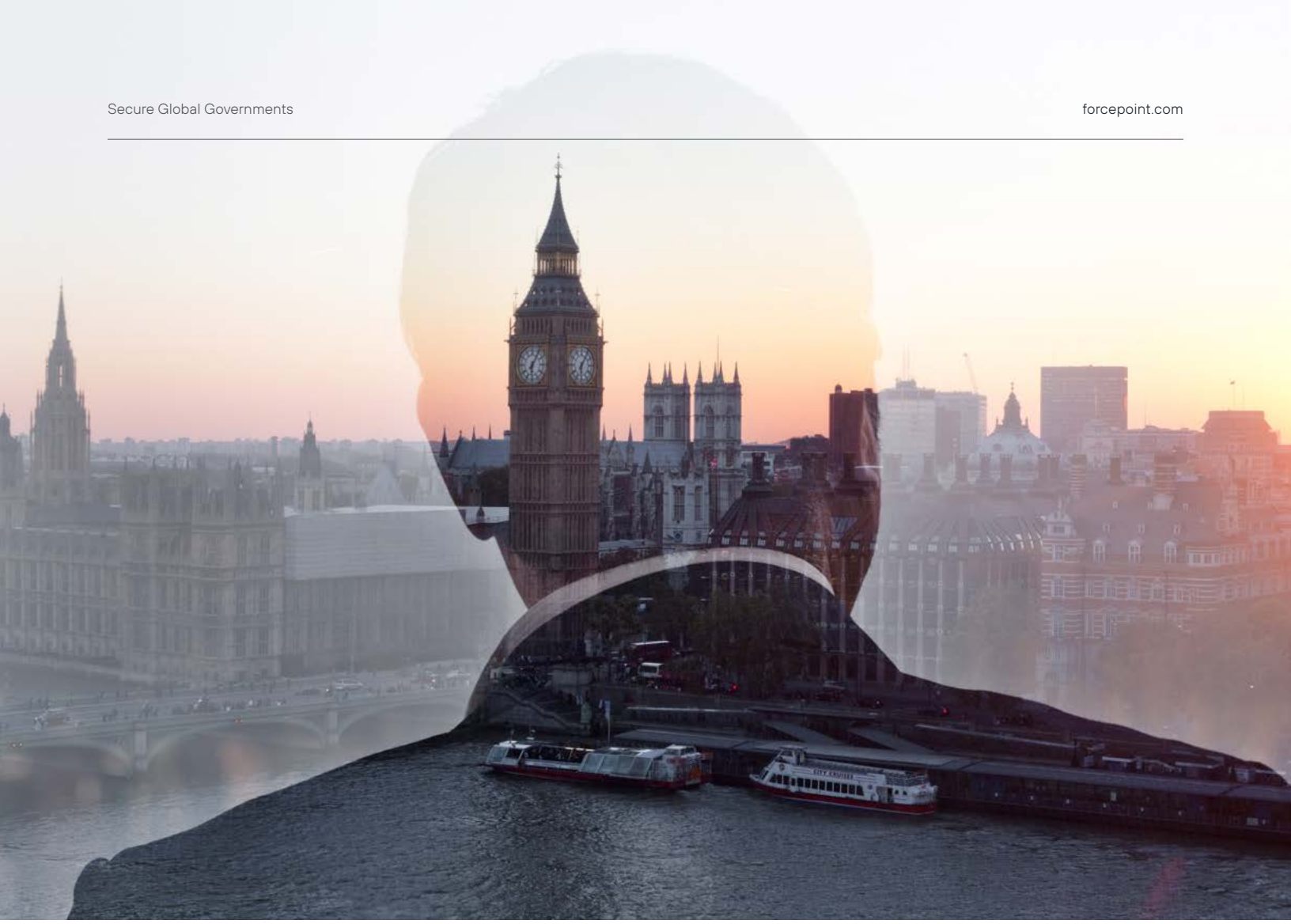
Secure Global Governments

With Forcepoint Solutions

Forcepoint

Brochure

What's Inside:



A Proven Leader in Defence-Grade Cyber Security

Forcepoint brings more than 20 years of expertise supporting the unique and complex missions and objectives undertaken by the people who protect national security and mission-critical information. Intelligence communities, defence departments and civilian agencies require rapid, accurate and secure ways to support their data-driven missions.

Forcepoint solutions bring together data security, network, web and cloud security; threat protection; advanced monitoring; Cross Domain protection and Zero Trust control to empower agencies to use data where and how your people need it safely. Our mission is to simplify security and protect data wherever it resides.

The Forcepoint portfolio of cyber security solutions are designed to meet the most stringent security requirements and mission objectives

Forcepoint technology is built from the ground up to meet your essential needs:

Adaptive Security

Ensure that critical and sensitive data remains protected and guarded while enabling rapid authorised access and transfer.

Access Anywhere

Securely access mission-critical data whenever and wherever it's needed: air, space, land or sea, on network or in the cloud.

End-to-End Visibility and Control

Protect data against intentional or malicious compromise everywhere it resides and moves across the organisation and wherever the mission takes it.

Advanced Analytics

Rapidly transform information into accurate insights to inform the right actions from across the organisation.

Integrated Solutions to Support the Mission

Forcepoint's integrated technology delivers comprehensive security to identify and respond to risks in real time. Forcepoint is a key partner for agency cyber security, with solutions scaled to support security programs.

Forcepoint Cross Domain Solutions (CDS) support thousands of government agencies and users worldwide.

The answer is to provide a Cross Domain Solution, a way for information to safely cross between untrusted and trusted IT systems allowing business processes to flow whilst protecting the confidentiality, integrity and availability of the trusted system.

Forcepoint Cross Domain Solutions have a proven track record of proactively preventing government and commercial organisations from being compromised, while fostering the secure access and transfer of information. These solutions strike the right balance between information protection and information sharing—a vital component to global and national security.

Forcepoint's Cross Domain Solutions (CDS) are designed to support the unique and complex missions and objectives undertaken by those who protect our national security—from intelligence communities to defence departments and civilian agencies.

Valued ('trusted') IT systems which handle sensitive information or control highly critical operations are separated from other less trusted IT systems ('untrusted'), to protect them from either deliberate or accidental misuse. Typically, business processes must flow between the trusted and untrusted systems. Whilst just connecting the two systems would make it easy to implement the business flow, generally the internal security controls that would then be needed to protect the system would be too expensive, too risky and impractical.

Cross Domain Solutions

A Cross Domain Solution (CDS) enables the secure movement of data between a network that requires protection and one or more external networks. The term CDS can have subtly different meanings in different organisations or nations. In some definitions, for example, the CDS is the core security enforcing component of a solution which is then surrounded by supporting components. In others, the term CDS covers everything from the core security-enforcing component extending out to the edges where data is being sent and received.

A CDS is different to the use of commercial security gateways. Although in the wider definition of a CDS above, commercial security gateways may be part of the solution, the key to the CDS is its ability to withstand advanced forms of attack and its ability to assure that by independent test and assessment.

A CDS typically exhibits some key characteristics such as protocol breaks, transformation and verification of data, deep content inspection and flow control. Advanced CDS perform some of this in hardware logic to overcome vulnerabilities that can be introduced into software.

Information eXchange (iX)

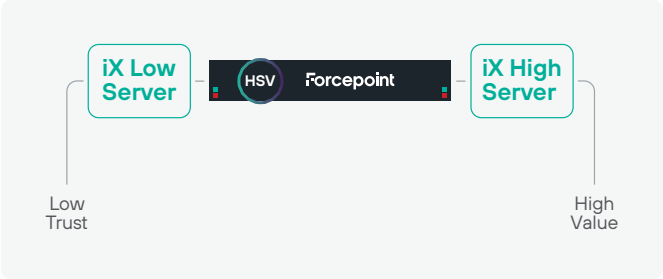
Deployed inline on a network perimeter, Forcepoint Information eXchange (iX) enables the secure transfer of email, web applications, file transfers and network/ logging traffic.

Inline Threat Removal

Forcepoint iX handles a wide range of protocols and associated data formats enabling threat removal for email, file transfer, web applications and network/ logging traffic. Located at the network perimeter, iX operates inline to remove threats from business content, including unstructured formats like Office and PDF, and application-specific structured data like XML and JSON.

Hardware Logic Verification

For systems that face the most sophisticated attackers and require a minimal attack surface, a pair of iX units can be deployed connected via Forcepoint High Speed Verifier (HSV). The HSV provides independent verification implemented in hardware logic and as such uses none of the software and networking components that might house a backdoor exploit or make it vulnerable to attack.



Key Benefits

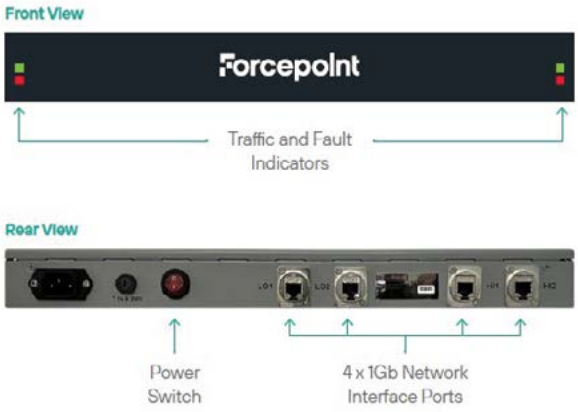
- → Simple setup. Intuitive GUI and configuration – up and running in under 10 minutes.
- → Multi-channelled. Multiple cross-boundary applications can share one iX.
- → Malware removal. Threats concealed in Office documents and PDFs are removed during transformation.
- → Stegware removal. Threats concealed in Web images and social media feeds using steganography (stegware) are removed during transformation.
- → Bi-directional protection. Stops malware being infiltrated, prevents covert outbound data loss and smashes Command and Control channels.
- → Auditing and off-box logging. For offline forensic examination

High Speed Verifier (HVS)

Deployed inline on a network perimeter, Forcepoint Information eXchange (iX) enables the secure transfer of email, web applications, file transfers and network/ logging traffic.

Inline Threat Removal

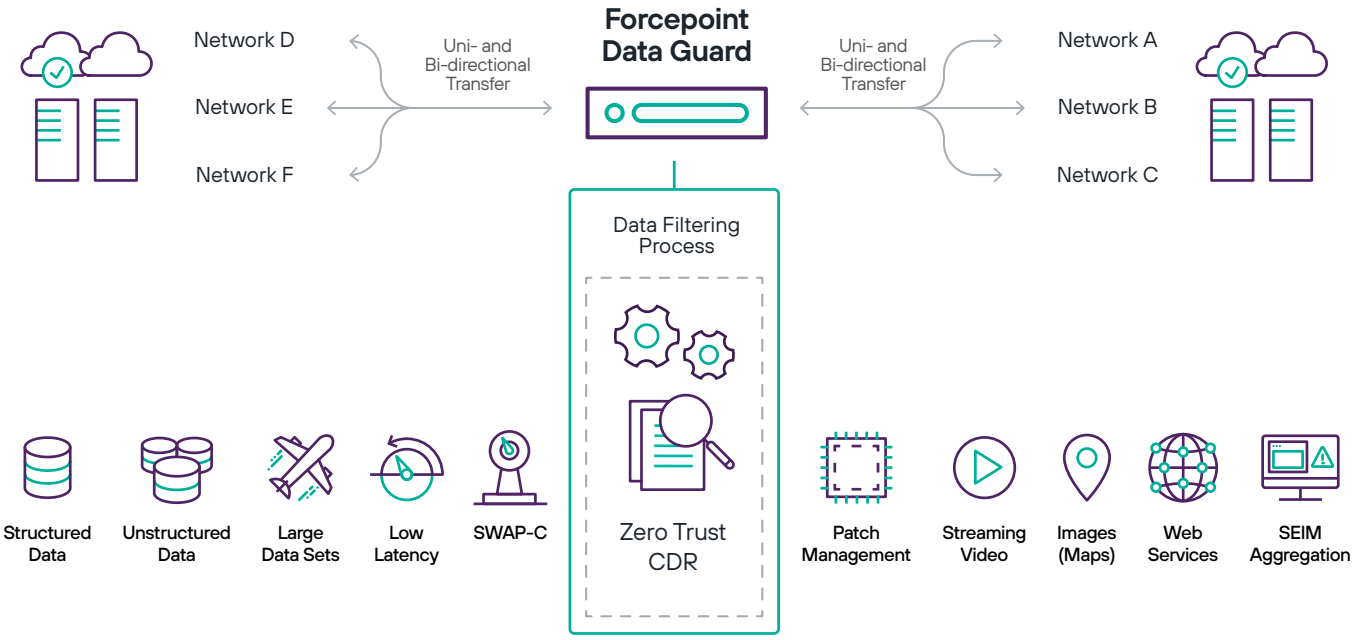
- → Supports bi-directional communication with data payload.
- → Hardware-enforced data verification, flow control and protocol break.
- → Defends against attacks concealed in data.
- → Verifies data is safe in hardware logic.
- → Enforces ultra-high assurance security..



Data Guard

Forcepoint Data Guard delivers this balance by enabling highly complex, bi-directional, automated data and file transfers between physically separated networks.

To provide defence-grade data control at scale, Data Guard leverages a trusted operating system and security policies that enforce role and process separation and isolation for automated, byte-level content inspection and sanitisation, with customisable rules to handle even the most specialised data types and protocols.



Supporting Today's Security Paradigms

Data Guard enables secure data and file (structured and unstructured data) movement between segmented networks in uni-, bi- or multi-directional fashion. The trusted operating system foundation derived from Red Hat Enterprise Linux with enhanced SELinux modules allows Data Guard to be used in highly regulated environments.

A Flexible Approach

Data Guard is highly flexible in its secure approach to high-assurance data movement through the robust security policies within adaptors, plugins and the filtering process. The rule engine provides APIs to handle rich data types including: HTTP header, JSON, SOAP, MIME, compression, HTML, XML, file sanitisation for Office, PDF and images, streaming data and the flexibility to secure most TCP and UDP protocols.

Key Benefits:

- → Full protocol break using common criteria-evaluated platform.
- → Highly customisable data validation rules for maximum flexibility.
- → Software implementation for all environments.
- → Enables high-availability network access.
- → Lowers operational expenses.

Data Diode

The Forcepoint Data Diode enables rapid, uni-directional, automated transfer of highly complex data to segment and protect networks, devices and other digital assets.

Securing One-Way Data Flows

Government organisations need to gather and share data across oceans, battlefields and offices rapidly and securely. Meanwhile, regulations such as Raise the Bar and GDPR have dictated a move to hardware-based data separation and require a solution that provides one-directional data flow.

Key Benefits:

- → Rapid, secure one-way and automated transfer of highly complex data with optical isolation.
- → Supports local log consolidation.
- → Safeguard communications between system integrators and regulated industries.
- → Lowers total cost of ownership as little to no maintenance is required.
- → Simplifies configuration, operation and monitoring.

One-Way Transfer

Policy Engine Guard

The Policy Engine Guard is used by organisations that need to tightly control business content that needs to pass across an external boundary or between separate internal zones over email, web or file transfer. It defends against known malware and accidental data loss by focusing on business content. It is ideally suited to systems in government, law enforcement, defence and critical national infrastructure.

Deep Content Inspection

The Policy Engine Guard intercepts content at the boundary point and uses Deep Content Inspection (DCI) to examine it for the presence of known threats and the possibility of accidental data loss. Embedded content, including archives, is unwrapped to gain a complete picture of the data being carried.

Key Benefits:

- → Protects organisations from accidental data loss and known malware infiltration at the network boundary.
- → Validation of S/MIME signed messages (email).
- → Address validation (email) and NTLM authentication of users (web).
- → Ability to apply policy based on identification of unstructured or structured protective marketing/ security labels and user clearances.

Modernising Government Security with a Zero Trust Approach

Within complex security ecosystems, Zero Trust cannot be merely a compliance exercise. Adding more point products and policies only makes security unmanageable. A more unified security platform is needed.

Forcepoint solutions go beyond static access controls to truly transform your security. We offer a unified security platform that spans the pillars of Zero Trust to provide both inbound threat protection and outbound data loss prevention. Forcepoint expertise in Cross Domain enables us to deliver the only integrated Zero Trust solution that is authorised to protect multi-level mission environments. This can support governments globally, whether they work from home, at secured facilities or at the tactical edge.

Zero Trust Security

Zero Trust Content Disarm and Reconstruction (CDR)

Stop known and unknown threats, zero-day attacks and malware

Detection-based defences alone simply can't keep up.

Rather than trying to detect malware, this model assumes nothing can be trusted. It works by **extracting the valid business information from files** (either discarding or storing the originals), **verifying the extracted information is well-structured**, and then **building new, fully functional files** to carry the information to its destination.

Zero Trust CDR is a game-changer for mitigating against the threat of even the most advanced zero-day attacks and exploits. Pivoting from detection to prevention in this way is especially important with the recent evolution in hybrid workforces and digital transformation and their resultant usage of content and electronic information everywhere.

Key Benefits:

- → Stops ransomware and zero-day threats without the need for the latest patches.
- → Reduce costs and frees up SOC teams—from day one, with zero false positives.
- → Enhances user experience and reduces latency by not subjecting incoming files to multiple scanners, sandboxing or flattening.
- → Defends a wide range of attacks vectors (i.e. web, email and file transfers).

Extract

Content from Original Data, Discard Unwanted Content

UNSAFE DIGITAL CONTENT

Verify

That the information is Safe

Build

And Deliver Safe Information and Data

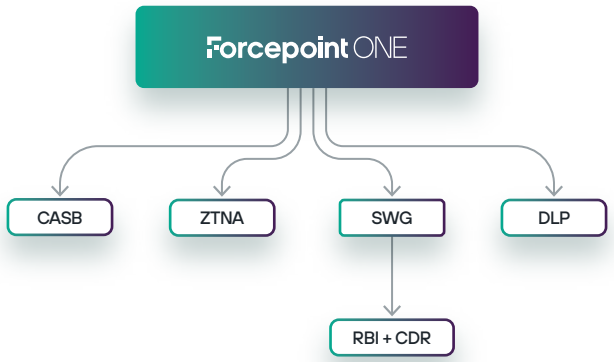
SAFE DIGITAL CONTENT

Forcepoint ONE

Security Simplified into an all-in-one cloud native security platform, Forcepoint ONE gives traditional and remote workers safe and controlled access to business information on the web, in the cloud and within private applications.

Key Benefits:

- → Single console policy management for CASB, ZTNA, SWG and RBI.
- → Unmanaged device support with patented reverse proxy.
- → Accelerated performance with 300+ PoPs with hyperscaler backbone.
- → Zero Trust security at scale.
- → Reduce risk and prevent data loss across use of the web, cloud and private apps.



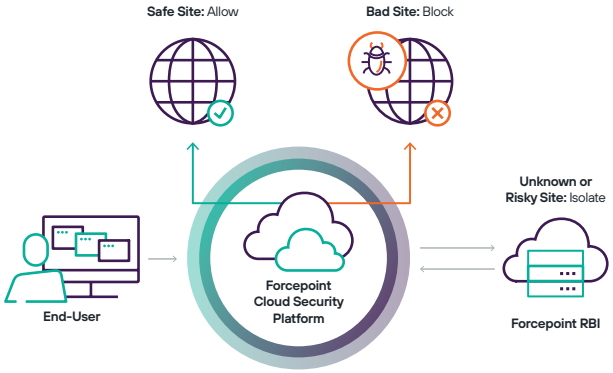
Remote Browser Isolation (RBI)

Neutralise web security threats and prevent attacks before they occur with RBI.

Remote Browser Isolation (RBI)

Employees need the freedom to work online. In fact, up to 75% of today's work is done browsing the web. It can be a dangerous place with cyber attacks stemming from malicious sites and drive-by downloads or being disguised as helpful links in emails.

Forcepoint RBI with Zero Trust Content Disarm and Reconstruction (CDR) makes Zero Trust Web Access easy to implement and adopt. Zero Trust Web Access allows employees to safely and efficiently be more productive from anywhere. **Block attacks without blocking work.**



Insider Protection

Insider Risk

Unrivalled visibility into user behaviour to detect threats from within.

Why Insider Threat?

Collect, Explore and Gain Insight.

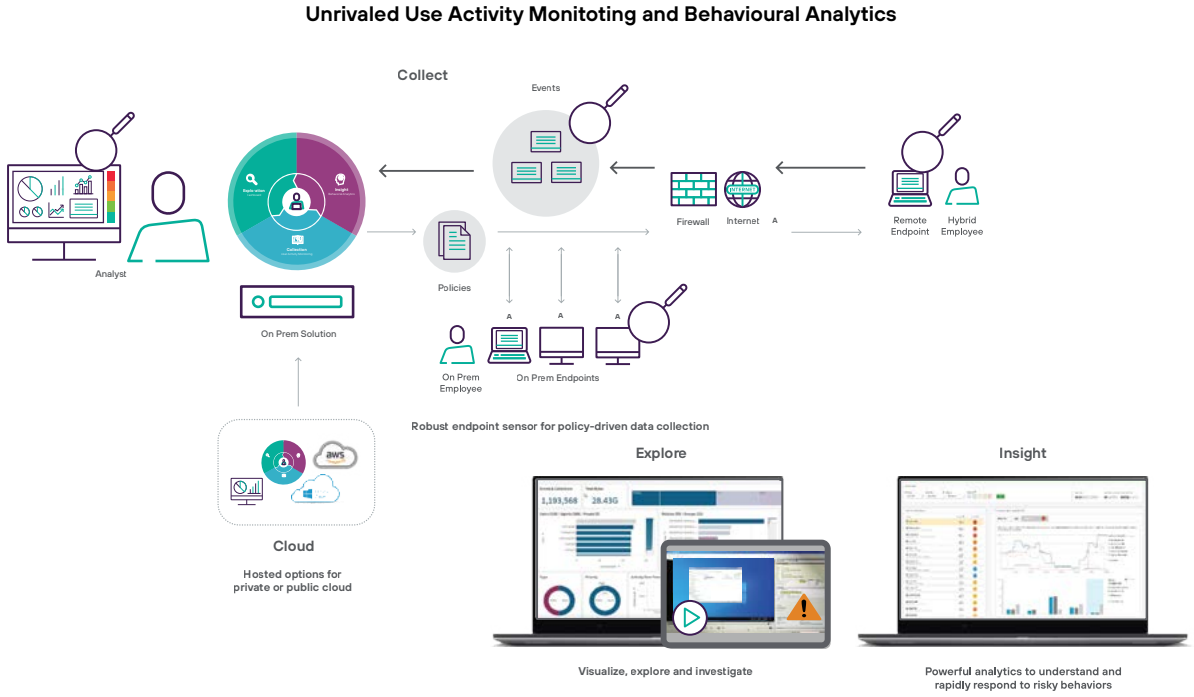
Collect behavioural data from channels such as web, file operations, keyboards and email.

Explore meaningful data using a powerful dashboard built for analysts, by analysts.

Gain Insight with powerful analytics to understand and rapidly respond to risky behaviours before harmful events occur.

Key Benefits:

- → Monitor a broad set of data sources and activities.
- → Custom configuration to suit specific requirements.
- → In-depth analytics to ensure rapid response to risky behaviours.
- → Collect behavioural data from multiple channels.
- → Protect your workforce from internal and external threats.
- → Safeguards your data and critical assets.
- → Increases visibility and user monitoring.



Data Loss Prevention (DLP)

Visibility and control everywhere your people work and data resides.

Data security is a persistent challenge. Forcepoint Data Loss Prevention (DLP) enables businesses to discover, classify, monitor and protect data intuitively with zero friction to the user experience. Audit behaviour in real time with Risk-Adaptive Protection to stop data loss before it occurs..

Key Benefits:

- → Unified policy across all/multiple channels: endpoint, network, cloud, web and email.
- → The easiest policy creation in the industry and most complete data identification library.
- → Support for structured and unstructured intellectual property (IP) data.
- → Implement consistent data loss protection with a single platform across the whole organisation.
- → Remove analyst blind spots to data usage with visibility to data everywhere.
- → Quickly and easily achieve data security compliance across all channels.

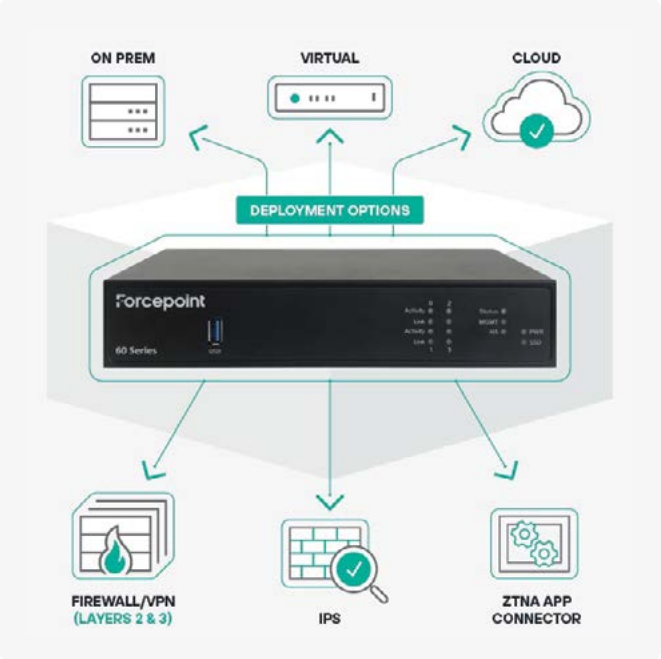
Network Security

Next-Gen Firewall

Fast, resilient security that scales easily.

AAA RATED BY CYBERRATING—Top-Rated NGFW and Secure SD-WAN

Blocking 100% of evasion attempts and 100% of exploits, Forcepoint Cloud Network Firewall was given a AAA rating when tested by CyberRatings.



Forcepoint Next-Generation Firewall can be deployed via a range of physical and virtual appliances to suit any size organisation and their unique needs.

All of Forcepoint's industry-leading NGFW security features are available on all appliances in the range along with centralised management, and the dependability needed in modern network security, along with no hidden costs such as per-user licensing for features like VPN connectivity.

Our products routinely undergo rigorous certifications testing to meet the most stringent needs of sensitive and critical industries, agencies, organisations and governments around the world

Key Benefits:

- → Industry-leading integrated intrusion detection and prevention.
- → Safeguard site-to-site and site-to-cloud communications.
- → Zero-touch deployment & updates of thousands of sites from a single console.
- → Built-in high-availability SD-WAN and ZTNA App Connector.
- → Easy integration with SASE/SSE platforms.
- → Simplify operations with centralised visibility and control.

Who is Forcepoint?

Forcepoint was purpose-built to provide next-generation cyber security solutions:

- → More than 20 years of expertise supporting the unique and complex missions undertaken by the people who protect national security.
- → One of the largest private cyber security companies in the world, with thousands of enterprise and government customers in more than 150 countries.
- → Leading supplier to global intelligence community and high-assurance cyber missions.
- → One of the most comprehensive security product portfolios in the industry.

The system was purposely designed: Each element is best-in-class and can stand alone or integrate within your existing environment to help solve critical security issues and protect employees, data and IP.

Forcepoint enables better decision-making and more efficient security through proactive and context-based technologies and data-centric, integrated solutions to help solve:

- → Cross Domain security
- → Cloud-based user and application protection
- → Next-generation network protection
- → Data security
- → Systems visibility

This risk-adaptive cyber security approach integrates best-in-class products with analytics and behavioural profiling, bringing agencies near real-time risk insights and automated remediation to better protect government users' data wherever it resides, including Controlled Unclassified Information (CUI).

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP-Brochure-Securing Global Governments] 16Oct2023