SOLUTION BRIEF

Dynamic Data Protection for Government

The Next Level in User and Data Security

CHALLENGE

- Government agencies need to manage the increasing risk of protecting sensitive data on their networks and the cloud
- Traditional data loss prevention (DLP) approaches apply stringent data protection policies that frustrate the end-user and lower agencies' operational efficiency

SOLUTION

- Integrates behavior-centric analytics with data protection tools
- Dynamically assigns risk levels based on account behavior
- Adapts security polices to the individual user's risk level as behaviors change

BENEFITS

- Automate policy enforcement to dynamically respond to changes in risk within an agency
- Eliminates the need for a single, static data protection policy set
- Allows for government agencies to achieve maximum data protection while performing at maximum efficiency

Prepare for the next level in user and data security with the integration of the market's most powerful endpoint and user behavioral analytics. Forcepoint Dynamic Data Protection significantly reduces 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. Today, government agencies 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 leave government systems drowning in alarms and alerts, and security organizations are struggling to review and triage security content, adjust system policies, and remediate risk.

Now, there is a smarter way to safeguard sensitive networks and data, no matter where they reside or are accessed.

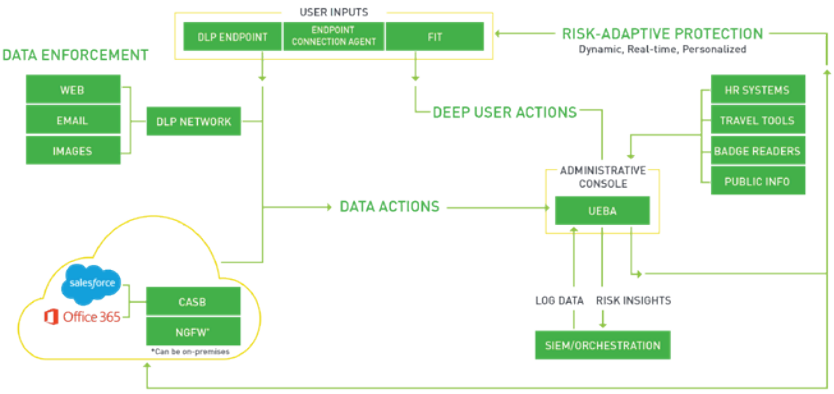
Forcepoint Dynamic Data Protection allows government agencies to identify high-risk activity and automate policies to protect data in near real time, providing the highest security with the greatest end-user productivity.

RISK-ADAPTIVE PROTECTION 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 traditional security systems and output from data loss prevention with that of other organizational sources (e.g., HR, travel logs, email and chat communication), you get a more informed contextual picture on 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 Protection to your organization. Risk-Adaptive Protection 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.

THE ROLE OF ANALYTICS IN HUMAN-CENTRIC SECURITY



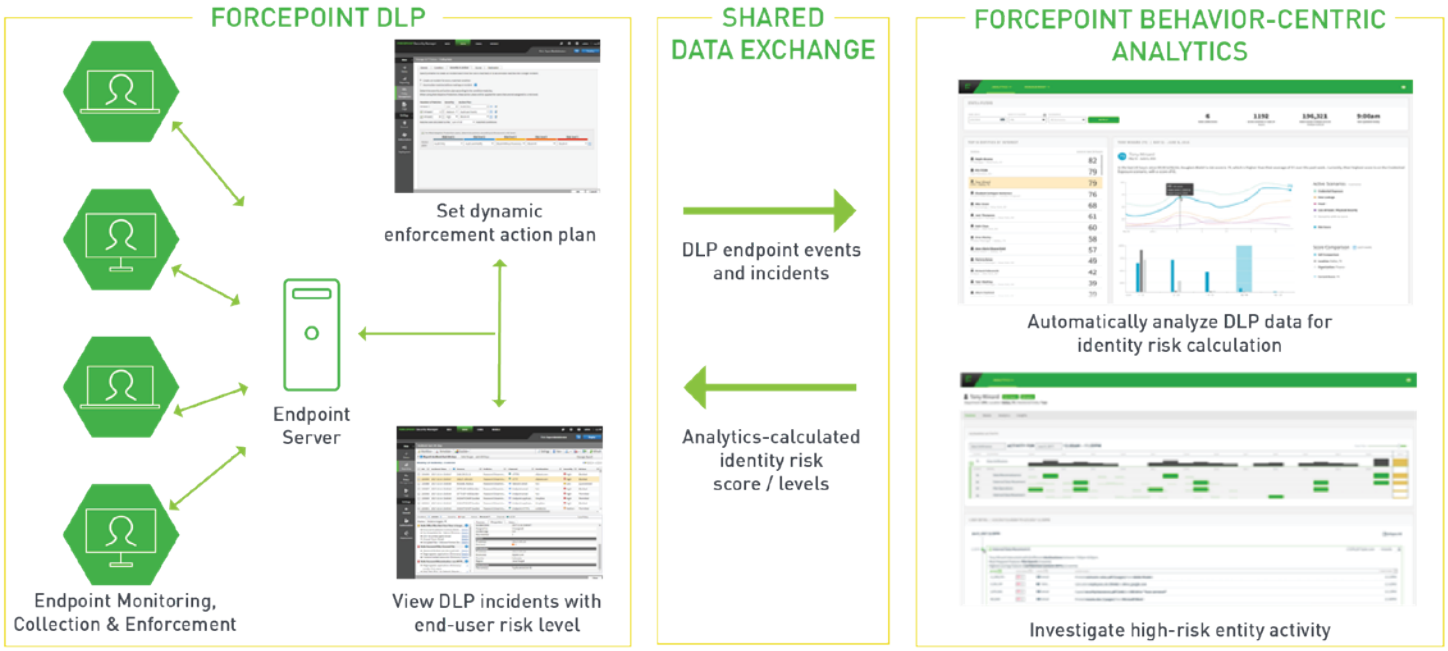
INTRODUCING DYNAMIC DATA PROTECTION

Dynamic Data Protection delivers a system for identifying and investigating entities that post potential risk to critical data and assets. It dynamically applies monitoring and enforcement controls to protect assets based on risk level of actors and the value of data.

DLP and Behavior-centric Analytics combine to create Automated Policy Enforcement:

- Behavior-centric Analytics profiles high risk user activity based on DLP incidents, data models, and endpoint collector events.
- Behavior-centric Analytics dynamically allocates a risk score to entities based on user activity.
- DLP applies automated controls to user interactions with sensitive data based on their current risk level.
- Behavior-Centric Analytics supports detailed investigation of high risk user activity.

DYNAMIC DATA PROTECTION: HOW IT WORKS



DDP orchestrates risk insights with adaptive enforcement to remove the need for human intervention. By using Dynamic Data Protection, government agencies can solve the fundamental challenges of traditional DLP deployments and more effectively protect sensitive information, including regulated data sources and personally identifiable information (PII). **This is first and only solution of its kind in the market, and the only one that can automate policy enforcement to dynamically respond to changes in risk within an agency.** With intelligent analytics, unified policy, and orchestration at its core, only Forcepoint can provide the end-to-end, human-centric security architecture required for the security challenges of today and tomorrow.