solution brief

Dynamic Data Protection for the Department of Energy

The next level in user and data security

Challenge

- Audit reports have cited vulnerabilities in DOE's ability to properly secure its information systems and data
- Legacy data loss prevention applies stringent policies that frustrate users and reduce agency 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

- Eliminates the need for a single static data protection policy set
- Allows DOE 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.

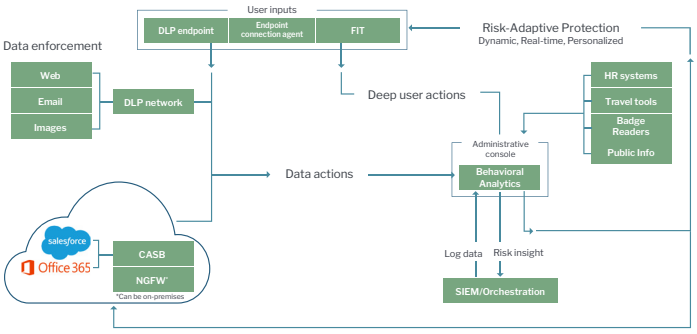
In recent years, the Department of Energy (DOE) has experienced significant intrusions to its networks. As a diverse enterprise comprised of 97 entities spread across 27 states, DOE has unique challenges in protecting its most sensitive data, regardless of where it is located on the network. Additionally, digital transformation, cloud, and mobility have driven information technology to an inflection point and security architectures to a breaking point. Like other government agencies, DOE struggles to empower it's 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 for DOE to safeguard sensitive networks and data, no matter where they reside or are accessed.

Forcepoint Dynamic Data Protection will allow DOE 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 for DOE, driven by analytics

Forcepoint is a key partner to DOE's multi-dimensional cybersecurity strategy, with solutions scaled to support the department's security program. Our risk-adaptive protection solutions integrate best-in-class products with analytics and behavioral profiling, bringing DOE near real-time risk insights and automated remediation to better protect critical data wherever it resides, including Controlled Unclassified Information (CUI) and sensitive data about the nation's power grid, nuclear weapons stockpile, energy labs, and critical infrastructure. 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

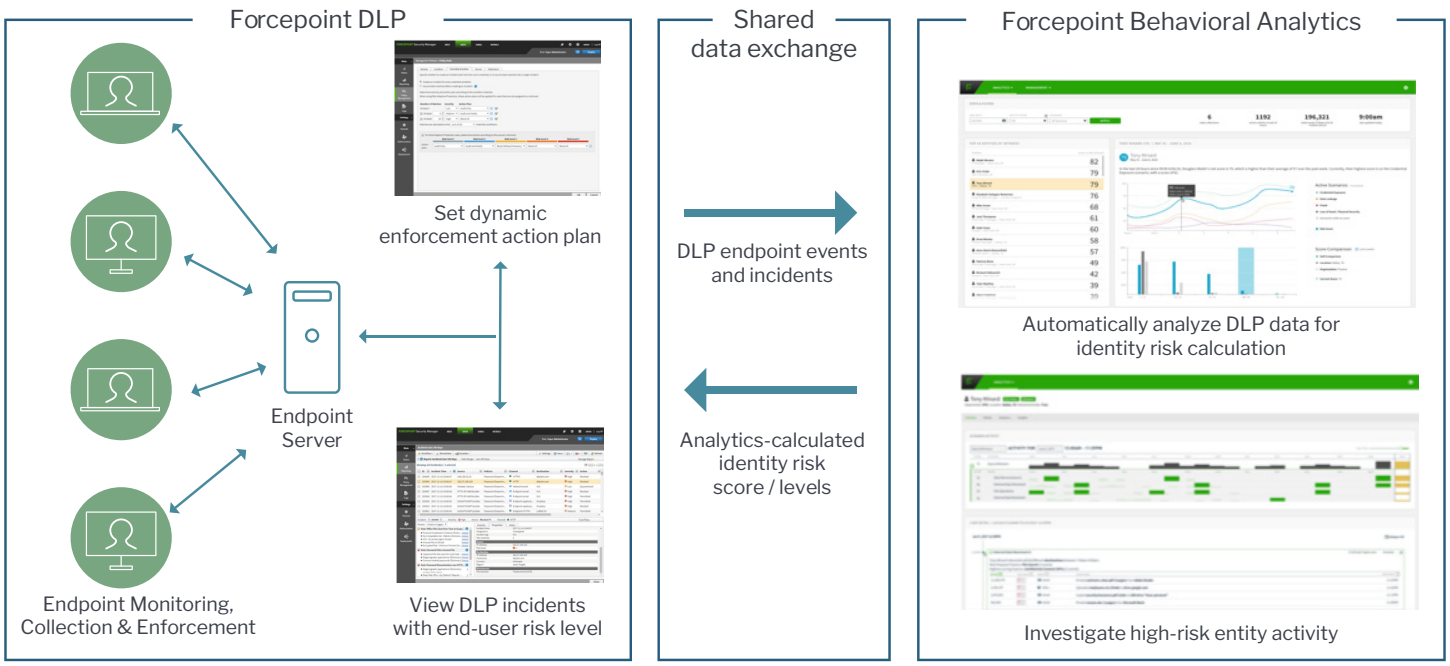
Introducing Dynamic Data Protection

Forcepoint Dynamic Data Protection (DDP) significantly reduces time to discovery, holistic forensic investigations, and alert burdens caused by false positives, allowing DOE to quickly respond to risk while maintaining optimum agency efficiencies.

DLP and behavior analytics combine to create automated policy enforcement:

- Behavior analytics profiles high risk user activity based on DLP incidents, data models, and endpoint collector events.
- Behavior 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 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, DOE 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 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 DOE's security challenges of today and tomorrow.

Contact
DOE@forcepoint.com