Forcepoint Web Security

Forcepoint's cloud and on-premises web security

Forcepoint

Brochure

Safeguarding the web so your business can thrive.

Threats over the web channel have grown more complex and become much more frequent recently, but many web security solutions don't provide the defense-in-depth that is necessary to stop advanced threats hidden in dynamic web content. In order to defend the modern enterprise and thrive, web security needs to go beyond DNS checks and IP reputation; web security needs to be able to mitigate risks in real-time by using full content inspection and in-line security scanning to protect against novel malware just as effectively as known malware.

Forcepoint Web Security

Customizable with the option to expand

Companies need customizable solutions that communicate together to protect against threats as they happen. Forcepoint Web Security offers real-time protection against advanced threats and data theft with multiple deployment options and modules to help tailor your web protection package to your organization's needs.

Forcepoint Web Security provides robust protection through content aware defenses and cloud app discovery and monitoring, reducing risks to sensitive data for both on premise and mobile users.

Best of all, Forcepoint Web Security easily integrates with other Forcepoint solutions for unified, consistent security controls that can protect against inbound and outbound threats with even the smallest of security teams.

Real-time analysis for advanced threat protection

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 purpose-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.

Integrated data theft defenses

Industry-leading integrated data theft defenses (optional) detect and intercept data theft attempts and provide regulatory compliance for data loss prevention (DLP). Examples of these capabilities include detection of custom-encrypted uploads, password file data theft, slow data leaks (Drip-DLP), optical character recognition OCR (Optical Character Recognition) of text within images and geolocation destination awareness.

Integrated sandboxing

Learn how to better protect your company's assets through automatic analyzing of malware behavior with the integrated sandbox service.

Cloud application discovery, monitoring and control

Discover cloud applications being used within your organization and prevent users from jeopardizing your data by sending to unsanctioned cloud applications and services. Easily add full Cloud Access Security Broker (CASB) capabilities for cloud applications using inline (proxy) integration.

Web Security Objectives:

Most of today's security solutions can't address Advanced Threats as they happen. Forcepoint Web Security is advanced, real-time threat defense.

- **Securing Every User, Everywhere, From Advanced Threats**
  Extend your protection seamlessly to both on-premises and remote workers, wherever they access the network.
- **Integrated 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.
- **Reduce Your Security Spend While Improving Operational Efficiency**
  Visibility and control for cloud applications within your organization. Quickly discover Shadow IT to ensure risk exposure is managed. Apply controls with full integrated Cloud Access Security Broker (CASB) features as part of the Web Security Gateway for cloud applications supported via inline (proxy) integration.

ENHANCED PROTECTION MODULES	MODULE FEATURES
Hybrid Cloud Deployment	**Extend web protection and policy enforcement to remote users** Deploy Forcepoint Web Security as a physical or virtual appliance for your private cloud. Either choice can be further extended with Forcepoint's global cloud infrastructure for remote user protection.
Web DLP	**Add a powerful, contextually aware DLP engine for added outbound protection against data theft** The Forcepoint Web 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, Optical Character Recognition, (OCR) against theft of data files in image files, or Custom Encryption Detection for detection of criminally-encrypted files.
Cloud Sandbox	**Integrate behavioral sandboxing for automatic and manual analysis of malware files** Analyze suspicious files in a virtual environment and look far deeper than simple file execution to provide the highest level of protection from advanced malware. Detailed forensic reporting is automatically provided when malicious files are detected.
Mobile Security	**Extend policies and protection to iOS and Android users** Extend your existing security policies to mobile devices and protect them from Advanced Threats, mobile malware, phishing attacks, spoofing and more. Forcepoint Mobile Security works with your mobile device manager (MDM) to provide full protection to mobile devices.
CASB	**Extend full CASB functionalities to complement existing ability to gain visibility into what cloud applications are being used** These full CASB functionalities can be used to control cloud applications for inline (proxy) deployments, and easily extended from the web security gateway.

The Power Behind 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:

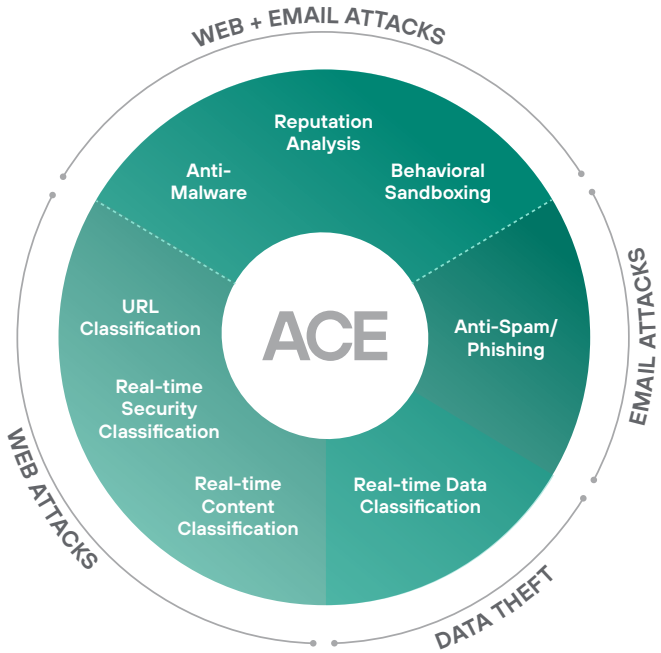
- → Forcepoint's own hash database of malicious files for identifying known malware
- → Heuristic rules to detect previously unknown malware
- → A third-party anti-virus vendor for signature-based malware protection

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.



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 categores to enable highly granular access filtering	●	●	●
Anti-Virus, Anti-Malware Applies state-of-the-art anti-malware protection capable of proactively blocking the latest in binary and script-based threats	●	●	●
Heuristic Analysis To identify and protect against malware that has not been encountered previously	●	●	●
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	●	●	●
Behavioral File Sandboxing Advanced Malware Detection adds the ultimate 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 file 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 unsanctioned cloud apps	●	●	●
Granular Sanctioned Cloud Application Access Control The add-on Cloud Application Control Module, or integration with the full CASB Suite provides granular control of activity within sanctioned cloud apps to give comprehensive security across all browser based activity	Add-on	Add-on	Add-on
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*)	●

	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
Advanced Data Protection for Cloud Applications Integration with the CASB Security Suite provides for advanced DLP policies to protect data at rest in cloud applications, as well as data as it moves to and from sanctioned cloud applications	Add-on	Add-on (limited*)	Add-on
Data Classification Labeling An additional add-on for the DLP Suite or CASB Security 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 Web DLP module, or 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 Integrate with SSO providers like Okta or Ping Identity to enforce even stronger identity-based access controls	●	●	●
Advanced User Behavior Analysis The add-on Dynamic User Protection product based in the Forcepoint cloud provides deep behavioral analysis to allow automatic adjustment of policy enforcement based on changes to the level of risk that an individual user exhibits	Add-on	Add-on	Add-on

*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 the highest number of private peering partnerships with tier 1 networks among web security vendors. 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, CSA STAR, SOC 1, and SOC 2.
- 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

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

[FP-Web-Security-Brochure-EN] 05Jan2021