FORCEPOINT

Solution Brief

Security Solutions to Protect the DOE's Most Sensitive Information

DOE Challenges

Evolving cyber threats and a growing attack surface have become increasingly complex issues for the United States Department of Energy (DOE), comprising multiple sites, national laboratories, and plants spanning more than 30 states, each with their own unique missions and risk profiles.

Cyber threats impact the success of the department's missions: to maintain the nation's nuclear deterrent, reduce the threat of nuclear proliferation, oversee the nation's energy supply, and manage the science and technology powerhouse of the 17 national laboratories.

Threat actors aim to cause damage, disruption, or unauthorized access to business-essential and mission-critical assets associated with the integrity and safety of personnel, the nation's nuclear weapons, energy infrastructure, and applied scientific research and development.

> We are one team, one fight, each department component must be "all in," fully invested in enterprise-wide cybersecurity collaboration—there can be no weak links.
> — Dan Brouillette, Deputy Secretary, United States Department of Energy

Why Forcepoint for DOE Cybersecurity?

In today's world, government agencies must think differently about their approach to modernizing legacy systems to meet the common goal of transitioning to a resilient cyber posture.

With an operating structure comprised of 107 departmental elements spread across more than 30 states, DOE needs a flexible and dynamic cybersecurity program to protect the critical information with which it is entrusted. Additionally, it needs an innovative partner who understands the complexity of creating efficient and effective, best-in-class security programs across DOE as a whole.

A Risk-adaptive Approach to Cyber Resilience

At Forcepoint, we recognize the need for government agencies to modernize and expand the capabilities of their cybersecurity infrastructure and enable an anywhere, anytime workforce.

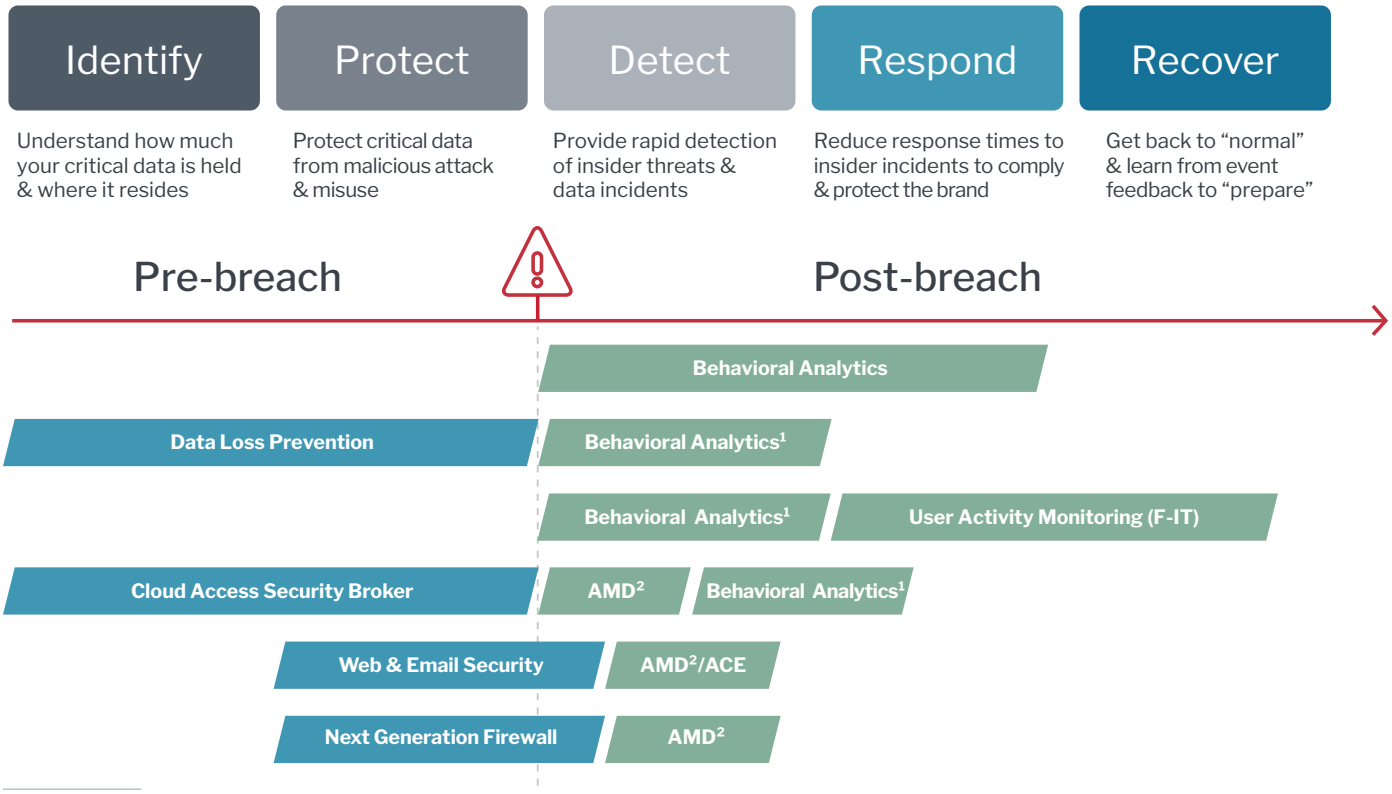
Forcepoint's portfolio comprises solutions to ensure secure data transfers, cloud-based user and application protection, next-generation network protection, data security, and systems visibility. Together, these solutions form the Forcepoint Converged Security Platform, a foundation for delivering seamless connectivity and risk-adaptive protection while eliminating friction created by imprecise and disparate policies.

With behavioral intelligence and analytics at its core, our Converged Security Platform enables security teams to identify risk in near real time and automate remediation to better protect critical data wherever it resides, including Controlled Unclassified Information (CUI) and sensitive data related to the nation's power grid, nuclear weapons stockpile, energy labs, and critical infrastructure. As a result, agencies can eliminate security blind spots and automate policy enforcement to provide a high level of security without frustrating end users or reducing their operational efficiency.

Forcepoint's Converged Security Platform enables security professionals to:

- Capture interactions between users and data everywhere
- Generate a dynamic risk score by understanding context
- Respond automatically to compromised, accidental, and malicious behavior
- Gain efficiencies in investigation and operations through context, such as detailed timelines of events

Forcepoint integrates best-in-class solutions to protect DOE



1 Integrated Behavioral Analytics
2 Includes Advanced Malware Defense Module

Become a cyber-resilient agency with Forcepoint

- **Collection of structured and unstructured data.** Understand where your critical resides and where your vulnerabilities may be. See the full picture, beyond SIEM, with behaviors from the widest variety of data sources.
- **Advanced detection.** Proactively detect high-risk behavior with our security analytics platform, providing unparalleled context to identify and stop malicious, compromised, and negligent users.
- **Threat identification and automated analysis.** Focus on behaviors, not just anomalies, with precise narratives that indicate unwanted behavior.
- **Real-time security and compliance display.** Efficiently pivot from alert to investigation with risk scores and in-depth analytics, all within a single platform.

info.forcepoint.com/doe-cybersecurity | doe@forcepointgov.com