Enabling Behavioral Analytics Using Micro Focus Interset

Advanced Authentication uses Risk Service to assess the risk associated with an access attempt based on the contextual information. For example, the contextual information can be IP address and device information.

Risk Service uses deterministic, rule-based computation. It enables organizations to find threats quickly with known attack patterns and take appropriate actions.

For more information about Risk Service, see Introduction to Risk Service (https://www.netiq.com/documentation/risk-service-2.0/admin/data/ovrvw_risk_srv.html).

Some threats are very complex and difficult to trace through rule-based computation. These unknown threats are unpredictable and do not leave any evidence behind. The evidence might be hidden within your data. These threats require a more sophisticated approach to anomaly detection using machine learning.

To enable the unknown threat or anomaly detection, **Risk Service** integrates with **Interset** and leverages its *User and Entity Behavioral Analytics* (UEBA) capability. Using the organization's data, Interset establishes the normal behavior for the organizational entities and then, using advanced analytics and machine learning, identifies the anomalous behaviors that constitute potential risks such as compromised accounts, insider threats, or other unknown cyber threats.

For more information, see User and Entity Behavioral Analytics (https://www.microfocus.com/media/flyer/user-and-entity-behavioral-analytics-flyer.pdf).

The following are a few examples of anomalies in behavioral access control:

- A large number of session authentication successes and failures
- A large number of application access events
- A large number of distinct applications accessed
- Unusual application access events
- Unusual browser used during authentication
- Unusual working hours or working days

This integration enables Risk Service to perform the following actions by using behavioral analytics:

- Detect compromised account and bots
- Detect insider threats
- Detect compromised network, host, and devices
- Detect unknown threats

In This Guide:

1 Example Scenarios

The following are a few common scenarios where enabling behavioral analytics helps accelerate threat detection:

1.1 Scenario: Compromised Account Detection

Albert works in a Healthcare organization. He browses news sites from his corporate computer. One day, he inadvertently clicks a malicious URL that injects the spyware script in his browser. The script starts accessing numerous sensitive applications and downloading the data.

Interset identifies a sudden increase in the number of access attempts and network lateral movements from Albert's system. Interset classifies this as high risk and shares his risk score with Risk Service. Advanced Authentication blocks Albert from accessing any application.

1.2 Scenario: Insider Threats Detection

Daniel, a helpdesk engineer, accesses the sensitive data and explores various corporate resources from home at night. Interset detects the anomalous behavior and classifies Daniel as a high-risk user. Interset shares the risk score with Risk Service. Advanced Authentication blocks access for Daniel before anything too malicious happens.

Olga, an engineer, is erroneously given access to a privileged application. She decides to browse that application from home on a weekend. Interset detects this privileged access abuse and increases her risk. Advanced Authentication blocks Olga's access to the application.

Lucio, a system admin, has access to a service account with higher privileges. He uses that account's credentials to access the restricted data. Interset detects the account misuse as high risk and shares this information with Risk Service. Advanced Authentication locks down this service account.

1.3 Scenario: Accidental Insider Threats Detection

Amrita, an HR professional, forgets to lock her computer. This allows a colleague to probe the sensitive data. Interset detects this account compromise with medium risk and results in the Advanced Authentication multi-factor authentication requirement the next day. This stops the colleague from the subsequent attempt to steal the data.

1.4 Scenario: Compromised Network, Host, or Device Detection

Interset detects an unusual number of access requests from similar IPs or similar devices. The overall risk is high as the organization might be under a stealth attack or at risk of a DDOS attack.

Interset detects an increase in the number of identities. It also detects an unusual number of access requests from these identities. Interset increases the overall risk of this B2C organization as the attackers might be creating an excessive number of identities by using social login. Attackers could also launch a DDOS attack with these valid identities.

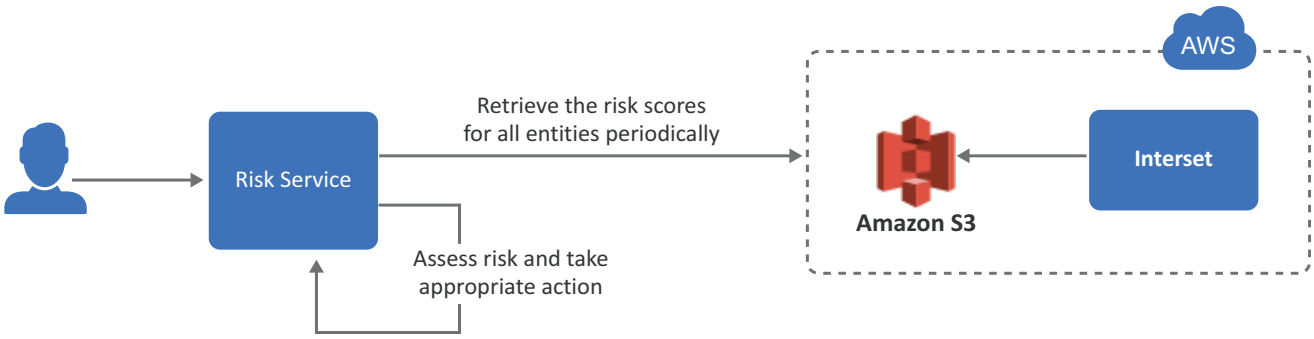
Thomas, an engineer, has malware running on his laptop. This malware uses his account to snoop the resources on the network. Interset detects the infected host by considering unusual access patterns and endpoint threat patterns. Interset determines the user as high risk. Advanced Authentication blocks his access.

2 How It Works

Risk Service periodically fetches risk scores for all entities from Interset. When a user tries to access a protected resource, Risk Service uses the risk score for assessing the risk.

While configuring Interset, you need to configure it to receive data from various applications used in your organization. Interset analyzes the behavior of entities and users using this data.

The following diagram illustrates how this integration works:



1. A user tries to log in to a protected resource.
2. Risk Service checks the behavioral risk score for this user in the risk score cache.

   Risk Service keeps retrieving the latest behavioral risk scores for all entities at a regular interval and updates the cache.
3. Risk Service assesses the score and takes appropriate action.

3 Prerequisites for the Integration

- ❒ An ArcSight Intelligence *(formerly Interset)* account on AWS is available. For more information, see ArcSight Intelligence (https://www.microfocus.com/en-us/products/arcsight-intelligence/overview).
- ❒ Risk Service 2.0 with Advanced Authentication 6.3.x or later (on-premises or on cloud) is installed and configured

Or,

Risk Service 2.0 with Advanced Authentication SaaS is subscribed

- ❒ AWS S3 URL to access Interest is available.
- ❒ AWS region name is available.
- ❒ AWS access key ID and secret access key required to access the AWS S3 URL are available.

4 Integrating Risk Service with Interset

To integrate Risk Service with Interset, perform the following actions:

1. Configure Interset in Risk Service
2. Modify the External Parameters Rule
3. Add BehavioralAnalyticsRule to a Risk Policy

Configure Interset in Risk Service

1. Click **Risk Settings** > **Configuration** (⚙) icon > **Behavioral Analytics**.
2. Select **Enable** for **Behavioral Analytics**.
3. Specify the following details under **READ BEHAVIORAL ANALYTICS DATA FROM INTERSET**:

Field	Description
Interset Data URL	The AWS S3 bucket URL from where you want to get the Interset data.
AWS Region	The AWS region where Interset is deployed.
Access Key ID	The AWS access key ID to access the Interset URL.
Secret Access Key	The AWS secret access key to access the Interset URL.
Update every	The interval for syncing the data from Interset. The recommended value is 360 minutes (sync four times a day).

NOTE: To prevent disruption of service, ensure that Access Key ID and Secret Access Key specified here are up to date when these are rotated as per AWS guidelines.

4. Click **Save**.
5. Continue with "Modify the External Parameters Rule" on page 4.

Modify the External Parameters Rule

When you configure **Behavioral Analytics**, Risk Service creates an `External Parameters` rule automatically with the appropriate values. The name of the rule is **BehavioralAnalyticsRule**. You can modify this rule if required.

1. Click **Risk Settings** > **Risk Rules** (☰) icon.
2. Click **BehavioralAnalyticsRule**.

This rule is configured with the default behavior to consider any user with Interset score less than 50 as a low-risk user. You can modify this rule to change how the score from Interset is interpreted. You can modify **Negate Result** and the value for the score (the default value for the score condition is < 50). Do not modify any other field.

Field	Details
Negate Result	Select this option to reverse the result of the rule evaluation.
Parameters Set 1	Modify the value for the score parameter, if required.

Add BehavioralAnalyticsRule to a Risk Policy

You can add `BehavioralAnalyticsRule` to an existing risk policy or you can create a new policy and add it.

1. To add it to an existing policy:
   - **1a** On the **Risk Settings** page, click the policy to which you want to add this rule.
   - **1b** Under **Rule Evaluation Order**, click **Add Rule** > **Add Existing Rule**.
   - **1c** Select `BehavioralAnalyticsRule`.
2. To add it to a new policy:
   - **2a** On the **Risk Settings** page, click the **Create a Risk Policy** icon.
   - **2b** Under **Rule Evaluation Order**, click **Add Rule** > **Add Existing Rule**.
   - **2c** Select `BehavioralAnalyticsRule`.
3. Configure a chain using this risk policy and configure a corresponding event. Using this event, you can implement the behavioral analytics capability for a resource.

   For more information about chains, see Creating a Chain. For information about creating and editing an event, see Configuring Events.