FORCEPOINT
POWERED BY Raytheon

Solution Brief

Incident Risk Ranking

THE ANALYTICS ENGINE BEHIND FORCEPOINT'S RISK-BASED DATA MODELING THAT CONTROLS AND SECURES CRITICAL DATA

Forcepoint DLP and Forcepoint DLP Endpoint give you unrivaled visibility and control over your critical data regardless of where it resides — in the Cloud, on the road or in the office. Forcepoint's data loss prevention (DLP) technologies lead the industry in protecting your critical data. Plus, they have the flexibility to protect your employees using Windows, Mac, or Linux endpoint devices. Forcepoint DLP and Forcepoint DLP Endpoint were the industry's first to include DLP Mac OS agent, PreciseID Fingerprinting and behavioral analytics.

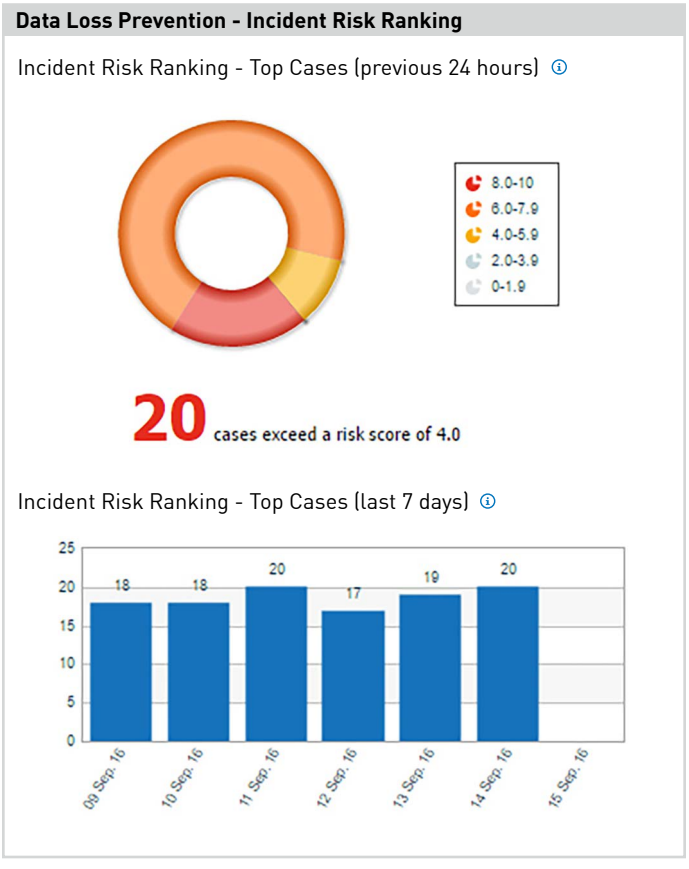
HOW IT WORKS

The Analytics Engine is the brain behind the risk-based data modeling. It's designed to deliver a holistic view of risk across multiple data loss channels and from all endpoint, gateway and cloud components. It can be deployed on virtual or physical hardware and can even work on a single data set, such as endpoint or email incidents. The Analytics Engine is included in all Forcepoint DLP licenses free of charge.

Now, Forcepoint advanced security analytic capabilities include **Incident Risk Ranking (IRR)**, a new feature of Forcepoint DLP version 8.2.5 that automatically groups incidents, giving them a risk score and ranking them according to those that pose the greatest risk.

Incident Risk Ranking uses statistical data modeling and behavioral baselines to automatically identify and group incidents into cases. (See Figure 1.) Each case is given a risk score 0-10, with 10 posing the highest risk to your organization.

Figure 1. Top Incident Cases for the past 24 hours and 7 days:



Forcepoint DLP version 8.2.5 also includes a new IRR dashboard that allows you to:

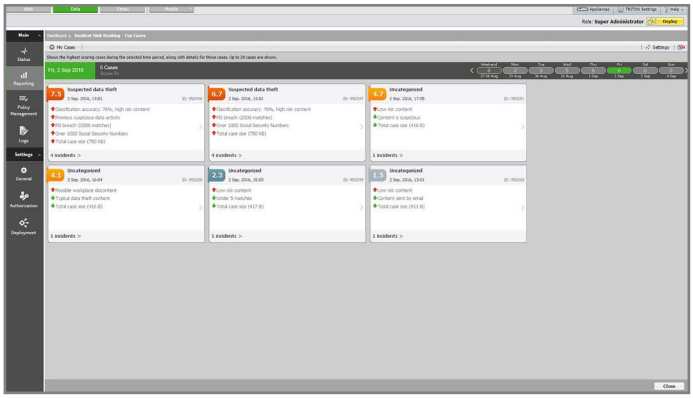
- See top clusters of incidents for the previous 24 hours (midnight to midnight) and 7 days.
- Quickly identify incidents from statistical data modeling and behavioral baselining for immediate remediation action.
- Instantly prioritize cases from high-to-low risk levels — with customizable risk score thresholds — delivered in an Incident Risk Ranking report stack.
- Know which cases exceed the risk score threshold in the selected time period.

The IRR daily report automatically stack ranks cases according to their score, enabling you to take remediation action and prevent future risks. (See Figure 2).

In the IRR report, each case is described by:

- The risk score of 0-10
- Classification of the incident
- Reason(s) the case is included in the report, with red up arrows indicating an incident raises the risk score and green down arrows indicating it lowers the risk score
- Unique case ID number
- The date and time of the last incident added to the case
- Whether the source for this case was a "user" or a "machine"
- The number of incidents in the case

Figure 2. Incident Risk Ranking Daily Report:



Forcepoint DLP and Forcepoint DLP Endpoint now go a step further in protecting your critical data wherever it lives with **Incident Risk Ranking*** a powerful new feature included in Forcepoint DLP version 8.2.5 at no additional cost.

*There is a five step process involved in building the Incident Risk Ranking report:

1. Related incidents form an activity chain of events and are then automatically grouped into cases.
2. A set of Bayesian data models classifies the activity — e.g., data theft — a broken business process or personal communication.
3. The system maintains both organizational and individual behavioral baselines to detect anomalous activity within each data set.
4. A risk score is calculated for each case by combining the results of the data models with the behavioral baseline analysis.
5. The results are formatted and presented to the security operations team in the IRR report.