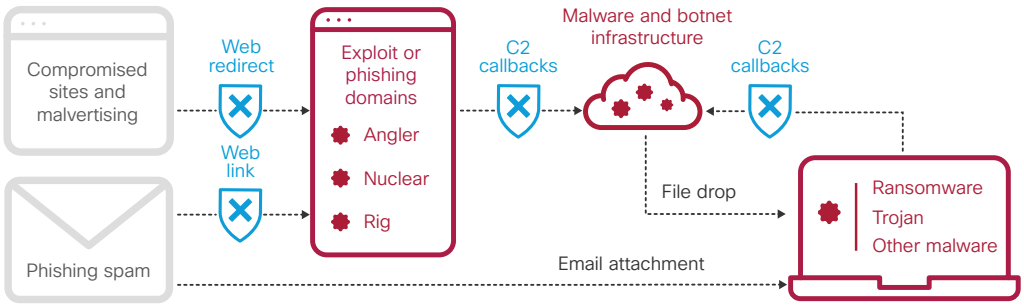
Cisco Umbrella

SOLUTION BRIEF

Nothing kills attacks earlier than DNS-layer security.

Protection both before and during the attack

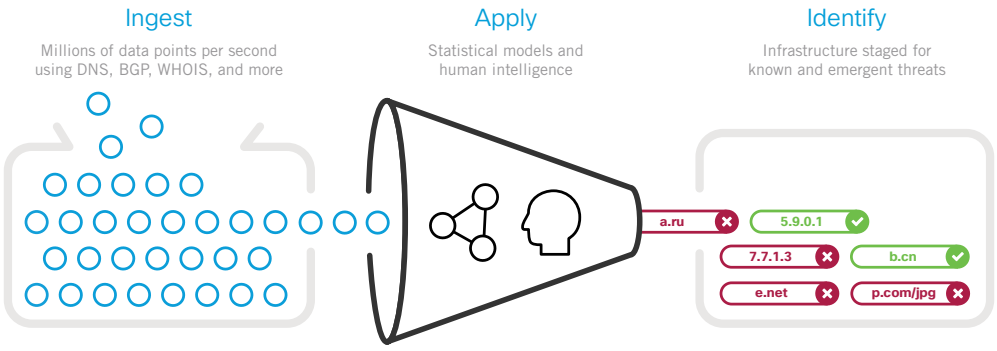
Attacks have many phases. Before launching, the attacker needs to stage internet infrastructure to support each phase. Two early phases are to redirect or link to a malicious web domain or send a malicious email attachment. For the former, most attacks leverage exploit kits (e.g. Angler) as the first stage before dropping the final payload. Cisco Umbrella effectively blocks initial exploit and phishing domains.



Attacks that target organizations often leverage email attachments or direct payload downloads. Yet attacks with an objective to exfiltrate data, still must initiate a command & control callback. Because Umbrella is built into the foundation of the internet, it identifies where these domains and other internet infrastructures are staged, and blocks requests over any port or protocol, preventing both infiltration and exfiltration attempts.

Predict threats before they happen

Similar to Amazon learning from shopping patterns to suggest the next purchase, or Pandora learning from music listening patterns to play the next song, Umbrella learns from internet activity patterns to automatically identify attacker infrastructure being staged for the next threat.



We analyze terabytes of data in real-time across all markets, geographies, and protocols. This diversity provides internet-wide visibility into where threats are coming from, who is launching them, where they call back to, how widespread it is, when was the first and last time we saw it, and much more. We combine human intelligence with 3D visualizations to learn new patterns. Then, we apply statistical models to categorize these patterns, detect anomalies, and automatically identify known and emergent threats.

An internet-wide view of threats

#1	fastest & most reliable DNS with 65M+ daily active users
80B+	daily internet requests or connections
3M+	daily new domain names discovered
60K+	daily malicious destinations identified
7M+	malicious destinations enforced at any given time
80M+	daily malicious requests blocked

Predictive intelligence

Our statistical models predict which domains and IPs will be malicious – often before any other security vendor.

For example, one model uses natural language processing to detect domain names that spoof brand and tech terms in real-time (cs.co/NLPRank).

Another uses sound wave analysis concepts to detect domains that have spikes in their DNS request patterns (cs.co/SPRank).

Block threats before they reach you

Today's security appliances and agents must wait until malware reaches the perimeter or endpoint before they can detect or prevent it. Umbrella is your first line of defense, stopping attacks earlier in the kill chain. By enforcing security at the DNS layer, Umbrella stops threats before they ever reach your network or endpoints. By analyzing and learning from internet activity patterns, Umbrella automatically uncovers attacker infrastructure staged for current and emerging threats, and proactively blocks requests to malicious destinations before a connection is even established or a malicious file downloaded. Umbrella can also stop compromised systems from exfiltrating data via command & control (C2) callbacks to the attacker's botnet infrastructure, over any port or protocol.

Unlike appliances, our cloud security platform protects devices both on and off the corporate network. Unlike agents, the DNS layer protection extends to every device connected to the network – even IoT. Umbrella truly is the easiest and fastest layer of security to deploy everywhere.

Reduce security alerts by 2-10x

Adding Umbrella as the first layer of defense in your security stack will block garden-variety threats that add noise, as well as advanced threats that no one else sees.