RSA NetWitness Detect AI
Identify Anomalies Early, Resolve Threats Faster
Advanced analytics and threat detection with the power and scale of the cloud

It All Starts with Data
Before NetWitness Detect AI leverages network, endpoint, and log data captured by RSA NetWitness Platform.

The cloud-based platform scales to process millions of data points, becoming smarter and more accurate as it aggregates more data.

Add Analytics and Machine Learning
Intelligent Peer Grouping
Since user behavior varies based on an individual’s role, responsibilities, location and other factors, RSA NetWitness Detect AI creates peer groups and compares peers to detect deviations. This also leads to more accurate alerts.

For example, if RSA NetWitness Detect AI sees that a user who normally never has a problem authenticating suddenly experiences several failed authentication attempts in a single day, it will look at similar users to see if they’re having the same problem. If they, too, are showing failed authentication attempts, it’s unlikely to signal a cyber threat.

Scalable SaaS Solution
NetWitness Detect AI scales to process billions of events daily and collects hundreds of thousands of organizational entities. Flexible licensing options accommodate the needs of both large enterprises and smaller organizations.

Easy to deploy and administer, with minimal hardware to install and manage. Begins processing data within hours, so you can quickly baseline behavior, start detecting high-risk anomalies, and achieve fast time-to-value.

Automatically and regularly refines its machine learning algorithms to provide high-fidelity threat detection without burdening analysts with extra work.

Innovative Statistical Analysis
NetWitness Detect AI aggregates multiple indicators of suspicious activity, then applies a dynamic statistical risk scoring model. This approach alleviates analysts’ burdensome workloads by producing higher-fidelity alerts triggered only when a risk score exceeds established thresholds.

Intelligent Peer Grouping
Since user behavior varies based on an individual’s role, responsibilities, location and other factors, RSA NetWitness Detect AI creates peer groups and compares peers to detect deviations. This also leads to more accurate alerts.

For example, if RSA NetWitness Detect AI sees that a user who normally never has a problem authenticating suddenly experiences several failed authentication attempts in a single day, it will look at similar users to see if they’re having the same problem. If they, too, are showing failed authentication attempts, it’s unlikely to signal a cyber threat.

Scalable SaaS Solution
NetWitness Detect AI scales to process billions of events daily and collects hundreds of thousands of organizational entities. Flexible licensing options accommodate the needs of both large enterprises and smaller organizations.

Easy to deploy and administer, with minimal hardware to install and manage. Begins processing data within hours, so you can quickly baseline behavior, start detecting high-risk anomalies, and achieve fast time-to-value.

Automatically and regularly refines its machine learning algorithms to provide high-fidelity threat detection without burdening analysts with extra work.

Innovative Statistical Analysis
NetWitness Detect AI aggregates multiple indicators of suspicious activity, then applies a dynamic statistical risk scoring model. This approach alleviates analysts’ burdensome workloads by producing higher-fidelity alerts triggered only when a risk score exceeds established thresholds.

It’s All Started with Data
Before NetWitness Detect AI leverages network, endpoint, and log data captured by RSA NetWitness Platform.

The cloud-based platform scales to process millions of data points, becoming smarter and more accurate as it aggregates more data.

Add Analytics and Machine Learning
Intelligent Peer Grouping
Since user behavior varies based on an individual’s role, responsibilities, location and other factors, RSA NetWitness Detect AI creates peer groups and compares peers to detect deviations. This also leads to more accurate alerts.

For example, if RSA NetWitness Detect AI sees that a user who normally never has a problem authenticating suddenly experiences several failed authentication attempts in a single day, it will look at similar users to see if they’re having the same problem. If they, too, are showing failed authentication attempts, it’s unlikely to signal a cyber threat.

Scalable SaaS Solution
NetWitness Detect AI scales to process billions of events daily and collects hundreds of thousands of organizational entities. Flexible licensing options accommodate the needs of both large enterprises and smaller organizations.

Easy to deploy and administer, with minimal hardware to install and manage. Begins processing data within hours, so you can quickly baseline behavior, start detecting high-risk anomalies, and achieve fast time-to-value.

Automatically and regularly refines its machine learning algorithms to provide high-fidelity threat detection without burdening analysts with extra work.

Innovative Statistical Analysis
NetWitness Detect AI aggregates multiple indicators of suspicious activity, then applies a dynamic statistical risk scoring model. This approach alleviates analysts’ burdensome workloads by producing higher-fidelity alerts triggered only when a risk score exceeds established thresholds.

Intelligent Peer Grouping
Since user behavior varies based on an individual’s role, responsibilities, location and other factors, RSA NetWitness Detect AI creates peer groups and compares peers to detect deviations. This also leads to more accurate alerts.

For example, if RSA NetWitness Detect AI sees that a user who normally never has a problem authenticating suddenly experiences several failed authentication attempts in a single day, it will look at similar users to see if they’re having the same problem. If they, too, are showing failed authentication attempts, it’s unlikely to signal a cyber threat.

Scalable SaaS Solution
NetWitness Detect AI scales to process billions of events daily and collects hundreds of thousands of organizational entities. Flexible licensing options accommodate the needs of both large enterprises and smaller organizations.

Easy to deploy and administer, with minimal hardware to install and manage. Begins processing data within hours, so you can quickly baseline behavior, start detecting high-risk anomalies, and achieve fast time-to-value.

Automatically and regularly refines its machine learning algorithms to provide high-fidelity threat detection without burdening analysts with extra work.

Innovative Statistical Analysis
NetWitness Detect AI aggregates multiple indicators of suspicious activity, then applies a dynamic statistical risk scoring model. This approach alleviates analysts’ burdensome workloads by producing higher-fidelity alerts triggered only when a risk score exceeds established thresholds.

Intelligent Peer Grouping
Since user behavior varies based on an individual’s role, responsibilities, location and other factors, RSA NetWitness Detect AI creates peer groups and compares peers to detect deviations. This also leads to more accurate alerts.

For example, if RSA NetWitness Detect AI sees that a user who normally never has a problem authenticating suddenly experiences several failed authentication attempts in a single day, it will look at similar users to see if they’re having the same problem. If they, too, are showing failed authentication attempts, it’s unlikely to signal a cyber threat.

Scalable SaaS Solution
NetWitness Detect AI scales to process billions of events daily and collects hundreds of thousands of organizational entities. Flexible licensing options accommodate the needs of both large enterprises and smaller organizations.

Easy to deploy and administer, with minimal hardware to install and manage. Begins processing data within hours, so you can quickly baseline behavior, start detecting high-risk anomalies, and achieve fast time-to-value.

Automatically and regularly refines its machine learning algorithms to provide high-fidelity threat detection without burdening analysts with extra work.