Forcepoint

Dynamic Data Protection

Dynamic Data Protection

Dynamic Data Protection gives your team the power to identify and investigate the entities that pose a potential risk to critical data and assets. Then, it dynamically applies monitoring and enforcement controls to safeguard assets based on individual risk levels and the value of the data being accessed.

Our solution enables automated policy enforcement that:

› Profiles high-risk activity based on data incidents, data models, and endpoint collector events

› Dynamically allocates individual risk scores based on a person's behavior and the value of the data they access

› Applies automated controls to any interactions with sensitive data based on individual risk level

› Supports detailed investigations into high-risk activity

Prepare for next-level human-centric data security with Forcepoint Dynamic Data Protection. Reduce time to discovery, investigation backlog, and alert burden caused by false positives so you can respond to risk quickly while safeguarding organizational efficiency.

Digital transformation, cloud, and mobility have driven information technology to a crossroads—and security architectures to the breaking point. As a result, organizations struggle to empower mobile workforces, maintain applications, and properly protect data as it flows between environments. The problem? Traditional approaches to data protection tend to be rigid, limiting enforcement to permit or block only. This leads to an endless cycle of alarms and alerts, as security teams struggle to identify, triage, optimize system policies, and remediate true risk. The good news? Now there's a smarter way to safeguard critical and sensitive data, no matter where it lives or travels.

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 and workforce productivity.
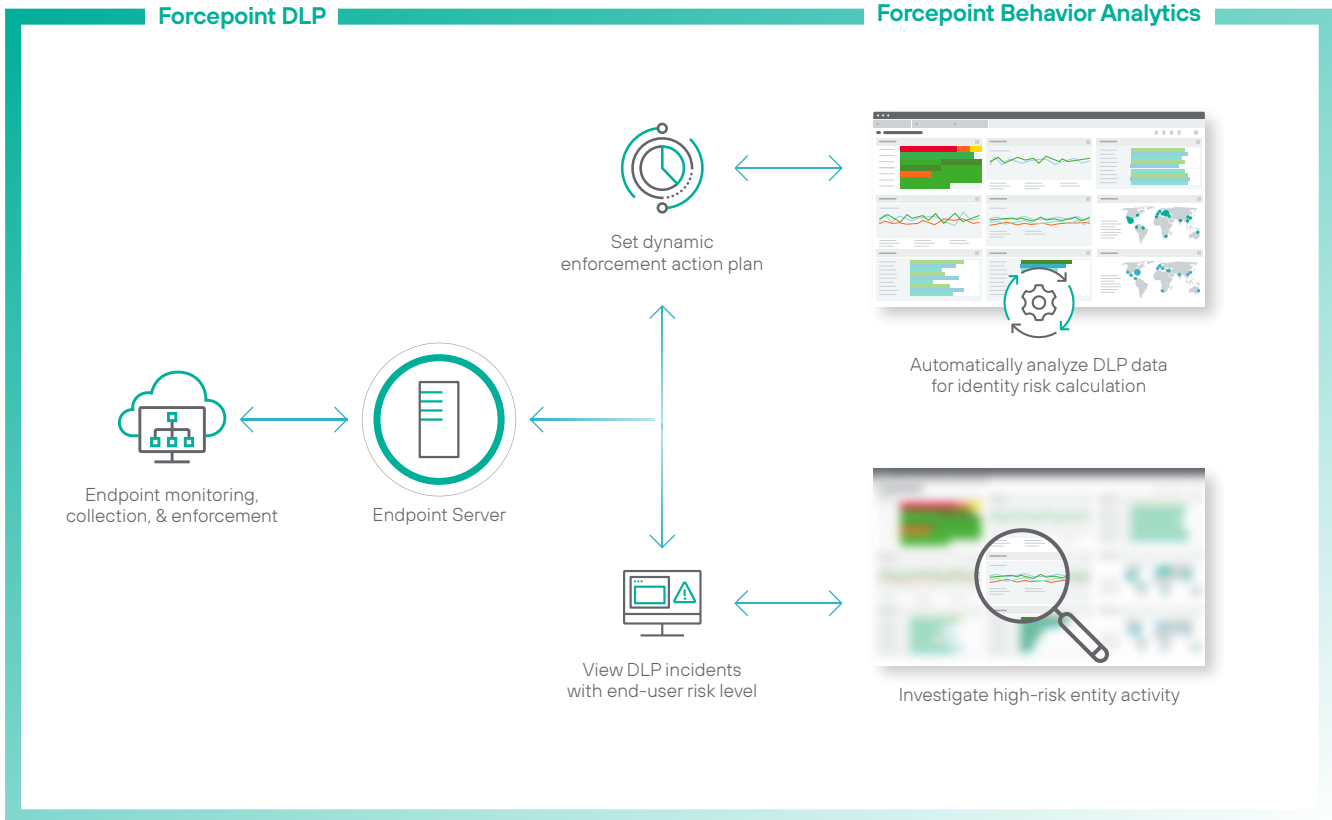
Risk-adaptive security built on analytics

As the foundation for adaptive security, behavior-centric analytics combines user and data activity from monitoring and enforcement points across endpoint network and cloud to comprehensively understand user behavior. With this approach, you'll gain more context into behavior—making it easier to spot anomalies that deviate from the norm. Armed with this context, analytics can trigger enforcement toolsets to adapt policies based on changes in risk levels. This risk-adaptive security automatically responds to risk and optimizes policies down to the human level—controlling data and access on-premises, at endpoints, and in the cloud.

Advantages of risk-adaptive protection

→ Seamless migration from audit-only to selective, risk-based enforcement

→ 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

Forcepoint Dynamic Data Protection: How it works

Forcepoint DLP

Forcepoint Behavior Analytics

Set dynamic enforcement action plan

Automatically analyze DLP data for identity risk calculation

Endpoint monitoring, collection, & enforcement

Endpoint Server

View DLP incidents with end-user risk level

Investigate high-risk entity activity

Gain insight and overcome the need for human intervention

With Forcepoint Dynamic Data Protection, organizations can overcome the fundamental challenges of traditional DLP and more effectively protect sensitive information, including regulated data sources, intellectual property, and personally identifiable information.

Forcepoint DDP is the first and only solution of its kind on the market; 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 organizations need to meet the security challenges of today—and tomorrow.

Ready to learn more about how Dynamic Data Protection can go to work for your business? Connect with an expert at:

forcepoint.com/contact