FORCEPOINT

Solution Brief

Forcepoint Dynamic Data Protection

Prepare for the next level in user and data security with Forcepoint Dynamic Data Protection. Significantly reduce time to discovery, holistic forensic investigations, and alert burdens caused by false positives, allowing you to quickly respond to risk while maintaining optimum business efficiencies.

Digital transformation, cloud, and mobility have driven information technology to an inflection point and security architectures to a breaking point. As a result, organizations struggle to empower their mobile workforce, maintain the right application for the task at hand, and provide proper protection for data as it flows throughout the environment. Traditional approaches to data protection tend to be rigid, limiting enforcement to permit or block only. This leads to practitioners drowning in alarms and alerts. As a result, security organizations struggle to indentify and triage security content that poses the greatest risk, adjust system policies, and remediate risk.

Now, there is a smarter way to safeguard critical and sensitive data, no matter where it resides or is being accessed. By integrating behavior-centric analytics with data protection tools, Forcepoint Dynamic Data Protection allows you to prioritize high-risk activity and automate policies to protect data in near real-time, providing the highest security with the greatest end-user productivity.

Risk-adaptive security driven by analytics

At the forefront of delivering adaptive security, behavior-centric analytics ingests data from traditional security systems and non-traditional data sources, and then combines them for a richer picture of context around the end users within an organization. By fusing data from data loss prevention (DLP) with that of other organizational sources (e.g., HR, travel logs, email, and chat communication), you get a more informed contextual picture of behavior to quickly identify anomalies within that picture.

Using this context, analytics directs enforcement toolsets to adapt policies automatically based on changes in risk levels, providing risk-adaptive security to your organization. Risk-adaptive security automatically responds to risk and adapts policies down to an individual user level—controlling data and access on-premises, on endpoints, and in the cloud.

Advantages of risk-adaptive protection

- Reduced volume of alerts and false positives that need to be triaged
- Enhanced flexibility with granular enforcement controls based on individual user risk levels
- Individualized one-to-one enforcement of policies
- Increased productivity with proactive, dynamic, and automated enforcement

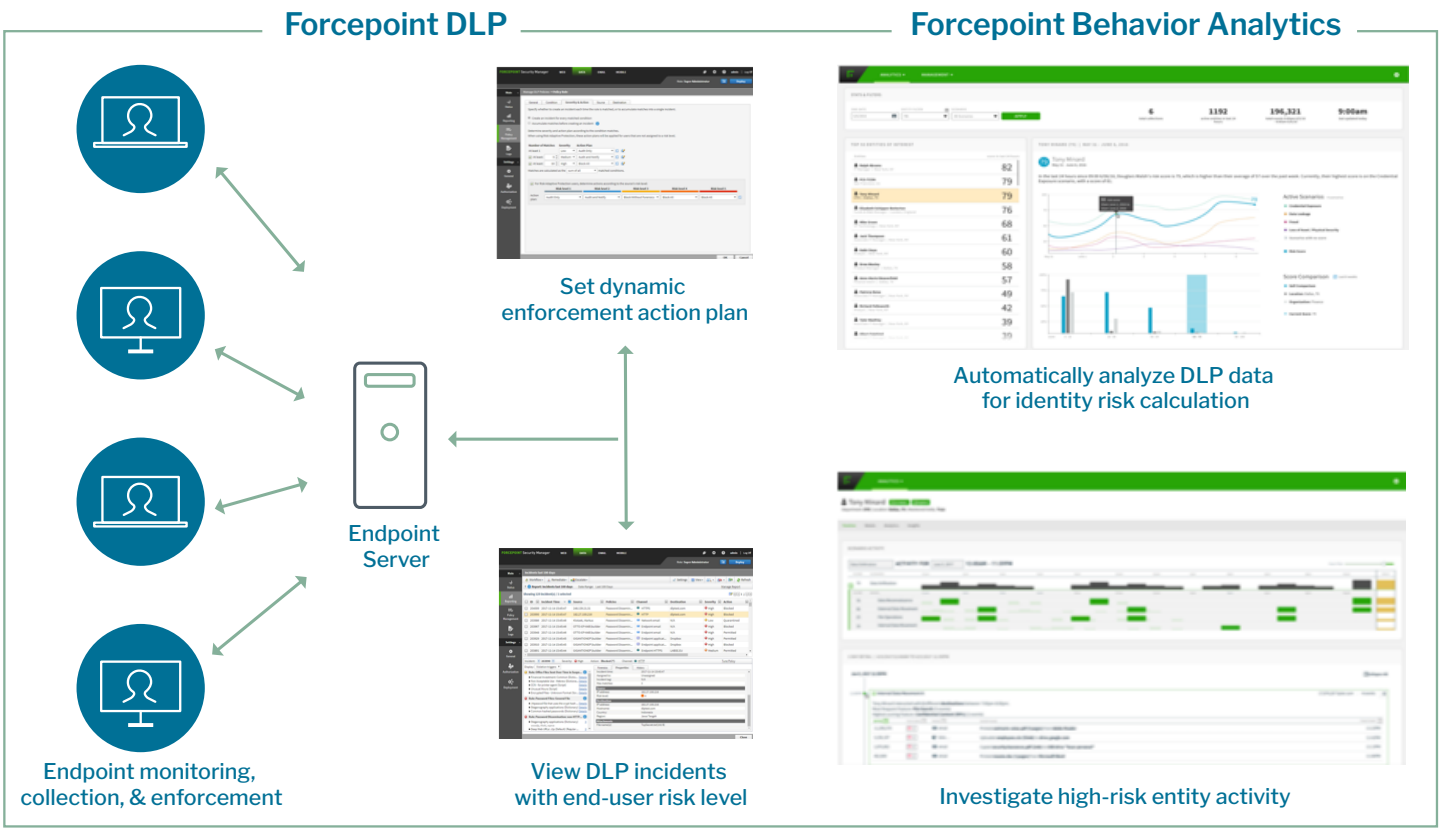
Dynamic Data Protection

Dynamic Data Protection delivers a solution for identifying and investigating entities that pose a potential risk to critical data and assets. It dynamically applies monitoring and enforcement controls to protect assets based on risk level of users and the value of data being accessed.

DLP and Behavioral Analytics combine to enable automated policy enforcement that:

- Profiles high risk user activity based on DLP incidents, data models, and endpoint collector events
- Dynamically allocates a risk score to entities based on user activity and the value of the data they access
- Applies automated controls to user interactions with sensitive data based on their current risk level
- Supports detailed investigation of high-risk user activity

Forcepoint Dynamic Data Protection: How it works



Gain insights with adaptive enforcement to remove the need for human intervention

By using Forcepoint Dynamic Data Protection, organizations can solve the fundamental challenges of traditional DLP deployments and more effectively protect sensitive information, including regulated data sources and PII. This is the first and only solution in the market of its kind, and the only one that can automate policy enforcement to dynamically respond to changes in risk within an organization. With intelligent analytics, unified policy management, and automation at its core, only Forcepoint can provide the end-to-end, behavior-centric security architecture required for the security challenges of today and tomorrow.

forcepoint.com/contact