Risk-Adaptive Protection Overview

Forcepoint

Table of Contents

02 Introduction
Overview
Analyst Efficiency
Risk-Adaptive Policy

03 Forcepoint RAP Architecture
Solution Architecture
Endpoint Integration Architecture

06 Forcepoint Autopilot & IOBs
Activity Monitoring
IOBs
Anomaly Detection

10 Forcepoint Risk Calculations
Risk Calculation
Analyst Efficiency
Risk-Adaptive Policy Enforcement

13 Forcepoint Solution Overview

Introduction

Risk-Adaptive Protection (RAP) is an intregal part of the Forcepoint Data Loss Prevention (DLP) solution that is designed to alert organizations of risky behavior, so they can protect critical data and reduce the risk associated with insiders. The solution collects user behavior and Forcepoint DLP incidents then computes the user's risk using Forcepoint's Indicator of Behavior (IOB) analytic models. This risk score is actively communicated to DLP to automate policy enforcement based on the risk level.

The following sections detail the key functions of RAP:

Architecture
Overview of the end-to-end service and the endpoint integration.

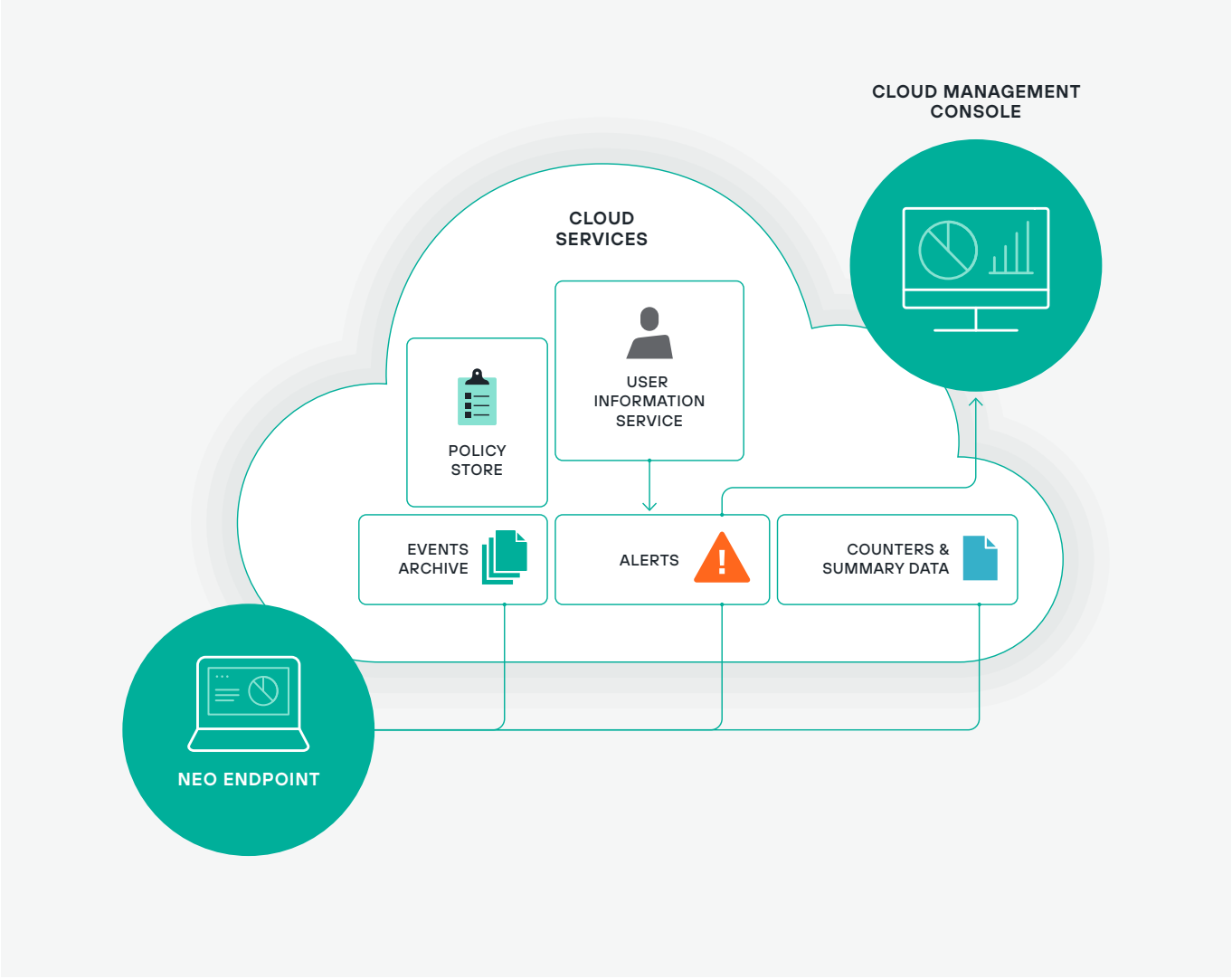
Autopilot
Outlines the preconfigured activity monitoring rules and trailblazing IOBs.

Risk Calculation
Details Forcepoint's forward-thinking, risk-based approach.

Forcepoint RAP Architecture

Solution Architecture

The Risk-Adaptive Protection solution operates within both the endpoint and cloud, which balances immediate detection and enforcement capabilities with scalability.

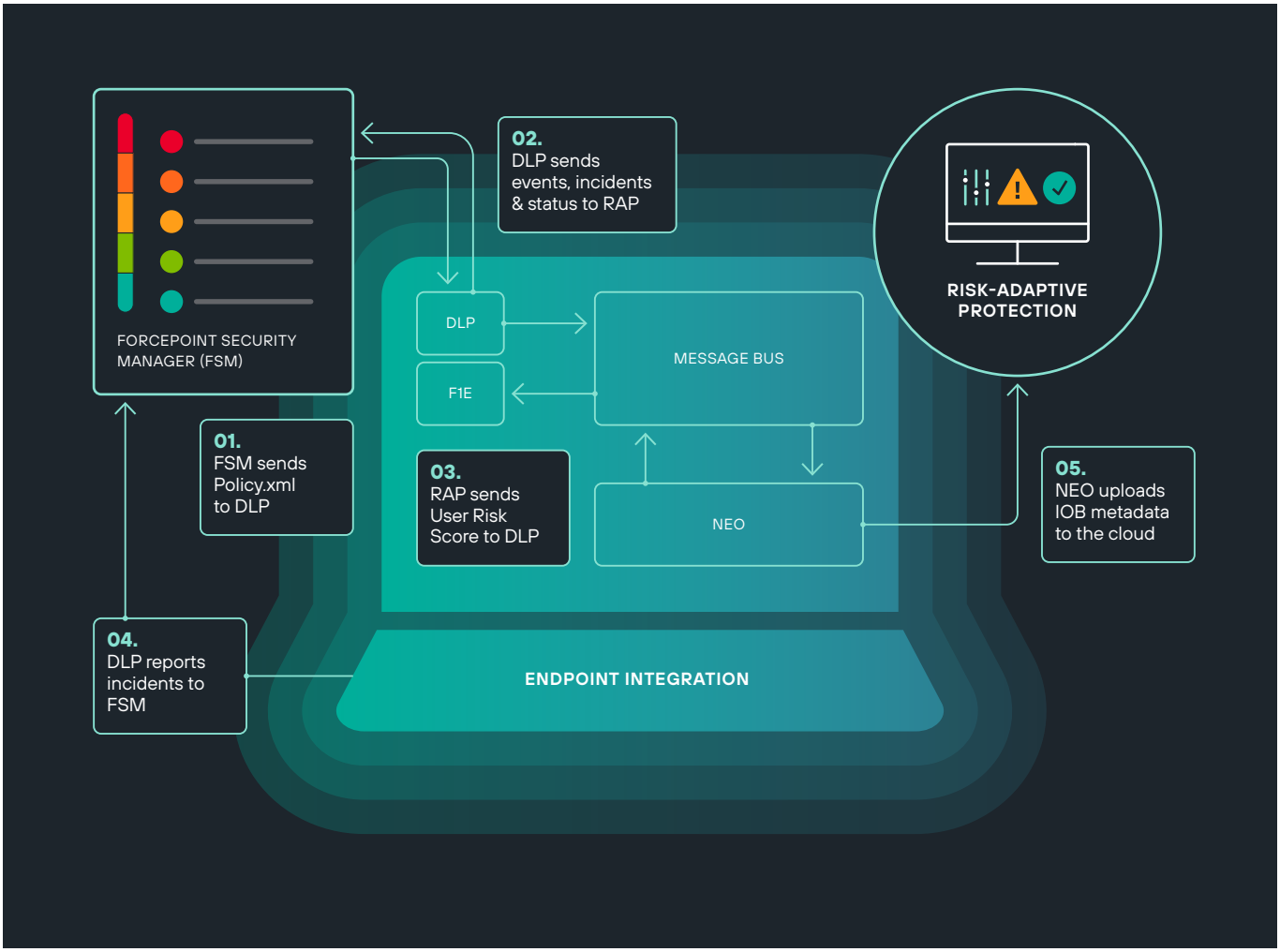


RAP's core operations take place within three distinct areas:

- → **Neo Endpoint** — At the endpoint level, activity data is collected, organized, and then analyzed for the purpose of risk score calculation.
- → **RAP Cloud** — When risky behavior is identified at the endpoint, the associated alerts and events are sent to native cloud services to support analyst investigations.
- → **Cloud Management Console** — Purposefully designed to optimize analyst efficiency and capacity, the console displays users prioritized by order of highest risk score.

Endpoint Integration Architecture

RAP is a solution developed by Forcepoint which replaces broad static policies with personalized and automated data security.



Endpoint integration consists of both the Neo (RAP) and F1EV1 (DLP) agents on a single endpoint. In this mode, DLP policies are created on the Forcepoint Security Manager (FSM) and sent to the agent in order to set the threshold for automated enforcement.

The Neo Message Bus is leveraged to facilitate communication between the two agents. It is here where DLP activity is sent to Neo in order to support risk calculation, while the risk score is sent to DLP for the purpose of automating policy enforcement.

As part of this integration, the following message types are sent:

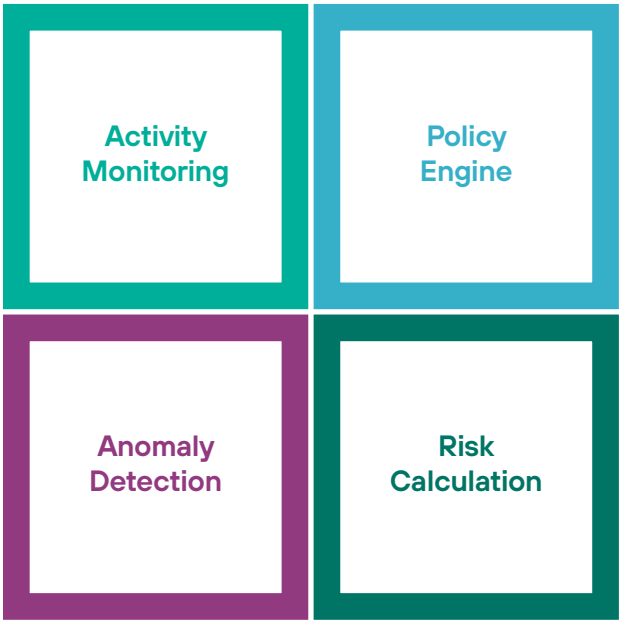
- → **Activity** — DLP events and incidents are sent to RAP in the the form of activity.
- → **Risk Score** — 0 to 100 score calculated through a combination of DLP and RAP events for the purpose of streamlining analyst investigations.
- → **Risk Level** — Adapted from risk scores, Risk Levels are thresholds between 1 and 5 used to dictate risk-adaptive DLP policies.

Forcepoint Autopilot & IOBs

Autopilot

Autopilot (AP) is a pre-configured risk assessment that continuously collects, enriches, and correlates events in order to detect suspect behavior. With zero need for configuration, AP applies the necessary context to events in order to detect Indicators of Behaviors and generate alerts that elevate the user's risk score.

Autopilot consists of:



Activity Monitoring

This stage consists of gathering raw activity from various channels and normalizing the data into events that adhere to a standardized infomation model. Once collated, the events are ready to enter the risk analysis process.

Autopilot enables instant activity monitoring configured across the following channels:

- Printing
- Web Traffic
- Removable Storage
- Network Share
- Email
- Screen Capture*
- Clipboard*
- Cloud Desktop*
- Local Hard Drive*
- Windows Event Log*

* WINDOWS ONLY

Policy Engine

Once the data is parsed and aggregated, it is run against the policy engine, which detects indicators of behavior and triggers alerts.

Anomaly Detection

Counters are sets of event data that establish an individual's baseline activity for specific applications and actions. The events are analyzed with the anomaly detection engine to identify outlier behaviors, which also produce alerts.

Risk Calculation

When an alert is triggered, it carries a specific associated risk impact, longevity factor, and reduction function that escalate the user's risk score based on the severity of the behavior.

Indicators of Behavior

Indicators of Compromise (IOC) are the forensic artifacts that indicate intrusion with a high degree of confidence. In an effort to shift modern security strategy to the human-centric approach, Forcepoint X-Labs has pioneered the Indicator of Behavior (IOB), which is a forensic artifact used to indicate behavior or intent with a high degree of confidence.

IOB 711 - SCREEN CAPTURE

User stockpiles data from business applications through screen capture

IOB 511 - PERSONAL EMAIL

User exfiltrates business files to a personal email address

IOB 265 - PERSONAL PRINTER

Printing documents locally on a personal printer

As Autopilot collects and correlates events, they are analyzed in the policy engine. When an event triggers an alert, an IOB is matched to the behavior.

RAP leverages the IOB Catalog to characterize observed behaviors in order to build a narrative explaining the intent behind the user's actions. While an individual IOB doesn't necessarily equate to malicious intent, the combination of multiple IOBs does indicate high-risk behavior is occurring.

Anomaly Detection

There are IOBs tied to specific variations of anomalous behavior. The example below illustrates how anomalies, and their associated impacts are identified.

IOB 267 - ANOMALOUS PERSONAL CLOUD UPLOAD

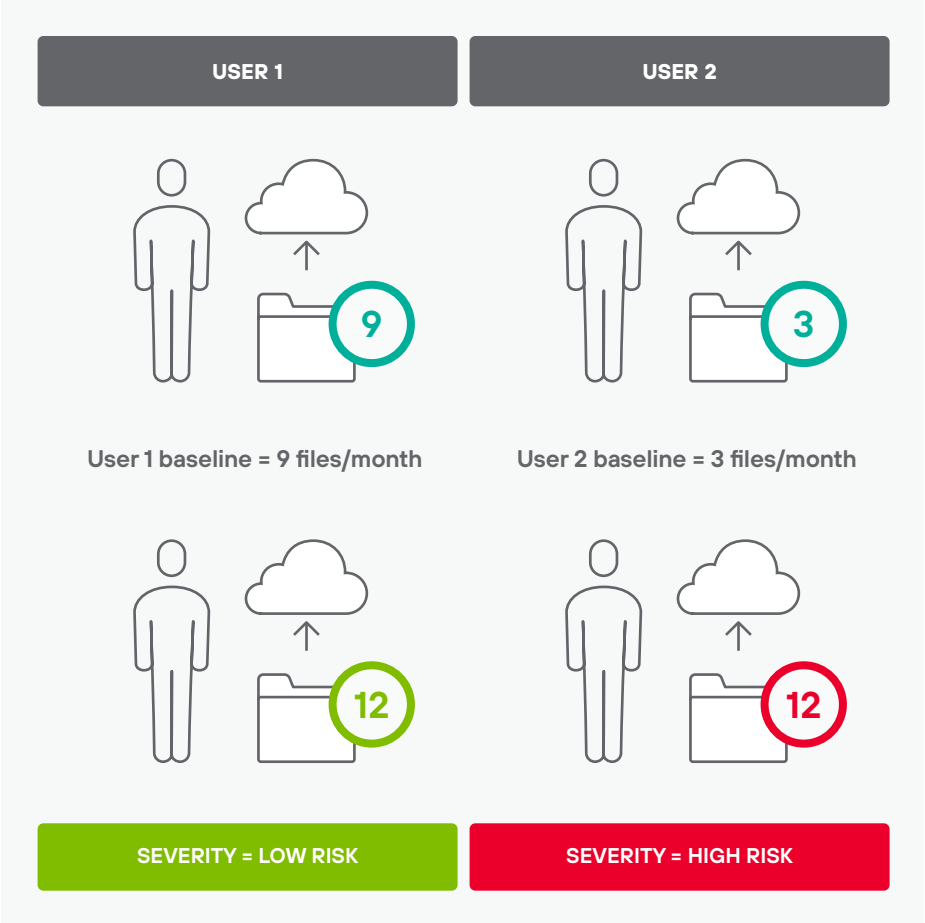
Volume of uploads to personal cloud anomalous compared to history of self.

- → **User uploaded 140MB to personal cloud storage**
- → **Typical personal cloud upload size is 4MB.**
- → **= High Severity Anomaly**

Anomaly Detection

- Distance from individual user baseline determines severity
- Mean calculated over 20 days
- Determined by file count or size

Two separate users upload 12 files to personal cloud storage:



Forcepoint Risk Calculation

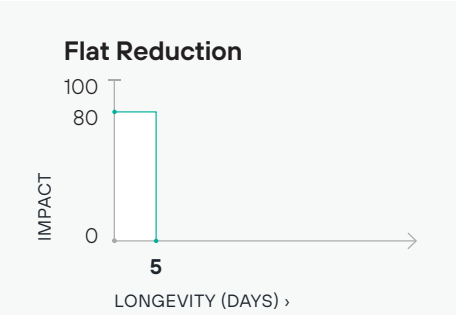
Risk Calculation

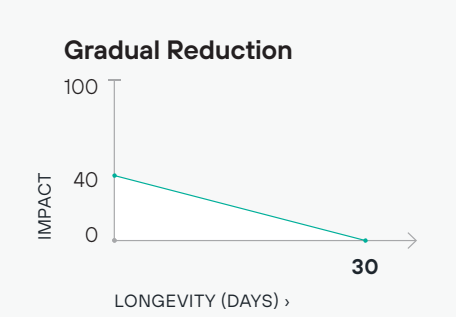
Traditional security tools generate a myriad of logs that rely on analysts to connect disparate events to discern whether the incident is worth further investigation or a false positive. The introduction of risk scoring eases the load on analysts as pre-defined expert-logic provides them with immediate prioritized conclusions.

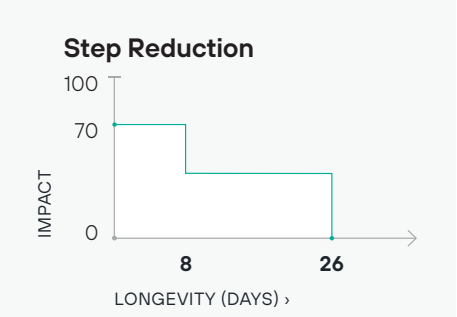
Calculation of user risk is the cornerstone of Forcepoint's RAP platform. As each alert is triggered, the risk is impacted based on the severity, resulting in a score between 0-100. This risk score is the sum of multiple correlated indicators of behavior which enables an exponential uplift in analyst efficiency and powers risk-adaptive data protection policies.

IOBs are made up of three core parameters that influence risk:

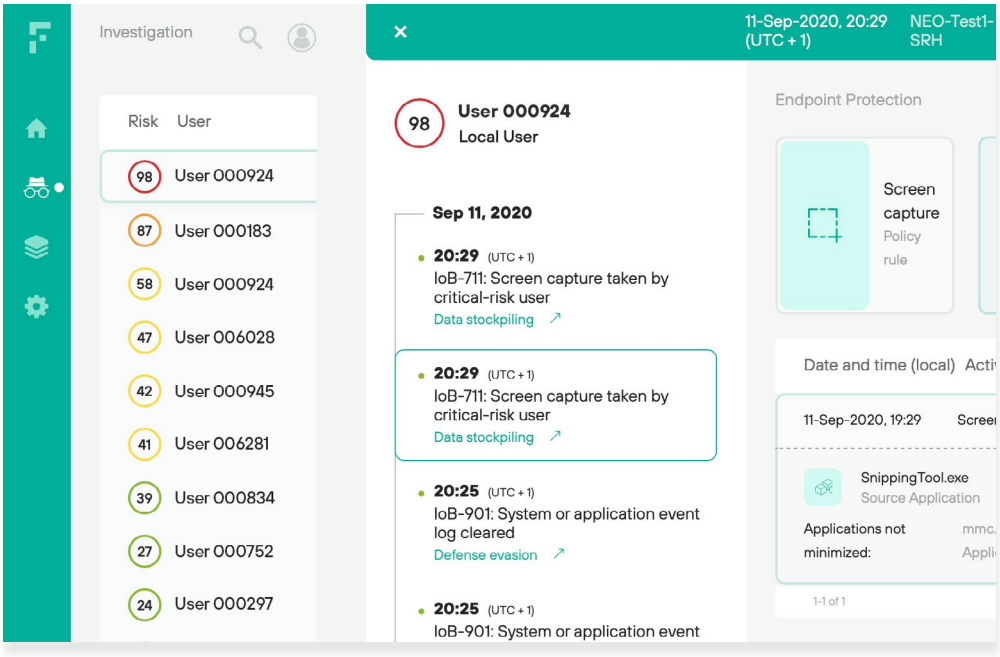
- → **Risk Impact** — The weight associated with an IOB is determined by the type of activity and the severity of the action compared to the user's baseline behavior.
- → **Longevity** — Each IOB carries a unique longevity factor which reflects how long the risk from a specific activity is valid. As time passes, certain IOBs are no longer considered when calculating a user's risk.
- → **Reduction Function** — Defines how the risk impact of an alert degrades over time. Illustrated below, different IOBs decay at different rates, depending on the associated function.





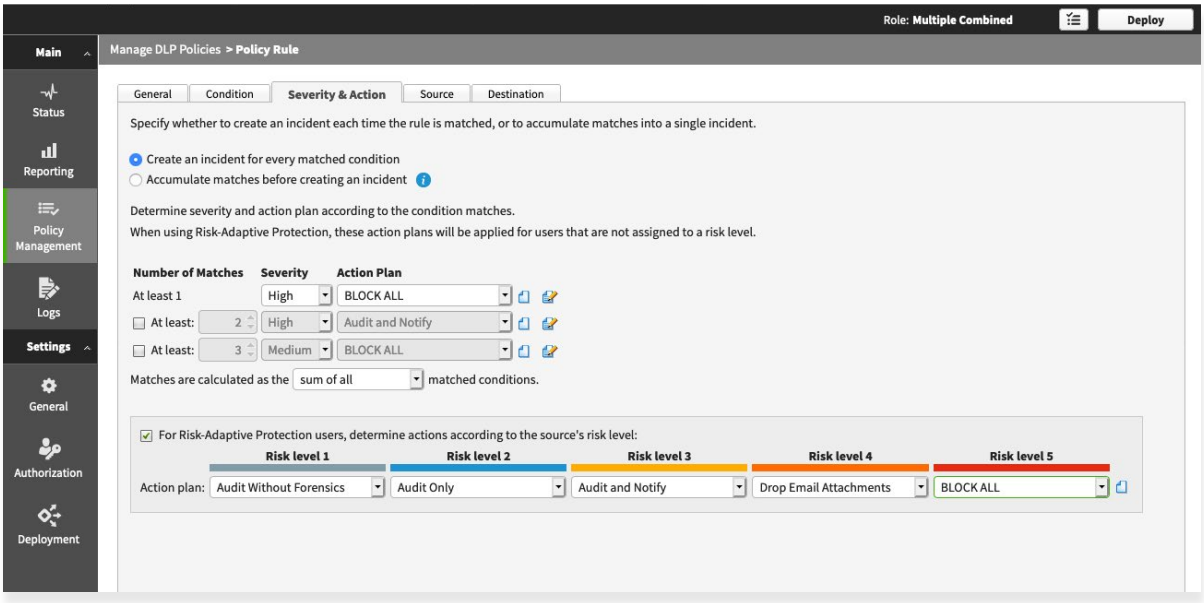


Analyst Efficiency



The risk score optimizes analyst efficiency and capacity through the prioritization of users in order of risk. To aid investigation, metadata is automatically extracted from the local roaming user profile to enrich the alerts.

Risk-Adaptive Policy Enforcement



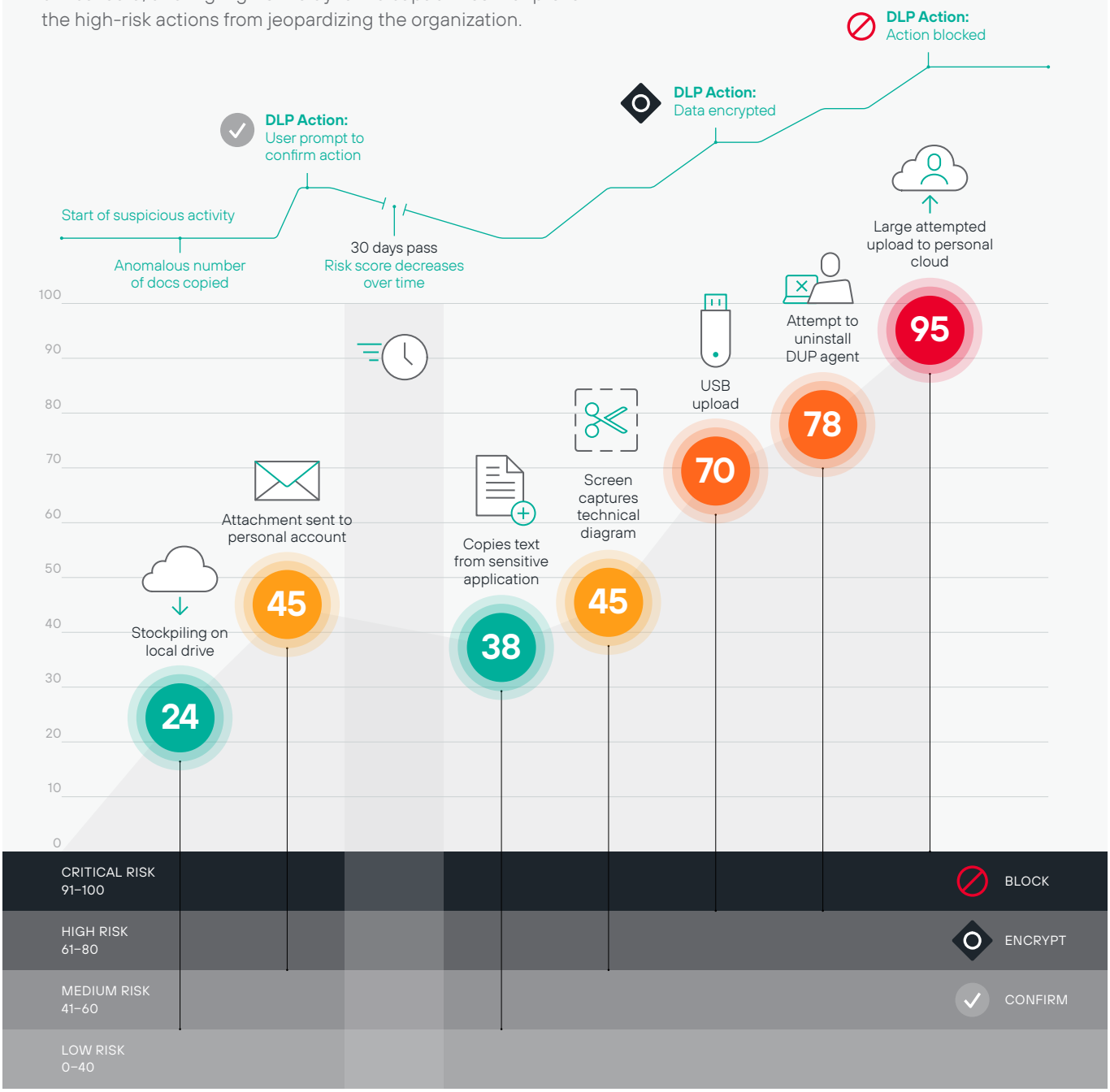
The risk score is also leveraged for risk-adaptive DLP policies. Thresholds are set which allow policies to escalate depending on the individual's risk level. Enforcement options include: Audit, Block, Notify, Confirm Prompt, Encrypt, and Drop Email Attachment. Additional enforcement options can be created for even greater enforcement granularity.

Forcepoint Solution Overview

Solution Overview

This section combines the concepts discussed throughout this document to illustrate RAP's valuable synergies when paired with Forcepoint DLP.

The diagram below depicts a scenario in which a disgruntled employee attempts to evade security controls in order to exfiltrate critical data, and highlights the dynamic capabilities that prevent the high-risk actions from jeopardizing the organization.



Solution Overview

This section is an in-depth review of the above diagram. Each box will explore the user's action, the associated risk score impact, and the risk-adaptive policy that was triggered as a result.

24

IOB 311 - ANOMALOUS NUMBER OF FILES COPIED

User Activity: Suspicious number of files copied from network share to local drive, i.e., Stockpiling.

Explanation: By itself, this activity is not considered risky enough to warrant alerting an analyst. However, this activity raises the user's risk score as this activity has been seen to precede data exfiltration.

DLP Action: None, the risk score is Low Risk (0-40), and this activity does not involve data transmission.

45

IOB 511 - PERSONAL EMAIL WITH ATTACHMENT

User Activity: Attachment sent to personal email address, i.e., Exfiltration.

Explanation: This activity is an example of the gray area of data protection, as it challanges the balance of user productivity and security. Based on the file size involved in this transaction, and the user's previous activity, the risk score is elevated to the Medium Risk level.

DLP Action: As the risk score elevates to Medium Risk (41-60), a confirm action is required by the end user which requires them to acknowledge the risk of their activity.

30 days pass
Risk score declines based on reducing function

38

IOB 611 - COPY TO CLIPBOARD

User Activity: Text copied from sensitive application, i.e., Defense Evasion.

Explanation: This is considered an evasion technique, meant to bypass security controls. This activity has been observed to preceed exfiltration, but could also be legitimate, which results in a slight impact to the risk score.

DLP Action: None, the risk score is maintained at Low Risk (0-40), as this activity does not involve data transmission.

Continued on next page ›

45

IOB 711 - SCREEN CAPTURE

User Activity: User collects data from business applications through screenshots, i.e., Stockpiling.

Explanation: This activity is seen a preparative action taken when the user intends to exfiltrate data. Based on the previous activities, it elevates the score to Medium Risk. Stockpiling has been observed in exfiltration and leaver scenarios.

DLP Action: None, while the risk level does meet the Medium Risk action threshold, it does not involve data transmission.

70

IOB 299 - USB UPLOAD

User Activity: USB upload, i.e., Exfiltration.

Explanation: Similar to the second activity, this activity resides in the gray area. However, based on the user's previous activities, this action is considered possible data exfiltration, which results in the score elevating to High Risk.

DLP Action: As the risk score elevates to High Risk (61-80), a DLP action is taken which encrypts all of the uploaded data, so it can only be accessed on the company device.

78

IOB 280 - TAMPERING WITH RAP AGENT

User Activity: User attempts to uninstall RAP agent, i.e., Defense Evasion.

Explanation: This is an evasion technique, meant to bypass controls by disabling security software. The attempt was unsuccessful due to built in anti-tampering controls. This activity has been observed to precede exfiltration, which impacts an already High Risk score.

DLP Action: None, while the risk level does meet the High Risk action threshold, it does not involve data transmission.

95

IOB 811 - PERSONAL CLOUD UPLOAD

User Activity: Large upload to personal cloud application, i.e., Exfiltration.

Explanation: Based on the user's history, this activity is considered a data exfiltration attempt, which escalates the risk score to Critical. Additionally this user has moved to the top of the analyst's dashboard for immediate investigation.

DLP Action: This activity has pushed the risk score to Critical Risk (81-100), which meets the Block threshold. This attempted data exfiltration is thwarted.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

© 2022 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.
[FP-RISK-ADAPTIVE PROTECTION OVERVIEW-US-EN] 14Apr2022