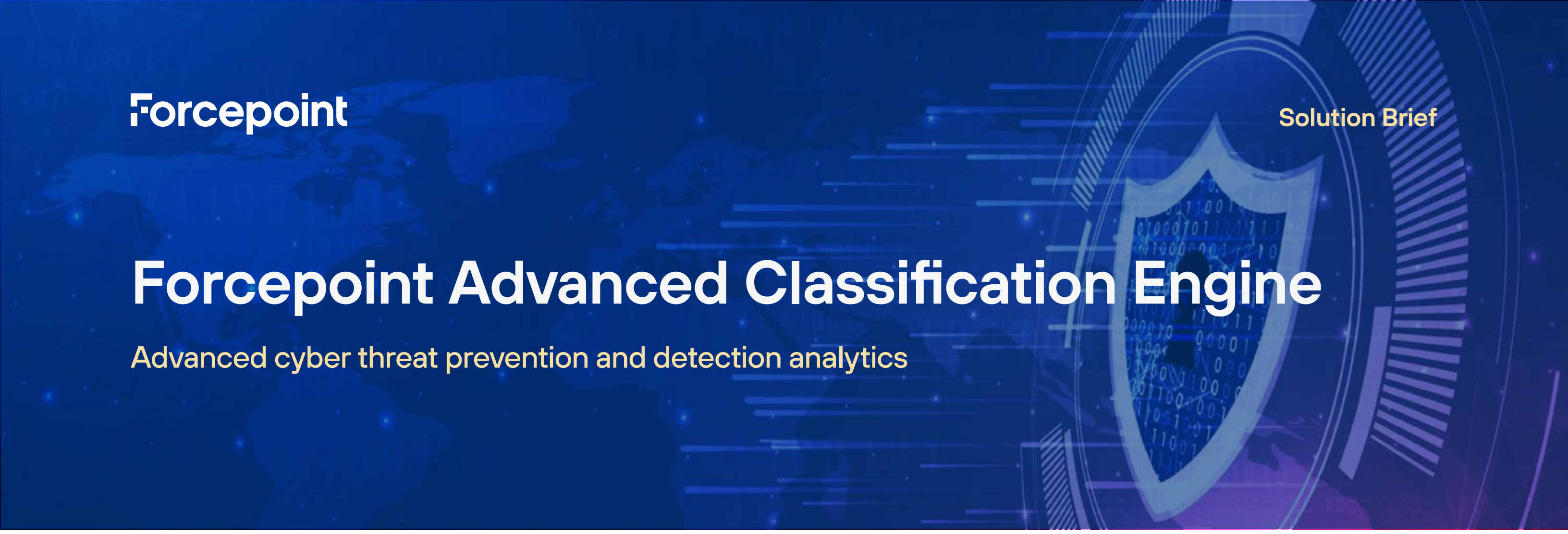


Forcepoint

Solution Brief

Forcepoint Advanced Classification Engine

Advanced cyber threat prevention and detection analytics

What is ACE?

- ACE is a suite of cyber threat prevention and detection analytics embedded into multiple Forcepoint solutions such as Forcepoint Web Security, Forcepoint Email Security, Forcepoint Next Generation Firewall (NGFW), and Forcepoint DLP (Data Loss Prevention).
- Forcepoint ACE, designed to offer a layered approach to cybersecurity, achieves defense-in-depth by using multiple methods to counter a given threat type. These various methods are grouped into specific defense assessment areas, and are made up of a unique blend of traditional and modern approaches to threat detection and prevention.
- Our set of anti-malware analytics are 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
- To protect against the most advanced threats, our Advanced Malware Detection & Prevention (AMDP) module offers the ultimate layer of defense through behavioral sandboxing.

Forcepoint's Advanced Classification Engine (ACE) stacks multiple threat detection and prevention capabilities to provide defense in depth against cyber threats. Hackers are continually creating more sophisticated attacks, so Forcepoint's X-Labs team is always innovating to keep defenses like ACE a step ahead of threat actors and give our customers the best hand at stopping cyber threats.

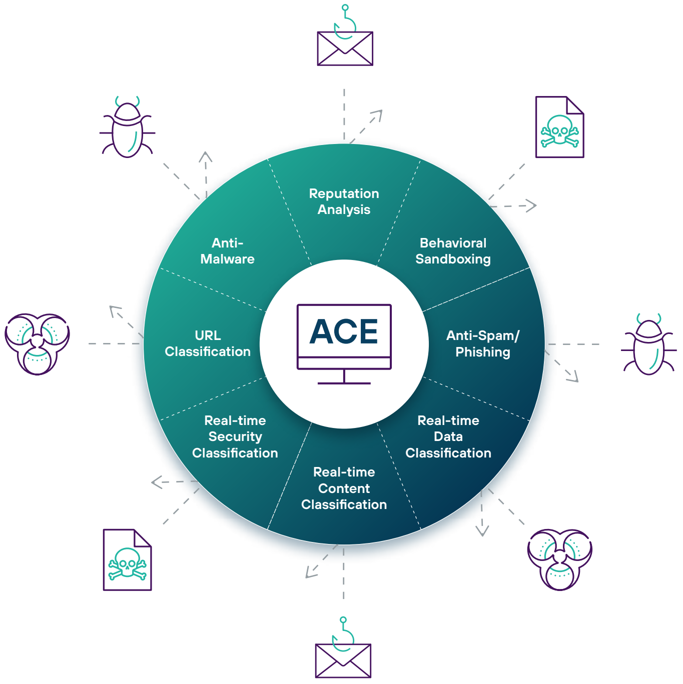
ACE supports Forcepoint's data-centric approach to cybersecurity by providing detailed, real-time categorization of content to enable a rich picture of the context surrounding cyber behavior and thus, more accurate determinations of risk. This enables the granularity of policy controls necessary to stop cyber threats in all their various forms, while still allowing users the freedom they need to carry out their work easily and effectively. ACE is able to gain the insights critical to enabling true defense in depth and in breadth. This is accomplished through a layered and modular approach to threat prevention based on analytics that understand normative versus anomalous cyber behavior, the disposition of web and email traffic, and the types of data moving around the enterprise. The different defense assessment areas within ACE share what they've learned with each other, allowing threat intelligence gained from one attack vector to influence analytics applied to another attack vector. For example, knowledge of a URL embedded within an email message benefits both the Web Security solution and the Email Security solution.

A user's intentions can change over time. Credentials can become compromised. Files and executables can start out benign and then later be manipulated to become malicious. A static, after-the-fact security approach will fail to do anything to stop these threats. It is imperative to have inline operation with evaluations done in realtime in order to be proactive, identify potential compromise at the outset, and stop malicious activity before critical data is put in jeopardy.

How Does It Work?

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. Each defense assessment area, and each underlying analytic, is purpose-built to offer the highest efficacy and efficiency for 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.

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. This improves threat defenses by identifying and classifying information crossing your environment to deliver real-time security classifications. Forcepoint ACE achieves optimum security efficacy and efficiency while also providing checks and balances to ensure accurate classification.


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

1. **Real-Time Security Classification.** Inspects all traffic content for malicious or suspicious code such as obfuscated scripts and iframe tags that often hide malware behind dynamic content.
2. **Real-Time Content Classification.** Employs advanced machine learning to quickly and accurately classify web pages into highly granular content categories for effective access filtering.
3. **URL Classification.** Applies current classification information for known web pages, and assesses new pages and links based on associated sites and redirections.
4. **Behavioral Sandboxing.** Allows suspicious files to be executed and evaluated for malicious activities in a secure sandbox which emulates a real machine
5. **Anti-Malware Engines.** Applies state-of-the-art antimalware protection capable of proactively blocking the latest in binary and script-based threats.
6. **Anti-Spam/Phishing.** Provides proactive protection against high volume spam and Phishing campaigns, as well as email-borne threats.
7. **Reputation Analysis.** Reputation databases (both third-party and Forcepoint proprietary) are applied to emails and URLs to block web and email traffic from untrustworthy sources.
8. **Real-Time Data Classification.** Classifies structured and unstructured data with parsing and decoding support to address outbound data theft.

ThreatSeeker Intelligence

Forcepoint ThreatSeeker Intelligence aggregates threat intel from ACE engines, firewalls, and endpoints deployed around the world to provide telemetry back to those devices, and provide continuous efficacy measurements as well as improvements. ThreatSeeker ingests global input from more than 130 countries and analyzes billions of requests per day to understand the efficacy of any given analytic at any given time. By working in concert with ThreatSeeker, ACE is able to counter the latest, most innovative threats just as well as known threats. ThreatSeeker collects content in all its online forms: web pages, documents, executables, scripts, streaming media, emails, mobile applications, and other Internet traffic. It processes billions of pieces of email and web traffic intelligence daily to uncover new trends in threats and identify further types of content to collect. As it operates, Forcepoint ThreatSeeker Intelligence:

→ Monitors popular websites to see if they've been compromised or hijacked

→ Follows breaking news, trending topics, and viral social media to identify additional content to assess

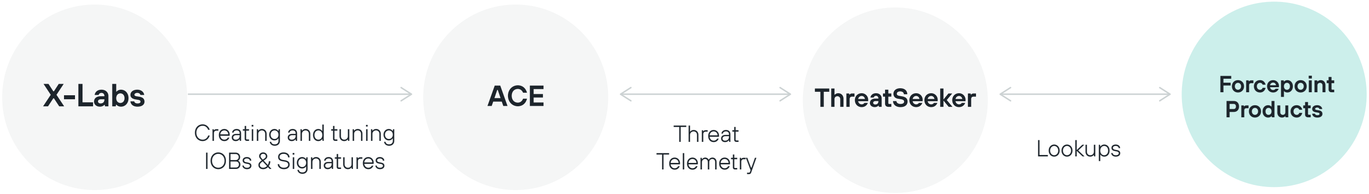
→ Tracks geographical hot spots, newly registered domains, and other potentially revealing internet activity

Synergy of ACE, X-Labs, and ThreatSeeker

In order to understand the full power of ACE it is important to consider how Forcepoint X-Labs, ACE, and ThreatSeeker Intelligence work together in a dynamic way to perpetually update our threat and risk mitigation tools so they're fully equipped to counter the latest, most advanced threat innovations.

The analytics used within ACE are maintained and tuned by Forcepoint X-Labs, our global team of threat researchers, data scientists, and engineers. ThreatSeeker informs ACE with directly actionable updates by continually collecting content and new trends, and this data allows X-Labs researchers to further optimize data models and analytics on an ongoing basis.

ACE, X-Labs, and ThreatSeeker Working Together

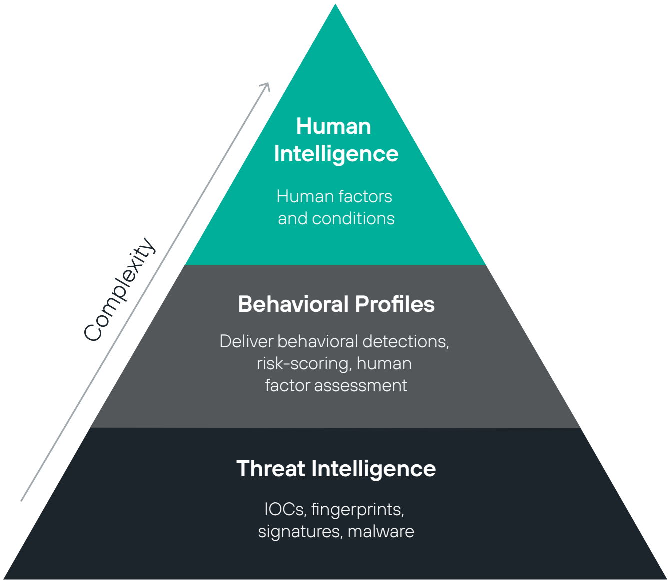


X-Labs is fundamental not just to ACE, but to all Forcepoint solutions.

X-Labs is fundamental not just to ACE, but to all Forcepoint solutions. X-Labs delivers behavioral analytics for Forcepoint's products and services which enable them to operate in a predictive rather than reactive fashion, ultimately containing threats and abuse before harm is caused. Leveraging these behavioral analytics, Forcepoint provides converged solutions to rapidly identify compromised users and automate protections. In this way, our customers can take action before a data breach occurs, stopping critical data theft, compromised users, regulatory violations, and other damages resulting from intentional or unintentional behaviors.

The experts at Forcepoint X-Labs continuously fine-tune the analytics used within ACE using a mix of both automated and manual (human expert) means. Automated methods are essential to process the volume of threat telemetry received through Forcepoint ThreatSeeker every day, while human experts are essential to creating and maintaining the most accurate inference engines. Machine learning algorithms and statistical analysis methods are used to ensure that ACE remains predictive, proactive, and relevant to our customer's needs. X-Labs researchers continually analyze the cyber threat landscape, identifying new attacker tactics, techniques, and procedures (TTP), and new Indicators of Compromise (IoC). Their findings are translated into analytics within ACE to offer enhanced threat prevention capabilities.

X-Labs in One View


Complexity
Human Intelligence
Human factors and conditions
Behavioral Profiles
Deliver behavioral detections, risk-scoring, human factor assessment
Threat Intelligence
IOCs, fingerprints, signatures, malware

Benefits:

- → Identify and mitigate risk **before** damage is done
- → **Anticipate** malicious activity
- → Shifting analyst time away from analyzing events to letting them focus on **high risk identities**

Conclusion

Forcepoint has shifted the paradigm in cybersecurity with a data-centric philosophy that is manifested across the full product portfolio through the efforts of X-Labs. ACE and ThreatSeeker are perfect examples of the application of a data-centric cybersecurity philosophy, interpreting the context of digital behavior to identify anomalous or suspicious behavior. Just as ACE takes a layered approach in order to attain superior efficacy and efficiency, building a risk mitigation program that layers the full breadth of Forcepoint solutions can equip your organization to counter malicious behavior before a data breach occurs, achieve superior external threat protection, and stop the most advanced cyber threats from the most sophisticated adversaries.

To get the latest research from Forcepoint X-Labs, **visit our Forcepoint X-Labs blog.**

forcepoint.com/contact