Advanced Persistent Threat Mitigation

hCaptcha Enterprise detects Advanced Persistent Threats (APTs) through its proprietary machine learning technologies, even if the attack is conducted across millions of IPs and thousands of devices.

APT Mitigation is hCaptcha's suite of extended features that include: Coordinated Attack Protection, Custom Threat Models, and After-the-Fact Alerts. These features are paired with our semi-managed SOC Monitoring Service to address the most sophisticated and persistent threat actors for unparalleled protection.

Detect and Defeat APTs

hCaptcha's APT Mitigation is built on an advanced feature-set that analyzes traffic to effectively detect malicious activity and APTs.

Using the latest machine learning technologies, fed by our continuous global intelligence, hCaptcha Enterprise's APT Mitigation automatically learns and identifies new threats and malicious traffic patterns, as well as escalating suspicious cases to the hCaptcha SOC team for further review and immediate countermeasures.

Why APTs Are Difficult to Detect

- Attacks are slow, methodical, and cautious as opposed to smash and grab assaults that are easily detected.
- The bots used are often proficient at imitating human behavior, and in some cases even replay the real user's mouse movements when captured from a compromised device.
- APTs frequently hide their identities behind residential IP networks, compromised corporate networks, and peer-to-peer proxies.
- Attackers spoof behaviors and user agents to impersonate other users or devices.
- Advanced techniques imitate legitimate browser activity, even storing individual cookies at scale to retain identities and status.
- Strong funding (often state sponsored) enables constant innovation; deterring APTs requires continuous adaptation.

This greatly reduces the workload on defenders, and significantly improves an organization's ability to guard against new and existing APT attacks like the following:

- Compromised 2FA User Logins.
- Sophisticated Low-Volume Distributed Account Takeover Attempts
- Fraudulent New Account Creation, Including Privileged Accounts
- Unauthorized Changes to Access Privileges
- Malware Insertion
- Ransomware Attacks
- Theft of IP and other Data Mining
- Personal or Financial Data Harvesting

Coordinated Threat Protection

hCaptcha's APT Mitigation uses a unique and innovative technology called Coordinated Attack Protection that identifies and groups APT related traffic, connections, and processes—even when occurring across different time-frames, software platforms, and attack methodologies.

In an attempt to identify and correlate seemingly different sessions and incidents with a single threat actor, legacy systems rely on IP addresses, user IDs, behaviors, and device fingerprints. But relying directly on these identifiers is problematic. IPs and user IDs are frequently spoofed and pure behavioral signatures are quite unstable. This results in high false-positive rates, especially when most people access services through multiple devices. Because APTs often use thousands of different, rapidly changing machines via cloud services or compromised residential botnet devices, the value of device fingerprints in sustained detection is also limited.

Coordinated Attack Protection uses Scoped UIDs that transcend these legacy identifiers. By using additional signatures derived from advanced machine learning techniques, Scoped UIDs are better equipped to identify and group all malicious connections, sessions, and incidents that are related to a common APT while maintaining user privacy because they do not link across sites.

Coordinated Attack Protection provides numerous benefits:

- Identify related security incidents and attacks that would otherwise be difficult to ascertain.
- Trace malicious deeds back to a single actor (or group), even when using multiple IPs, IDs, devices, and methodologies; or, when attacking different systems or applications.
- Detect malicious traffic that contains randomized IP addresses, headers, and user agents, and identify the APTs connected with it.
- Associate APT related activity with compromised users and specific devices, even after-the-fact.
- Discover at-risk accounts and sessions.
- Quickly mitigate account takeovers, credential stuffing, and other attacks, even if detection occurs after the action succeeds.

Effective APT mitigation without sharing excessive PII or compromising the user experience is not easy, but hCaptcha Enterprise proves that it is possible.

Custom Threat Models

The hCaptcha platform continuously learns and automatically adapts to new APT threats. But, when organizations are faced with unique situations and use-cases, they can leverage custom threat models to meet their needs.

For example, when specific attackers are known, or a business partner has a high volume of requests, organizations can easily modify associated parameters to handle these special cases.

Risk Insights

Risk Insights lets you analyze your traffic along a multitude of dimensions, and easily add your own business logic to tune sitekey risk models.

Whether targeting persistent threat actors, inauthentic human behavior, or fraud rings, this kind of traffic often shares common features that make it easily targetable by writing a Rule using Risk Insights dimensions, whether or not it is automated.

Threat X-Ray

Threat X-Ray gives you visibility into your traffic across many dimensions to provide you with the information needed to make informed decisions - whether to give the green light to the traffic, halt it in its tracks, or devise custom rules to address particular or similar anomalies.

Anomaly Alerts

Anomaly Alerts will notify you of potential threats and unexpected traffic surges. Our system is discerning, capable of distinguishing between benign and concerning anomalies. This means you only receive alerts when it really matters.

Retrospective Alerts

It's common for bad actors to compromise an account, and return to it later to carry out their attack. In some cases they may be connecting from the real user's machine when it has been compromised. This is especially true in APT scenarios.

Through hCaptcha's continuous analysis and applied machine learning, patterns emerge that identify and provide details about an APT attack in progress - for instance, compromised accounts. Organizations can use these retrospective alerts to respond before any major damage has occurred.

Retrospective alerts are immediately actionable, and increasingly valuable given the rising sophistication of APTs.

Semi-Managed SOC Monitoring

With our integrated APT SOC Monitoring Service, customers also directly benefit from our 24/7 in-house team of APT experts.

These specialists actively monitor your unique traffic needs, tune and optimize hCaptcha's features, help monitor your implementation for threats you might miss, and provide the knowledge and experience needed to provide maximum protection from APTs.

When threats do arise, our experts will work closely with your team to rapidly respond to the most sophisticated and persistent attacks.

APT Mitigation - More Than Just Bot Detection

By utilizing hCaptcha's APT Mitigation features, organizations can dramatically increase their defenses, and are better prepared to detect and respond to today's relentless and sophisticated attacks. Additionally, organizations that take advantage of our SOC Monitoring Service can rest assured that they have qualified experts directly at their disposal - ready to help optimize defenses and respond to attacks that do occur.

For example, when specific attackers are known, or a business partner has a high volume of requests, organizations can easily modify associated parameters to handle these special cases.

- **Extreme Performance and Scalability** - hCaptcha is multi-cloud on the CDN edge–reliably and efficiently scaling to millions of requests per minute.
- **Global Solution** - The service and dashboard is localized to 110 languages and works in every country. hCaptcha is also fully compliant with WCAG 2.1 and Section 508 to ensure accessibility.
- **Works Immediately** - hCaptcha starts working instantly. Its advanced machine learning uses your data and traffic patterns to automatically and continuously train, tune, and select the best model settings for optimum security and performance.
- **Easy Installation** – Available as a hosted service, your organization can quickly be up and running.