



# **FORCEPOINT Web Security**

**FORCEPOINT'S CLOUD AND ON-PREMISES WEB SECURITY**





# Forcepoint Web Security

## FORCEPOINT'S CLOUD AND ON-PREMISES WEB SECURITY

Your business and its data are under constant attack. Traditional security solutions no longer provide sufficient protection. In fact, they can put you at risk for data loss and litigation. Protecting your network and data against advanced threats, crypto-ransomware and exploit kits are crucial for the survival of your business in an increasingly risky mobile and cloud-connected digital world.

### Customizable with the option to expand

Companies need customizable solutions that communicate together to protect against these types of 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 single, consistent security controls that can protect against inbound and outbound threats with even the smallest of security teams.

### 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).



**“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**



# Forcepoint Web Security goes beyond anti-virus defenses via eight defense assessment areas

## Forcepoint Web Security

### Real-Time Analysis for Advanced Threat Protection

Forcepoint Web Security goes beyond anti-virus defenses via eight defense assessment areas, using a composite scoring process with the Forcepoint ACE predictive analysis. Multiple real-time content engines analyze full web page content, active scripts, web links, contextual profiles, files and executables.

### 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.



## Enhanced Protection Modules

### 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.

### Cloud Access Security Broker (CASB)

#### Extend full CASB functionalities to complement existing ability to gain visibility into what cloud applications are being used

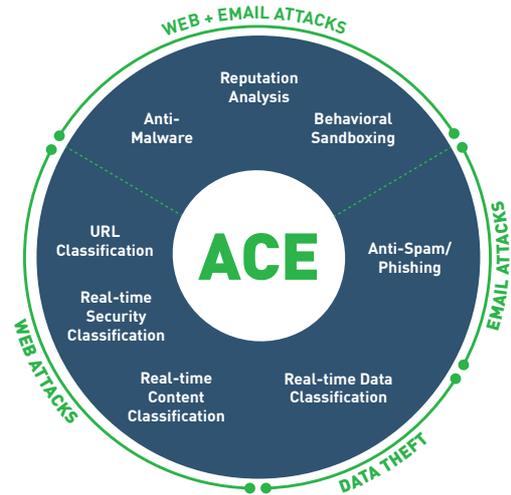
These full CASB functionalities can be used to control cloud applications for inline (proxy) deployments, and easily extended from the web security gateway.



# The power behind Forcepoint solutions

## Forcepoint ACE

Forcepoint ACE provides real-time, inline contextual defenses for web, email, data and mobile security by using composite risk scoring and predictive analytics to deliver the most effective security available. It also provides containment by analyzing inbound and outbound traffic with data-aware defenses for industry-leading data theft protection. Classifiers for real-time security, data and content analysis — the result of years of research and development — enable ACE to detect more threats than traditional anti-virus engines every day (the proof is updated daily at <http://securitylabs.forcepoint.com>). ACE is the primary defense behind all Forcepoint solutions and is supported by the Forcepoint ThreatSeeker Intelligence Cloud.



**Integrated set of defense assessment capabilities in 8 key areas.**

- ▶ 10,000 analytics available to support deep inspections.
- ▶ Predictive security engine sees several moves ahead.
- ▶ Inline operation not only monitors, but **blocks** threats.

## Forcepoint ThreatSeeker Intelligence

The Forcepoint ThreatSeeker Intelligence, managed by Forcepoint Security Labs, provides the core collective security intelligence for all Forcepoint security products. It unites more than 900 million endpoints, including inputs from Facebook, and, with Forcepoint ACE security defenses, analyzes up to 5 billion 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. The 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 Security Labs researchers. The powerful result is a single, unified architecture with one unified user interface and unified security intelligence.

## Other Capabilities

- ▶ **Remote User Protection.** Manage corporate, branch and remote users with one console and policy with Hybrid Cloud deployment.
- ▶ **Flexible SSL Inspection.** Granular SSL inspection capabilities let you monitor HTTPS traffic while maintaining privacy and regulatory requirements.
- ▶ **API for Threat Intelligence.** Ingest Published API makes your web security smarter by incorporating industry or region-specific threat intelligence and enables security management automation.
- ▶ **Application and Protocol Control.** Network Agent provides granular control over hundreds of protocols and applications for an enhanced security posture.
- ▶ **Flexible Reporting.** Four customizable dashboards, as well as more than 60 pre-defined and customizable reports, provide easy-to-read business and technical information as well as valuable insights into threat levels and more.
- ▶ **Multiple Deployment Options.** Choose from deployment with Cloud, hybrid or on-premises appliance (virtual or physical).
- ▶ **Proxy-Less Endpoint Protection.** Our solution protects users working in any network, anywhere. Applications continue to work in environments that typically cause problems with proxy based cloud solutions.
- ▶ **Integrated DLP Incident Risk Ranking.** Industry's first security analytics capability, lowers cost and increases efficiency of DLP investigations.
- ▶ **Expanded Internet Access for Roaming Users.** Apply different policies when an employee connects from corporate and non-corporate locations (i.e. video streaming allowed when at home, blocked when at a registered corporate location).
- ▶ **Cloud App Control.** Block the use of unsanctioned cloud applications while permitting the use of those deemed organization-approved. Easy to add full CASB capabilities to accommodate web security solutions to provide control for cloud applications for inline (proxy) deployment mode.
- ▶ **Web Security Cloud Migration tools.** Upgrade from Forcepoint's leading on-premises appliances to the industry's most secure cloud, Forcepoint Web Security Cloud.



## ABOUT FORCEPOINT

Forcepoint is transforming cybersecurity by focusing on what matters most: people's behavior as they interact with critical data and systems. This human-centric approach to cybersecurity frees employees to innovate by understanding the normal rhythm of user behavior and the flow of data in and out of an organization. Forcepoint behavior-based solutions adapt to risk in real time and are delivered via a converged security platform to protect network users and cloud access, prevent confidential data from leaving the corporate network, and eliminate breaches caused by insiders. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.

[www.forcepoint.com/contact](http://www.forcepoint.com/contact)

©2019 Forcepoint.

[BROCHURE\_FORCEPOINT\_EMAIL\_SECURITY\_EN] 400002.040919



**Australia & New Zealand Reseller**

[www.witzcybersecurity.com](http://www.witzcybersecurity.com)

[support@witzcybersecurity.com](mailto:support@witzcybersecurity.com)