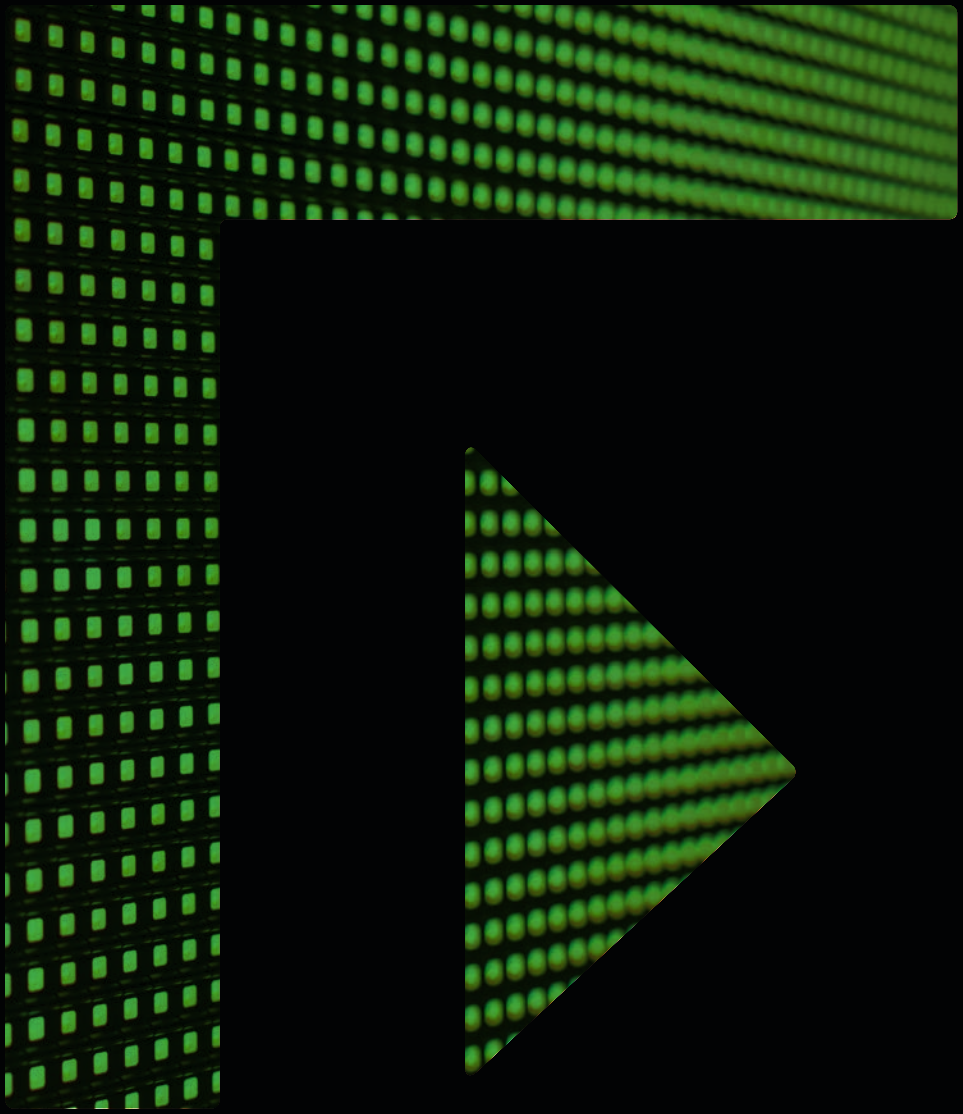


Forcepoint Email Security

FORCEPOINT'S CLOUD AND ON PREMISE EMAIL SECURITY

FORCEPOINT
POWERED BY Raytheon

Forcepoint Email Security

FORCEPOINT'S CLOUD AND ON PREMISE EMAIL SECURITY

Most large scale cyberattacks originate from email, using advanced, coordinated tactics, such as socially engineered lures and targeted phishing. As these multi-stage threats blend web and email elements throughout attacks, they present a "Kill Chain" of opportunities to stop them before the breach occurs.

Maximize your use and safety of email

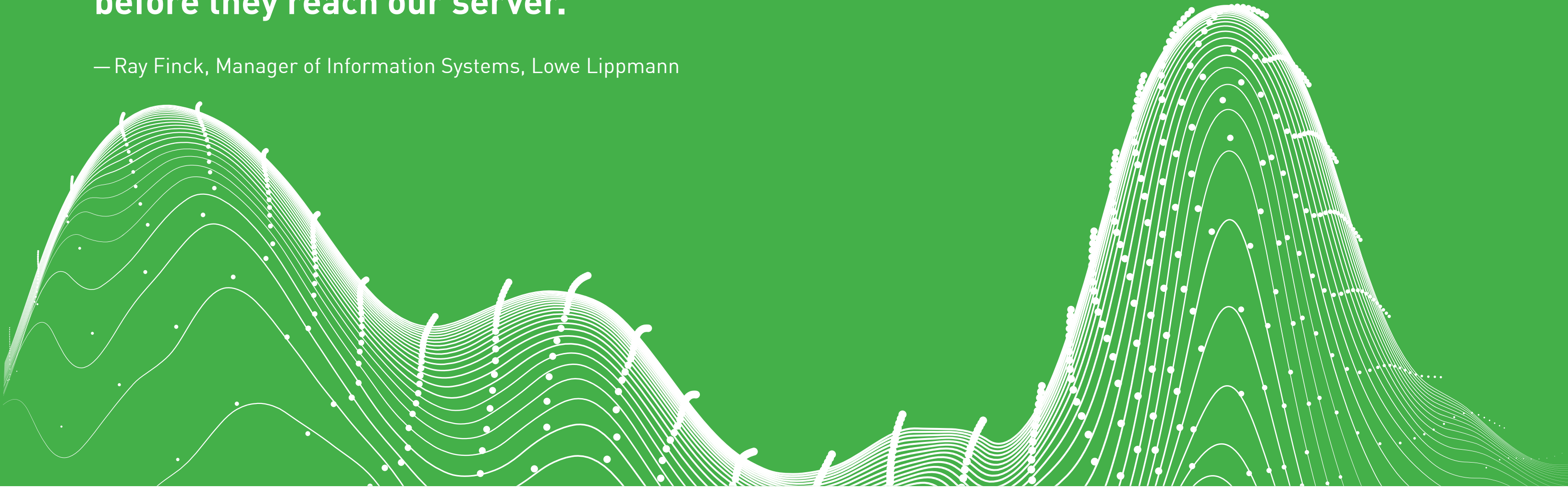
Forcepoint Email Security identifies targeted attacks, high-risk users and insider threats, while empowering mobile workers and the safe adoption of new technologies like Office 365 and Box Enterprise.

From inbound attack activity to outbound data theft or botnet communication attempts, Forcepoint Email Security secures mixed environments with content aware defenses, protecting email communications as part of a complete and connected defense system against Advanced Persistent Threats (APTs) and other types of advanced threats.

Email security challenges

- APTs commonly use email for early stages in their advanced attacks.
- Email must do more to address data theft and insider threats.
- Businesses are adopting Office 365 and other cloud-based services to expand and compete.
- Risky user habits can easily lead to security breaches and data loss.

> "Ultimately, we are very happy with the Forcepoint products. Forcepoint Email Security is doing its job and stopping any problems before they reach our server."
>
> — Ray Finck, Manager of Information Systems, Lowe Lippmann



Forcepoint Email Security capabilities

STOP APT AND OTHER ADVANCED TARGETED THREATS

Forcepoint's Advanced Classification Engine (ACE) is at the heart of all Forcepoint solutions. ACE identifies malicious lures, exploit kits, emerging threats, botnet communications and other advanced threat activity across the Kill Chain. This enables Forcepoint Email Security to identify the early stages of an attack. It can even identify Zero-day malware threats using powerful assessment capabilities that include fully-integrated, file behavioral sandboxing.

SECURE SENSITIVE DATA AGAINST EXTERNAL ATTACKS AND INSIDER THREATS

To prepare for a malicious insider threat or the potentially successful cyberattack, it's vital that outbound communications be monitored. This is also necessary both for data theft compliance needs as well as for business requirements. Only Forcepoint provides the technology to stop data infiltration and exfiltration with capabilities such as:

- OCR (Optical Character Recognition) scanning to identify sensitive data hidden in images such as scanned documents or screen shots.
- Encrypted file detection to recognize custom encrypted files designed to defy identification.
- Drip data loss prevention (DLP) monitoring to identify where sensitive data is leaked in small quantities over time.
- Advanced analysis of malicious files and macros typically embedded in with MS Office files.

SAFELY ADOPT CLOUD TECHNOLOGIES LIKE OFFICE 365 AND BOX ENTERPRISE WHILE SUPPORTING A MOBILE WORKFORCE

IT departments are strained to maintain current systems while supporting an increasingly mobile workforce and the demands to adopt new technologies like Office 365. Forcepoint Email Security provides industry-leading capabilities that leverage systems and other information to control communications, such as preventing total access to sensitive email attachments on vulnerable mobile devices, while permitting full access on fully-secured laptops. These inbound and outbound defenses are all supported on Office 365.

IDENTIFY "HIGH-RISK" USER BEHAVIOR AND EDUCATE USERS TO IMPROVE AWARENESS

The rich data collections in Forcepoint Email Security are used by a number of policies to report and identify systems that may require special IT attention. They generate a report on Indicators of Compromise to identify infected systems, and more proactive reports on suspicious behavior, including potential insider threats, such as "disgruntled employee" activity. User feedback capabilities educate employees as mistakes are made, helping them to better learn and understand safe email best practices.

Enhanced Protection Modules

OPTIONAL HYBRID CLOUD DEPLOYMENT

Leverage Forcepoint's global cloud services for performance and scalability
Combine on premise threat defenses with cloud-based pre-filtering services to preserve bandwidth with industry-leading anti-spam SLA's. The hybrid module adds URL Sandboxing and Phishing Education to the Email Security solution.

EMAIL DLP

Block data theft with enterprise-class content-aware DLP
Prepare for the insider threat and malware data theft, achieve compliance goals and further mitigate risks to personal information or IP. Advanced capabilities detect data theft concealed in images or custom-encrypted files, even when transmitted in small amounts over time to evade detection.

CLOUD SANDBOX

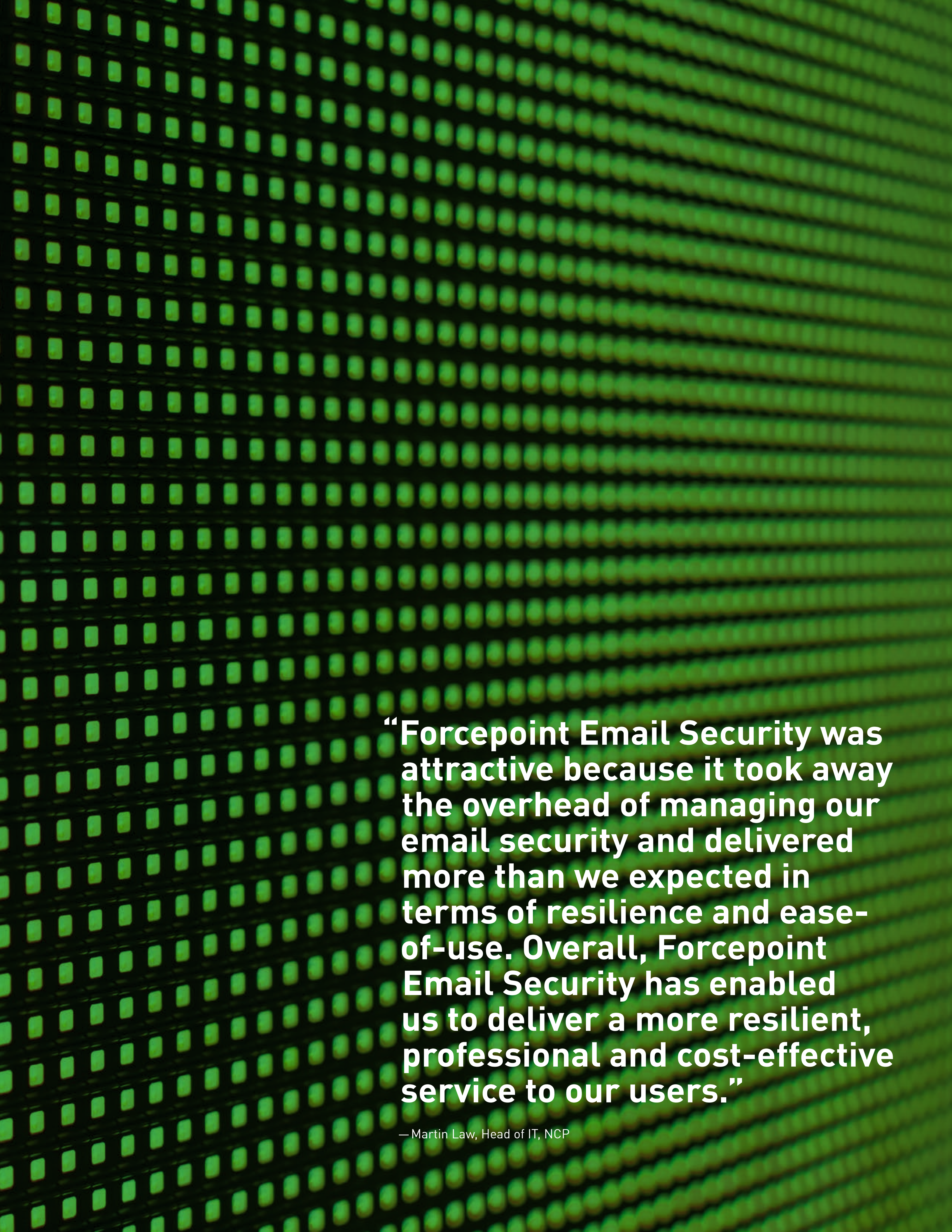
Integrate behavioral sandboxing for automatic and manual analysis of malware files
Supplement Forcepoint ACE analytics with an integrated file sandbox for additional deep inspection. Take advantage of behavioral analysis in a virtual environment to uncover the malicious behavior of Zero-day and other advanced malware. Test files automatically or manually to generate detailed forensics.

EMAIL ENCRYPTION

Ensure the confidentiality of sensitive communications
The Forcepoint Email Encryption Module is a policy-driven technology that enables secure delivery of email communications. It eliminates the traditional barriers of cost and complexity by offering easy administration, without complex key management or additional hardware.

IMAGE ANALYSIS

Identify explicit images to enforce acceptable use and compliance
The Forcepoint Image Analysis Module allows employers to take proactive measures to monitor, educate and enforce company email policy with regard to explicit or pornographic image attachments.



> “Forcepoint Email Security was attractive because it took away the overhead of managing our email security and delivered more than we expected in terms of resilience and ease-of-use. Overall, Forcepoint Email Security has enabled us to deliver a more resilient, professional and cost-effective service to our users.”
>
> — Martin Law, Head of IT, NCP

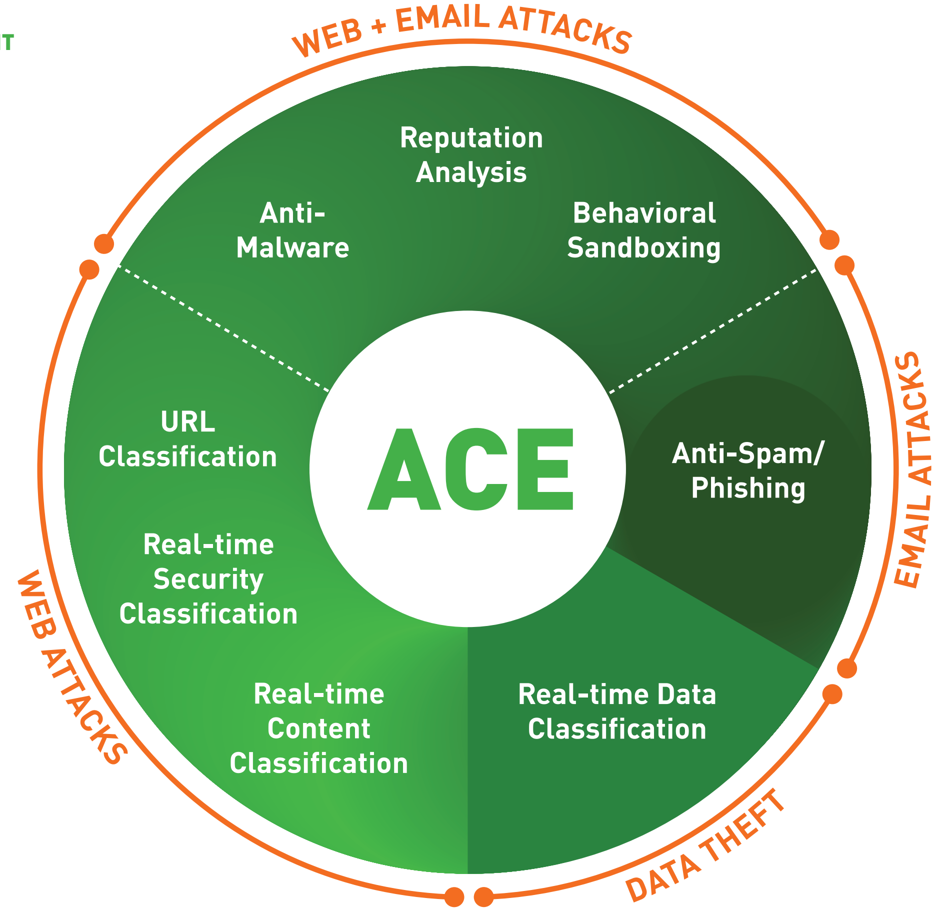
The power behind Forcepoint solutions

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 (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.

INTEGRATED SET OF DEFENSE ASSESSMENT CAPABILITIES IN 8 KEY AREAS.

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



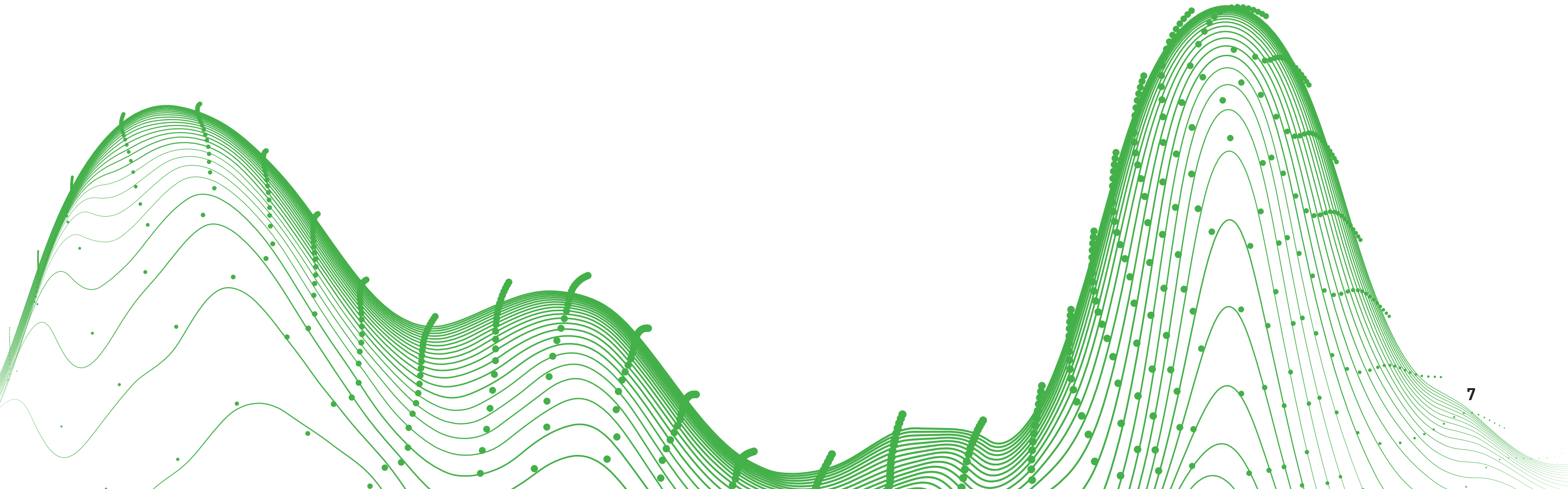
Forcepoint ThreatSeeker Intelligence

The Forcepoint ThreatSeeker Intelligence, managed by Forcepoint Security Labs, provides the core collective security intelligence for all Forcepoint security products. Together with Forcepoint ACE security defenses, Forcepoint ThreatSeeker Intelligence analyzes up to 5 billion requests per day, and unites more than 900 million endpoints, including those from Facebook.

This expansive awareness of security threats enables Forcepoint ThreatSeeker Intelligence to offer real-time security updates that block Advanced Threats, malware, phishing attacks, lures and scams, while simultaneously providing 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, Forcepoint ThreatSeeker Intelligence helps reduce your exposure to web threats and data theft.

TRITON Architecture

With best-in-class security and a unified architecture, TRITON Architecture 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.



CONTACT
www.forcepoint.com/contact

FORCEPOINT
POWERED BY Raytheon