FORCEPOINT Global Governments

EMPOWER • INNOVATE • GROW

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

FORCEPOINT BRINGS MORE THAN 20 YEARS OF EXPERTISE SUPPORTING INTELLIGENCE, DEFENSE AND CIVILIAN AGENCIES AROUND THE WORLD.

Forcepoint's solutions support the unique and complex missions and objectives undertaken by the people who protect national security. Our human-centric approach focuses on the intersection of people, data and networks – the human point. Through our human point system, our integrated solutions and services deliver security that works with and for users, enabling them to effectively and efficiently accomplish their missions.

From intelligence communities to defense departments and civilian agencies, cyber warriors require rapid, accurate and secure ways to interact with technology and data, wherever and however they may access it.

Our human point system and professional services help you solve your greatest security challenges:

- **Forcepoint Cloud Access and Gateway Security** supports government agencies as they move to the Cloud.
- **Forcepoint Cross Domain Solutions** deliver secure information access and transfer within and between extremely sensitive enterprises. Our Cross Domain suite (including Forcepoint Trusted Thin Client and Forcepoint High Speed Guard) operates in some of the most stringent environments in the world, providing a high degree of usability without compromising security.
- **Forcepoint User and Data Security** solves government user activity monitoring and insider threat challenges complemented by Forcepoint DLP and Forcepoint User & Entity Behavior Analytics solutions.
- **Forcepoint Network Security** combines the best of both worlds: Forcepoint NGFW's advanced security and centralized manageability plus the robust protection of the government-required Sidewinder Security Proxies.

Cloud Access and Gateway Security

Forcepoint Email Security

Protect your users against multistage advanced threats that often exploit email to penetrate your IT defenses. Our unrivaled email security applies thousands of real time threat analytics, behavioral sandboxing and other advanced defense technologies to identify targeted attacks. *FedRAMP In Process*

Forcepoint Web Security

A Secure Web Gateway that stops advanced threats from getting in and sensitive data from getting out, whether your users are in the office, working from home or in the field. Our cutting-edge classification engine, global threat intelligence, advanced malware detection and enterprise-class DLP work together for industry-leading security that's easy to deploy in the cloud, on-premises or in a hybrid environment. *FedRAMP In Process*

Forcepoint CASB

A Cloud Access Security Broker that provides the visibility you need to eliminate blind spots and data loss from sanctioned and unsanctioned cloud apps. It enables monitoring and reporting on user activity in real-time with a Risk Summary dashboard. Quickly assess risks to your data and network from shadow IT, dormant (i.e., inactive), orphaned (e.g., former employees) and external (e.g., contractor) cloud apps.

Cross Domain Solutions

Forcepoint Trusted Thin Client

Gives users secure, simultaneous access to information on any number of networks from a single endpoint. Designed for enterprise deployments, Trusted Thin Client provides administrators with centralized management and monitoring, scalability to easily add networks and clients, and the flexibility to enable users in offices, in-theater and in the field.

Forcepoint High Speed Guard

Permits highly complex, bi-directional, automated data transfers between multiple domains, specializing in real-time streaming video. High Speed Guard has demonstrated the fastest bi directional transfer rates of more than nine gigabits per second (Gb/s) on dual processor commodity servers. When implemented as Forcepoint High Speed Guard SP, the solution is adaptable to specific mission needs where strict size, weight, power and cooling (SWaP-C) specifications are required.

Forcepoint Trusted Gateway System

Delivers exceptional built-in manual review and automatic validations, such as virus scanning, file type verification, dirty word search and deep content inspection, enabling safe and simultaneous data movement between networks at different sensitivity levels.

Forcepoint Trusted Print Delivery

Allows users to print from existing applications at different security or sensitivity levels to a single printer located on the high-side network. Because it enables reduced printer hardware at individual security levels, it reduces capital investment, printer inventory, hardware maintenance/supplies and administration.

Forcepoint Trusted Mail System

Enables the policy-enforced exchange of emails and attachments between users on different networks eliminating the need to switch between email systems at multiple levels. Trusted Mail System provides a 'single inbox' that consolidates email and calendar entries residing on multiple networks, at the highest level, making it less likely that important and mission-sensitive email communications are overlooked.

Forcepoint SimShield

A fixed-format data guard with the capability to label, segregate, protect, and exchange data between systems executing at different sensitivity or classification levels. SimShield meets the data format, near real-time performance, and low latency requirements for distributed simulation operations, live training exercises, and test events.

Forcepoint WebShield

Delivers secure web search and browse-down capabilities from high side networks to lower level networks. Users surfing lower level networks can be restricted to specific server and file types as defined by security policies. All requests, responses and transfers go through security controls, such as, dirty word search, virus scan and malicious content checks.

Solutions that support the world's most high consequence missions.

User and Data Security

Forcepoint Insider Threat

Enables safe and effective use of mission-critical technologies by capturing technically observable human behaviors that include policy violations, compliance incidents, or malicious acts that may be warning signs of an impending breach. Our Insider Threat solution provides all the details, insight, and complete context using video replay to immediately assess the severity of the threat, remediate the problem, and build the policies to prevent it from happening in the future.

Forcepoint DLP

A powerful Data Loss Prevention (DLP) tool that helps you secure intellectual property, personally identifying information (PII), and other sensitive data – wherever it resides – on endpoints, in the cloud, or on-premises. Apply behavioral analytics and machine learning to cluster DLP incidents in order of business risk with Incident Risk Ranking (IRR), so your response teams focus on areas of greatest risk. For even greater protection against malicious or careless insiders, combine Forcepoint DLP with Forcepoint Insider Threat.

Forcepoint UEBA

A User and Entity Behavior Analytics tool that enables your security team to proactively monitor for high risk behavior inside the organization. Our security analytics platform provides unparalleled context by fusing structured and unstructured data to identify and stop malicious, compromised and negligent users. We uncover critical problems such as compromised accounts, espionage, intelligence theft, and fraud.

Analytics and Sandboxing

SureView Analytics

Traditional approaches to security analysis require organizations to set up data warehouses and ingest mass data. By contrast, we avoid this issue by using virtual data warehousing technology that accesses data at high speed without ever needing to move or copy it. SureView Analytics also employs federated search, powerful algorithms for automated information discovery and intuitive workflow tools.

Forcepoint AMD

Advanced Malware Detection sandboxing technology maximizes the security efficacy of Forcepoint's products. Even highly evasive threats are revealed through Deep Content Inspection at multiple levels, in dormant code, and in other indicators often overlooked by traditional sandboxing technologies. Eliminate the distraction of false positives with AMD. Keep your incidence response team focused on actual threats, not chasing down false positives or searching for incidents of compromise (IOCs).

Network Security

Forcepoint NGFW

Integrates application control, sophisticated evasion prevention and an intrusion prevention system (IPS) into a single solution that is cost-effective and easy to deploy. It has a proven capability to identify advanced evasion techniques (AETs) that evade other devices, and delivers exfiltration protection using both application and endpoint intelligence. Forcepoint NGFW optimizes and scales network security for your distributed enterprise with lower infrastructure costs and far less downtime.

ABOUT FORCEPOINT

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide. For more about Forcepoint, visit www.forcepoint.com and follow us on Twitter at @ForcepointSec.

CONTACT

www.forcepoint.com/contact

[BROCHURE_FORCEPOINT_FEDERAL_GLOBAL_GOVERNMENTS_OVERVIEW_EN]
400015.102417