Forcepoint Web Security

Forcepoint cloud and on-premises web security

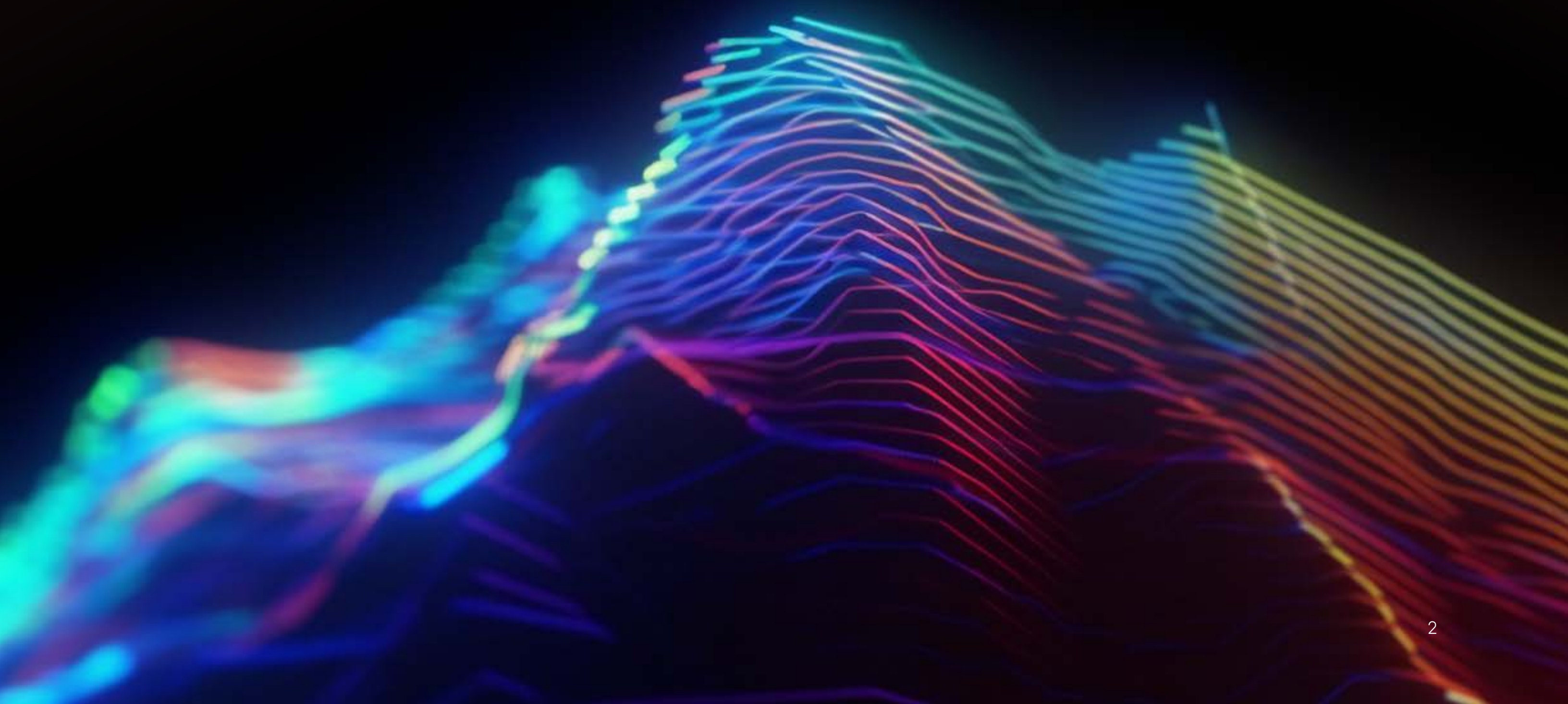
Forcepoint

Brochure

forcepoint.com

Protecting productivity for the modern enterprise

Web use is fundamental to productivity in the modern enterprise, and even fundamental to regular daily life. However, this is a large vulnerability as threat actors constantly innovate new ways of delivering malware and stealing data online, and even well-meaning employees accidentally click on links they probably shouldn't, or save information in a web service they shouldn't – often in an effort to get around friction and be more productive. This is why we need a modern, Zero Trust approach to web access. An approach built around a flexible architecture to deliver a multitude of options for connectivity that allow better performance in more places, and support for as many working scenarios as possible, without compromising on our industry-leading data security and threat protection capabilities.



Forcepoint Web Security

Flexibility for better protection in more places

Forcepoint Web Security is built with a uniquely flexible architecture to accommodate a wide variety of deployment needs. This distributed enforcement architecture gives you more options for where or how security policy should be enforced in different situations – whether you need traffic inspected in the cloud, on-premises, at the endpoint, or a mix of all of the above.

Many organizations prefer the benefits of a SaaS service to minimize management requirements and avoid delays to new version updates. However, there are still requirements for certain industries and geographies to have more direct control over the security hardware and insure that data is inspected on-premises. Others prefer a hybrid approach with on-premises management at the HQ and cloud enforcement for branch sites and roaming users. All of these are easily supported by Forcepoint's uniquely flexible architecture

Real-time analysis for advanced threat protection

Forcepoint's Advanced Classification Engine (ACE) inspects traffic content and usage patterns using up to eight different defense assessment areas for identifying malware, phishing, spam, and other risks to the enterprise.

At the heart of ACE is a decision engine that identifies the nature and format of the digital artifact being analyzed and routes it through to the most appropriate defense assessment area for real-time scanning. Each defense assessment area, and each underlying analytic, is built to offer the highest efficacy and efficiency for real-time analysis of that artifact. These defense assessment areas are all modular by design, permitting Forcepoint X-Labs to add, swap, and tune them as the threat landscape evolves.

Easy dashboard access to forensic data

The Forcepoint Web Security advanced threat dashboard provides forensic reporting on who was attacked, what data was targeted, the data's intended endpoint and how the attack was executed. Security incidents include data theft capture when possible. Defenses analyze inbound and outbound communications.

Uncompromising data theft defenses

Augment the built-in data theft capabilities with Forcepoint's industry-leading Data Loss Prevention (DLP) solution to add advanced classifiers like exact data matching and machine learning capabilities for even stronger controls with lower false-positives. Additional capabilities include detection of custom-encrypted uploads, password file data theft, slow data leaks (Drip-DLP), optical character recognition (OCR) of text within images and geolocation destination awareness.

Web Security Objectives:

Many web security solutions are really only effective against known malware. Forcepoint Web Security uses built-in machine-learning and heuristics to identify new threats just as effectively as known ones.

› **Securing Every User, Everywhere, From Advanced Threats**
Extend your protection seamlessly to both on-premises and remote workers, wherever they need to be productive

› **Shadow IT Visibility and Control**
Discover cloud applications being used within your organization. Monitor usage of those applications to determine and block those that represent the greatest risk.

› **Secure Sensitive Data**
With best-of-breed data loss prevention capabilities built-in you have all you need to identify and control the movement of sensitive data to websites and unsanctioned web applications – mitigating the most costly risks associated with Shadow IT use.

Integrated sandboxing

Learn how to better protect your company's assets through automatic analyzing of malware behavior by adding the integrated sandbox integrated sandbox service, Advanced Malware Detection and Prevention (AMDP).

Cloud application discovery, monitoring and control

Discover cloud applications being used within your organization and their associated risk levels with easy options to restrict access based on risk. Built-in data theft controls help maintain control over sensitive and regulated data by making it easier to limit which types of data can be sent to various cloud applications. Augment these controls with Forcepoint's SaaS app security solution to add API and reverse proxy capabilities.

ENHANCED PROTECTION MODELS	MODULE FEATURES
Remote Browser Isolation (RBI)	RBI isolates web traffic in a secure environment and streams the web interaction back to the user so any malware that may be present cannot infect the user's device, only the isolated browser which is deleted at the end of the session. RBI is included for web traffic 'uncategorized' sites and can be augmented with the 'Selective Isolation' license to add coverage for up to 10 web content categories, or the 'Full Isolation' license to add coverage for as many web content categories as you want.
Data Loss Prevention (DLP)	Add a powerful, contextually aware DLP engine for added outbound protection against data theft. Augmenting Forcepoint Web Security with Forcepoint Enterprise DLP provides containment defenses against data theft and enables regulatory compliance with over 1,700 pre-defined policies and templates. It also includes industry-leading protection such as Drip-DLP against slow data leaks, OCR against theft of data files in image files, or Custom Encryption Detection for detection of criminally-encrypted files.
Advanced Malware Detection and Prevention (AMDP)	Integrate behavioral sandboxing for automatic analysis of malware files. Analyze suspicious files in a virtual environment to provide the highest level of protection from advanced malware. Detailed forensic reporting is automatically provided when malicious files are detected.
Cloud Access Security Broker (CASB)	Augment the built-in cloud application visibility and control capabilities in Forcepoint Web Security with Forcepoint's CASB solution to add reverse proxy and API controls to cover unmanaged device access to managed cloud applications, data discovery, and more.

Forcepoint Solutions

Forcepoint ACE

ACE is a time-tested, deep-inspection engine that uses heuristics, reputations, and malware signatures to provide threat avoidance capabilities to the Forcepoint product suite.

ACE delivers defense-in-depth through layered sets of threat detection analytics, which comprise the eight defense assessment areas of ACE. ACE offers optimum protection by invoking the most effective defense assessment area and analytic at the right time.

For example, our set of Anti-malware analytics is powered by:

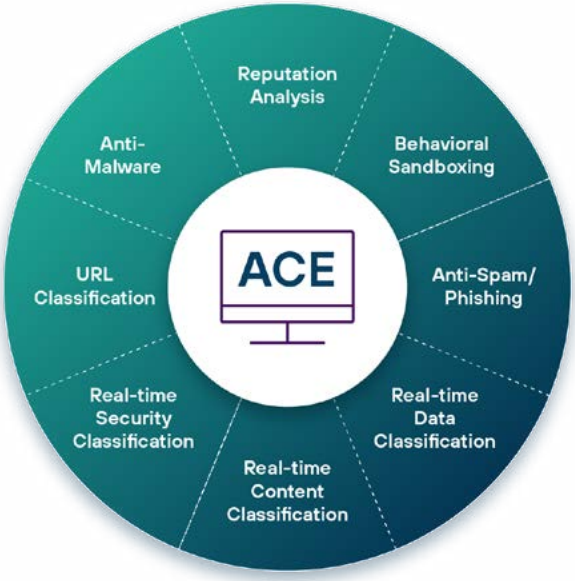
- → Forcepoint's own hash database of malicious files for identifying known malware
- → Heuristic rules to detect previously unknown malware
- → A third-party anti-virus vendor for signature-based malware protection

Forcepoint ThreatSeeker Intelligence

The Forcepoint ThreatSeeker Intelligence, managed by Forcepoint X-Labs, provides the core collective security intelligence for all Forcepoint security products. It unites more than 900 million endpoints with Forcepoint ACE security defenses and analyzes billions of requests per day. This expansive awareness of security threats enables the Forcepoint ThreatSeeker Intelligence to offer real-time security updates that block advanced threats, malware, phishing attacks, lures and scams, plus provides the latest web ratings. Forcepoint ThreatSeeker Intelligence is unmatched in size and in its use of ACE real-time defenses to analyze collective inputs. (When you upgrade to Web Security, the Forcepoint ThreatSeeker Intelligence helps reduce your exposure to web threats and data theft.)

Unified architecture

With best-in-class security and a unified architecture, Forcepoint offers point-of-click protection with real-time, inline defenses from Forcepoint ACE. The unmatched real-time defenses of ACE are backed by Forcepoint ThreatSeeker Intelligence and the expertise of Forcepoint X-Labs researchers. The powerful result is a single, unified architecture with one unified user interface and unified security intelligence


ACE
Reputation Analysis
Behavioral Sandboxing
Anti-Spam/ Phishing
Real-time Data Classification
Real-time Content Classification
Real-time Security Classification
URL Classification
Anti-Malware

Integrated set of defense assessment capabilities in 8 key areas

- → Thousands of analytics available to support deep inspections
- → Predictive security engine sees several moves ahead
- → Heuristic analysis identifies new threats as they appear

> "Forcepoint has enabled us to think differently, architecturally, and leverage more cloud applications for improved business outcomes."

Chris Anderson,
Head of Infrastructure Services,
Bendigo and Adelaide Bank

	ON-PREM	HYBRID	CLOUD
Threat Prevention Capabilities Product features			
Proxy (SSL) In-line inspection of all web traffic ensures maximum security efficacy	●	●	●
Real-time Security Classification Employs many types of analysis to identify malicious code that is often hidden behind dynamic content	●	●	●
Real-time Content Classification Classifies web content from any and all web pages into over 130 categories to enable highly granular access filtering	●	●	●
Anti-Virus, Anti-Malware Applies anti-malware protection capable of proactively blocking the latest in binary and s cript-based threats	●	●	●
Heuristic Analysis To identify and protect against malware that has not been encountered previously by using machine learning to tune and update heuristics.	●	●	●
Reputation Analysis Reputation databases prevent traffic from being redirected to untrustworthy sites	●	●	●
URL Database Classifies known URLs and assesses new URLs based on associated sites and redirections	●	●	●
File Sandboxing Advanced Malware Detection adds the layer of security to ensure protection against zero-day threats nefariously hidden in files	Add-on	Add-on	Add-on
Remote Browser Isolation When the solution detects a risky site that should be blocked but the business needs to allow access anyways, the risky session can be handled via Remote Browser Isolation to ensure security while still permitting access	Add-on	Add-on	Add-on*
File Type Blocking (inbound) Allows blocking of inbound files based on based on true file type type within a policy	●	●	●
Cloud Application Risk Database Identify the risk level of cloud apps that are being used across the enterprise	●	○	●
ThreatSeeker Global Threat Intelligence Aggregates threat intel from Forcepoint products deployed around the world and provides threat telemetry back to all Forcepoint security solutions	●	●	●
Data Protection Capabilities Product features			
Cloud Application Visibility The Cloud Apps dashboard gives visibility into all sanctioned and unsanctioned cloud apps in use across the enterprise	●	○	●
Unsanctioned Cloud Application Blocking Use web access controls to restrict access to risky, unsanctioned cloud apps. cloud apps	●	○	●
Standard Compliance DLP Protects sensitive info such as PII, PHI, PCI as well as password files and custom encrypted files from being sent over the web channel (for on-prem and hybrid this is provided via the Web DLP module, or integration with the full DLP Suite)	Add-on	Add-on (limited*)	●

* Included for uncategorized sites

	ON-PREM	HYBRID	CLOUD
Data Protection Capabilities Product features			
Advanced DLP Classifiers The add-on Web DLP module, or integration with the full DLP Suite provides use of advanced classifiers such as precise fingerprinting for full and partial matches, as well as machine learning to identify novel structured and unstructued data based on positive and negative training samples	Add-on	Add-on (limited*)	Add-on
Data Classification Labeling An additional add-on for the DLP Suite to provide robust data classification capabilities to ensure all data is properly labeled and protected throughout the enterprise	Add-on	Add-on (limited*)	Add-on
Extensive Global Compliance Policy Library The add-on Forcepoint Data Protection Service (DPS) for integration with the full. DLP Suite provides an extensive library of policies that allows practitioners to easily enforce regulatory compliance around the world	Add-on	Add-on (limited*)	Add-on
Web Control Capabilities Product features			
Granular Web Access Controls Allows finely tuned control of corporate web and cloud app use	●	●	●
Granular Social Media Controls Control permissible use of social media and distinguish between sections like mail, games, chat, posting, photo uploads, and more	●	●	●
Connection-based Policy Switching/Context Aware Policy Switching Automatically adjust policy based on how and where the user is connecting from	●	●	●
Productivity Controls/Quotas Enforce quotas on any web categories during business hours to help maintain productivity	●	●	●
Single Sign On Enforce identity-based access controls via integration with SAML 2.0 compliant Identity Providers	●	●	●

* Currently the hybrid deployment's integration with DLP and CASB features is limited to traffic flowing through the on-prem proxy.

The Forcepoint cloud

- 160 PoPs world-wide means, no matter where users are connecting from, they are never far from a Forcepoint PoP so they will always have a good user experience.
- Forcepoint has a large number of private peering partnerships with tier 1 networks. This means Forcepoint customers' web traffic traveling through the Forcepoint Cloud gets an express route through the internet.
- Forcepoint only uses the highest-tier data centers (tier 4) to provide the most fault tolerance and the highest level of uptime to our customers.
- The Forcepoint cloud is fully compliant with leading cloud standards and certifications such as: ISO 27001, ISO 27018, and SOC 2 Type II.
- A variety of traffic steering options including explicit proxy, transparent proxy, IPSEC and GRE tunnels, EasyConnect, and Forcepoint Endpoints means enterprises always have plenty of secure options for getting web traffic to the Forcepoint cloud. With up to 5 Gbps tunnel support for IPSEC and GRE, all sizes of enterprises will have the throughput capabilities they need.
- The Forcepoint cloud supports integration with any SAML 2.0 Identity Provider to allow the enforcement of strong identity-based authentication and access control.
- Forcepoint Web Security's Dedicated IP add-on allows customers to egress their cloud traffic via a dedicated IP provided by Forcepoint without any additional latency or need to backhaul traffic back on-premises. This feature unlocks advanced Multi-Factor Authentication (MFA) scenarios for large enterprises or modern B2B organizations such as only allowing sensitive cloud app access from a restricted set of IP addresses.

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, X and LinkedIn.

[Forcepoint Web Security - Brochure] 12Nov2024