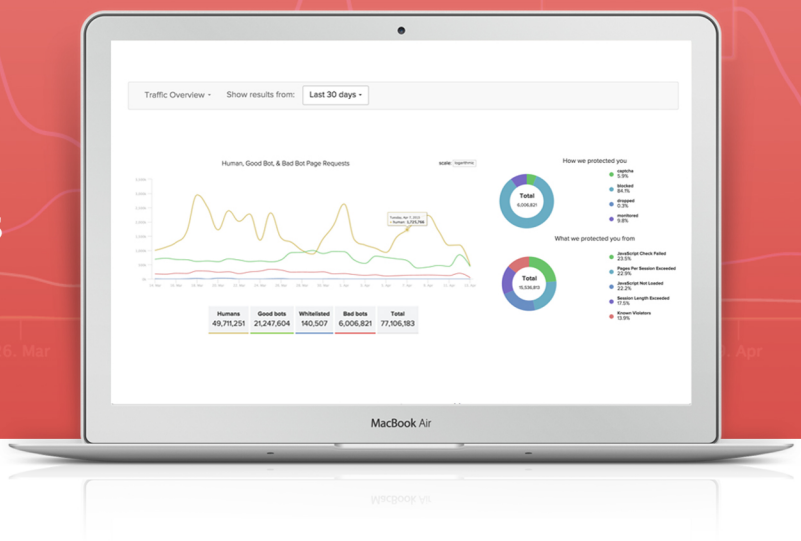
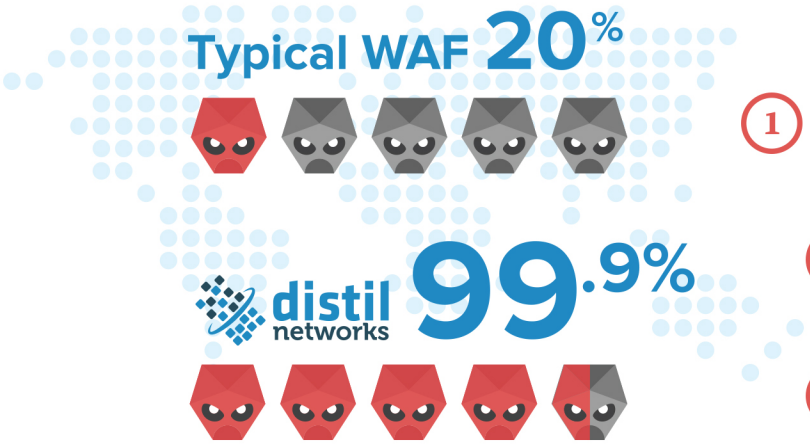
The first easy and accurate way to defend websites against malicious bots.



Distil Networks protects your website from fraud, brute force attacks, web scraping, account hijacking, unauthorized vulnerability scans, spam, and man-in-the-middle attacks. Slash the high tax that bots place on your internal teams and web infrastructure by outsourcing the problem to the team with a maniacal focus on blocking malicious bots.



1. Harden your website security by eliminating malicious bots
2. Protect data from web scrapers, unauthorized aggregators and competitors
3. Increase insight and control over human, good bot and bad bot traffic
4. Deploy on the Distil Cloud CDN or Distil Appliance (Physical | Virtual | AWS)

Trusted by the world's most successful websites

TravelBrands · Aol. · StubHub! · Thomson Reuters · Dowjones · yellowbook · B&H Photo Video Pro Audio · easyJet · glassdoor · Discount Tire · skyscanner · Purch

"Distil Networks' service sounded like the stuff of magic. It has proven to be so."

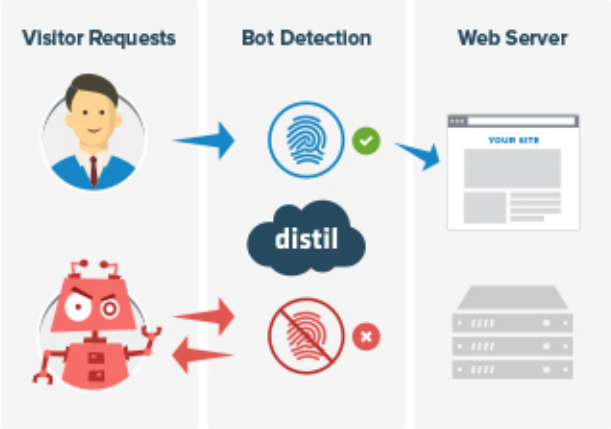
Kurt Freytag
Head of Product & Engineering
CrunchBase

ACCURATE PROTECTION

Firewalls, WAFs, and IDS systems were never designed to stop and manage the volume, variety and sophistication of today's bots and botnets. The Distil Difference? Ease-of-use and accuracy. Distil's self-optimizing protection blocks 99.9% of malicious bots without impacting legitimate users. Quickly fine-tune your own settings, and enjoy complete control over how you manage bots and use the service.

Inline Fingerprinting

Analyzes over 40 bits of information from each client request. Fingerprints stick to the bot even if it attempts to reconnect from random IP addresses or hide behind an anonymous proxy.



Known Violators Database

Real-time updates from the world's largest Known Violators Database of bad bot fingerprints is based on the collective intelligence of all Distil-protected sites. In addition, Distil curates real-time threat intelligence feeds from third party fraud, spam, malware and proxy lists-- all of which is updated and used to protect customers in real-time.

Behavioral Modeling and Machine Learning

Machine-learning algorithms pinpoint behavioral anomalies specific to your site's unique traffic patterns. Distil also proactively predicts a bot based on correlating dozens of dynamic classifications. This is in stark contrast to the reactive approach inherent in web application firewalls that depend on static rules such as rate limiting.

Browser Validation

Distil validates a browser is exactly what it claims to be, and deep interrogation makes sure the browser is being used by a human not a bot. Even browser automation tools like Selenium and PhantomJS can't escape Distil's detection.

'Good Bot' Authentication

Validate that good bot requests (Google, Bing, etc.) map to the correct user agent and IP range.

Advanced Rate Limiting

Predictive analytics show you how your traffic will be affected when dialing up or down rate limits such as pages per minute, pages per session, and session length. Distil's rate limits are not restricted to specific IPs, making them much more accurate.

FLEXIBLE DEPLOYMENT

Distil's multiple deployment options don't require changes to your underlying web infrastructure and won't impede current or future integrations.

Distil Cloud CDN

- Deploys in minutes
- Blazing fast Anycast and DNS-based GeoIP Routing
- Automatic content compression optimizes for faster delivery
- Automatically increases infrastructure and bandwidth to accommodate spikes
- 17 datacenters automatically fail over when a primary location goes offline

Distil Appliance

- Deploys in days
- Install on virtualized or bare metal appliance(s)
- High availability configurations with failover monitoring
- Heartbeat up to the Distil Cloud ensures real-time protection from Disti's Known Violators Database