2. Available parameters

Parameter	Description
-Connection	A connection obtained by using the Connect-CAClient command. See Connecting to Change Auditor.
-TDServer	The Threat Detection server fully qualified domain name.
-TDPassword	The password used to access the Threat Detection server. Use the integration password that was specified during the Threat Detection server deployment.
-HistoricalDays (Optional)	The number of days of historical events to send to the Threat Detection server. For details, see Historical events and your baseline calculations.
-AllowedCoordinators (Optional)	The DNS or NetBIOS name of the coordinators permitted to send events. If none are specified, all coordinators installed at the time of configuration are permitted to send events. **NOTE:** The list order does not determine which coordinator is selected to send events.

Example: Creating a configuration

```
New-ThreatDetectionConfiguration -Connection $connection -TDServer
'ServerName.Domain.Com' -TDPassword $TDPassword -HistoricalDays 30
-AllowedCoordinators @('machine1.domain.com','machine2.domain.com')
```

Get-CAThreatDetectionConfiguration

Use this command to view the Threat Detection configuration information and information about the associated subscription.

Table 3. Available parameters

Parameter	Description
-Connection	A connection obtained by using the Connect-CAClient command. See Connecting to Change Auditor.

Example: Review Threat Detection configuration details

```
Get-ThreatDetectionConfiguration -Connection $connection
```

Command output

The command returns the following information. For more information about some of these settings see the Change Auditor SIEM Integration Guide.

Table 4. Available configuration information

Setting	Description
TDServer	The Threat Detection server fully qualified domain name.
ConfigurationState	State of the configuration: • Configured: Threat Detection has been configured • Unconfigured: Threat Detection has not been configured • A valid Change Auditor Threat Detection license is required
HistoricalDays	How many days of historical events have been sent to Threat Detection server
TDServerStatus	Status of the Threat Detection server: • Online • Offline
DataProcessingStatus	Status of the data processing. For example, building baseline.
TDServerVersion	Threat Detection server version.
TDSubscriptionId	Threat Detection subscription ID.
StartTime	Starting point in time for events to send.
Subsystems	Subsystems that have been selected for event sending.
TDSubscriptionEnabled	Whether the Threat Detection subscription is enabled.
NotificationInterval	How often how often (in milliseconds) events are sent.
HeartbeatInterval	Interval (in milliseconds) that a heartbeat check is made for the configuration.
BatchSize	Batch size. (The maximum number of events to include in a single notification message.)
NotificationUrl	Url for notifications.
HeartbeatUrl	Url for heartbeat notifications.
LastEventTime	When the last event was sent.
LastEventResponse	Last event response (For example OK, HTTP 429 - Too many events being sent, and HTTP 401 - Unauthorized access.)
LastHeartbeatTime	When the last heartbeat was sent.
LastHeartbeatResponse	When the last heartbeat response. (For example OK, HTTP 429 - Too many events being sent, and HTTP 401 - Unauthorized access.)
EventsSent	Number of events sent.
BatchesSent	Number of batches sent.
HeartbeatsSent	Number of heartbeats sent.
BookmarkTime	Time of the event that was last sent.
AllowedCoordinators	List of coordinators permitted to send events.
LastCoordinator	The coordinator that is sending events. If the subscription is disabled, this is the last coordinator sending the events.

Set-CAThreatDetectionConfiguration

Use this command to modify the list of allowed coordinators for the Threat Detection configuration.

Table 5. Available parameters

Parameter	Description
-Connection	A connection obtained by using the Connect-CAClient command. See Connecting to Change Auditor.
-AllowedCoordinators (Optional)	The DNS or NetBIOS name of the coordinators permitted to send events. If none are specified, all coordinators installed at the time of configuration are permitted to send events. **NOTE:** The list order does not determine which coordinator is selected to send events.

Example: Modifying a configuration

```
Set-CAThreatDetectionConfiguration -Connection $connection -AllowedCoordinators
@('machine1.domain.com','machine2.domain.com')
```

Example: To clear a previous list of allowed coordinators

```
Set-CAThreatDetectionConfiguration -Connection $connection -AllowedCoordinators @()
```

Remove-CAThreatDetectionConfiguration

Use this command to remove a Threat Detection configuration.

NOTE:

In the current version of Change Auditor, deleting the configuration only removes configuration information from Change Auditor. It does not remove data or configuration on the Threat Detection server.

- If you are removing the configuration as a part of a clean up process, you can delete the Threat Detection server after removing configuration.
- If you are removing the configuration and plan to start over with the same Threat Detection server, you can either revert to a snapshot of the server taken right after it was deployed or replace the existing Threat Detection server with a new server.
- If you are removing the configuration and plan to start over with a new Threat Detection server, you can either revert to a snapshot of the server taken right after it was deployed or replace the existing Threat Detection server with a new server.

Table 6. Available parameters

Parameter	Description
-Connection	A connection obtained by using the Connect-CAClient command. See Connecting to Change Auditor.

Example: Remove the Threat Detection configuration

```
Remove-ThreatDetectionConfiguration -Connection $connection
```

3

Appendix: System Architecture

- Threat Detection system overview

Threat Detection system overview

The integration process to analyze events includes the following:

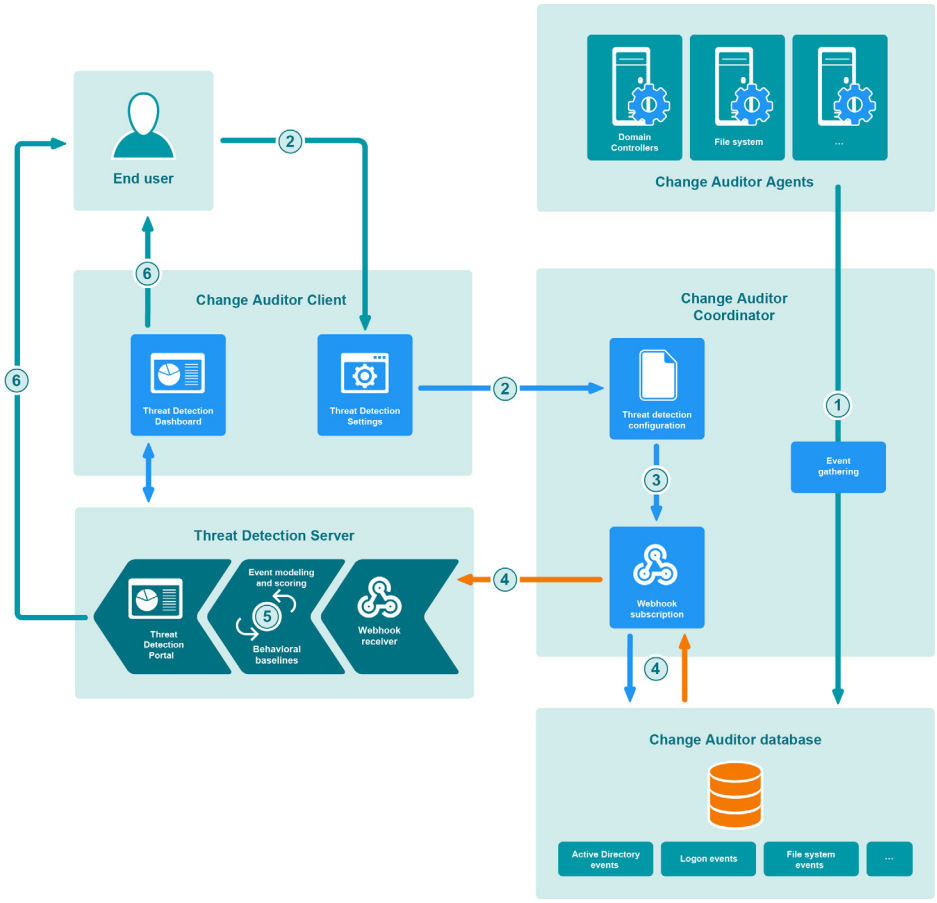

Figure 1. Event processing for Threat Detection

1. Change Auditor agents collect events from various systems and the coordinator writes the events into the database.
2. Users create a Threat Detection configuration using the Change Auditor client.
3. As part of the configuration, the coordinator creates the webhook subscription to send events to the Threat Detection server. The subscription contains information such as where to send events (the URL of the webhook receiver in the Threat Detection server), which events to include, and the coordinator responsible for event forwarding.
4. The designated coordinator continually queries events from the Change Auditor database and sends them to the webhook receiver in the Threat Detection server.
5. Threat Detection server performs event modeling and scoring.
6. Threat indicators, alerts, and risky users are displayed in Threat Detection dashboard.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

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.