FORCEPOINT

Solution Brief

Department of Health and Human Services

Security solutions to protect HHS' most sensitive information

HHS CHALLENGES

- Cybersecurity incidents and breaches impede HHS's ability to offer essential healthcare programs and services, threaten major elements of our country's critical infrastructure, and compromise patients' health and safety.
- HHS is responsible for protecting massive amounts of data—particularly healthcare data, which is extremely valuable to cyber criminals. Media reports have identified the value of electronic health records (EHRs) to be as much as 10 times that of a credit card number.
- Threats facing HHS come not just from individual actors, but also from organized groups representing or acting on behalf of criminal organizations and foreign nation states with sophisticated tools and resources.

Why Forcepoint for HHS cybersecurity

In today's world, government agencies such as the Department of Health and Human Services (HHS) must think differently about their approach to legacy system modernization in order to meet their goal of transitioning to a cyber-resilient posture. Our goal is to ensure that our solutions help all of our government clients eliminate security blind spots, provide visibility to identify risk early and automate policy enforcement, and deliver the high level of security that agencies need without frustrating end users or lowering the operational efficiency of government. With over 79,000 employees over 11 operation divisions, HHS needs an enterprise-wide cybersecurity program to protect its critical information.

Additionally, initiatives like IT modernization, cloud, and mobility are driving HHS information technology to an inflection point and security architectures to a breaking point. HHS must now have consistent security on-premises and in the cloud.

It is imperative for HHS to identify and prioritize actions for reducing risk and align policy and technological approaches to develop cyber resilience.

A new way forward for HHS

HHS requires a smarter way to safeguard sensitive networks and data, no matter where they are accessed or reside. Forcepoint is a key partner to HHS' Enterprise Risk Management (ERM) approach to cybersecurity, with solutions scaled to support the department's security program. Our risk-adaptive approach integrates best- in-class products with analytics and behavioral profiling, providing HHS with near real-time risk insights into the enterprise's most critical risks. Forcepoint solutions uniquely address HHS' multifaceted challenges, including protecting data on internal systems, overseeing the cybersecurity of data in cloud environments, and ensuring that all end users are adhering to sound cybersecurity principles. With intelligent analytics, unified policy, and orchestration at its core, Forcepoint provides the end-to-end, human-centric security architecture required for the security challenges of today and tomorrow.

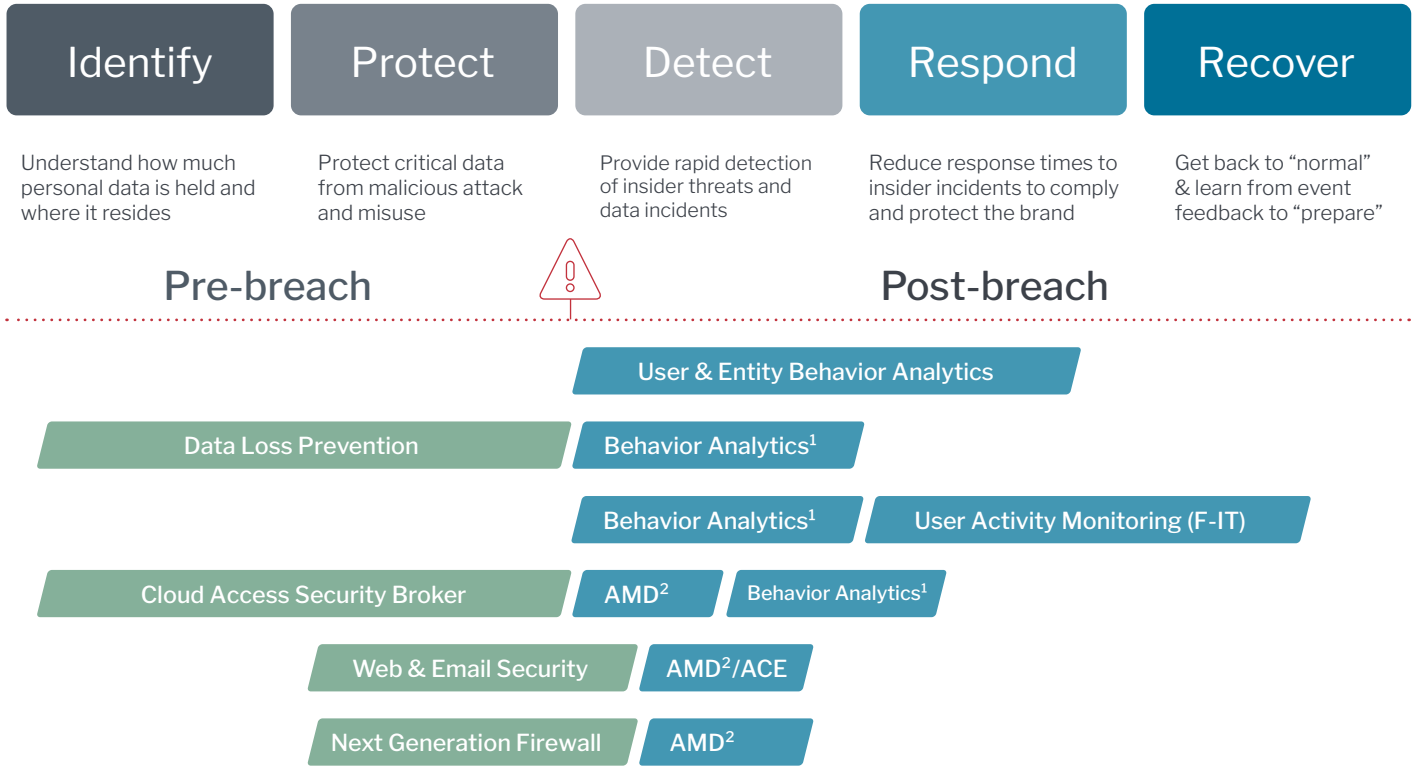
A risk-adaptive approach to cyber resilience

Forcepoint offers solutions scaled to support the modernization of HHS security programs. Forcepoint's human-centric cybersecurity portfolio brings together a broad set of capabilities that protects sensitive networks and data—wherever they are accessed and wherever they reside. Each element is best-in-class and can stand alone or integrate with your existing environment to help solve critical security issues to protect employees, data, and IP. Forcepoint's risk-adaptive security approach enables better decision-making and more efficient security through proactive and context-based technologies, and data-centric, integrated solutions. Our solutions help ensure secure data transfers, cloud-based user and application protection, next-gen network protection, data security, and systems visibility.

Forcepoint's integrated cyber solutions have been accepted into the CDM Approved Product List (APL), and are uniquely designed to take on the cyber challenges of the future and help HHS move towards cyber resiliency.

Forcepoint's Human Point System Enables HHS 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



1 Integrated Behavioral Analytics
2 Includes Advanced Malware Defense Module

Become a cyber resilient agency with Forcepoint

- **Real-time collection:** Understand where your critical data resides and the location of potential vulnerabilities. See the full picture—beyond SIEM—with behaviors from the widest variety of data sources. Only Forcepoint covers structured and unstructured data to leave no detection gaps.
- **Advanced detection and behavior:** Proactively detect high-risk behavior. Our security analytics platform provides unparalleled context to identify and stop malicious, compromised, and negligent users.
- **Threat identification and automated analysis:** Reduce response time. Forcepoint focuses on behaviors, not just anomalies, with precise narratives that indicate unwanted behavior.
- **Real-time security and compliance display:** Quickly and efficiently investigate. Efficiently pivot from alert to investigation with risk scores and in-depth analytics within a single platform.

forcepoint.com/contact