Cisco Umbrella

DATASHEET

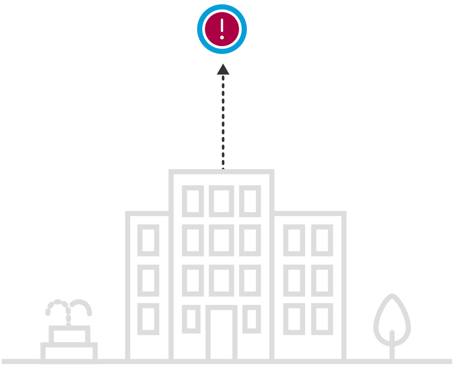
Investigate attacks like never before.

Attackers are pivoting through your infrastructure. What if you could pivot through theirs?

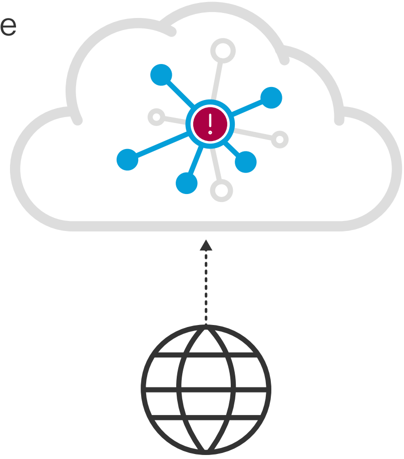
Many security products provide visibility into what's happening on your own network. But do you see what's happening on the whole internet, beyond your perimeter? That's where attackers are staging infrastructure in preparation for launching attacks.

Cisco Umbrella Investigate provides the most complete view of an attacker's infrastructure, and enables security teams to discover malicious domains, IPs, and file hashes, and even predict emergent threats.

Researching security incidents with Investigate



Your view of local traffic to a suspicious domain or IP



Investigate's view of global traffic to associated domains and IPs

How we do it

Begin with a massive, diverse dataset
In 2006, we started building the world's largest internet security network to acquire global intelligence. Today, over 65 million daily active users across 160+ countries point their DNS traffic to our global network – providing visibility into more than 100 billion internet requests every day. Plus, more than 500 peering partners exchange BGP route information with us, which shows us the connections and relationships between different networks on the internet. This massive and diverse set of data gives us a view of the internet like no other security company.

Apply statistical models
To discover patterns and detect anomalies across our data, we design statistical models to categorize and score it. For example:

- Many models analyze spatial relationships, such as graphing the relationships between networks across the internet.
- Some models analyze time-based relationships, such as discovering domain co-occurrences as a result of consecutive DNS requests over very short timeframes, repeated by thousands of users.
- Other models analyze statistical deviations from normal activity, such as measuring the geographic distribution of IP networks requesting a domain name.
- Utilizing natural language processing, the NLP Rank model identifies phishing domains that spoof brand names by analyzing their lexical structure and location on the internet.

By the numbers

- 65 million active enterprise and consumer users daily
- Users from 160+ countries
- 100 billion DNS requests daily
- 500+ peering partners exchange BGP routes with us, which enhances our view of the internet

Combine human intelligence
These models are built and tuned by the Cisco Umbrella security researchers – our team of data scientists, engineers, mathematicians, and security researchers. The Umbrella security researchers leverage 3D visualization, numerous data mining techniques, and security expertise to develop the models and add additional context to the output of the models. They continuously come up with new ways of analyzing the data to find new connections and patterns.

Result: Predictive intelligence
As a result of this analysis, we can accurately identify malicious domains, IPs, networks, and file hashes across the internet, and even predict where future attacks may be staged.

How it helps you

- **See attacks like never before with internet-wide visibility:** Our view into global internet requests shows where attackers are staging infrastructure and how bad, good, or unknown domains, IPs, ASNs, and file hashes are connected.
- **Speed up incident response:** Incident response times can lag when security teams do not have the right context or access to pertinent information early in the investigation. By speeding up incident investigations, you can respond faster and reduce attacker dwell time in your environment.
- **Prioritize incident investigations:** To properly triage incidents, you need to get accurate information and the relevant context quickly. Our unique view of the internet enriches your security event data and threat intelligence with global context to help better prioritize investigations.
- **Use threat intelligence more effectively:** Bolster your outdated, commodity threat feeds with our up-to-the-minute, internet-scale intelligence.

Use Cases

- Speed up investigations
- Stay ahead of attacks
- Prioritize investigations and response
- Enrich security systems with real-time data

How you can use Investigate

Dynamic search engine
Our web-based console gives you real-time access to all of our intelligence and the ability to interactively pivot on different data points during investigations. You can either query Investigate for exact matches to domain names, IP addresses, email addresses, ASNs, and file hashes, or use pattern search for more flexible queries of certain terms, brand names, patterns, and non-exact matches.

RESTful API
Investigate provides API access to bring contextual data into your SIEM, threat intelligence platform, or incident workflow so you can quickly surface high impact security incidents.

Product capabilities

- Associate attacks with specific domains, IPs, ASNs, and malware in order to map out attacker infrastructure.
- See suspicious spikes in global DNS requests to a specific domain.
- Predict where future attacks might be staged by identifying related domains and IPs that are associated with malware.
- Research the behavioral indicators and network connections of malware samples with data from Cisco AMP Threat Grid.
- Use WHOIS data to see domain ownership and uncover malicious domains registered with the same contact information.
- Leverage our risk scoring across a number of domain attributes to assess suspicious domains.
- Detect fast flux domains and domains created by Domain Generation Algorithms.
- Access the largest passive DNS and WHOIS database to see historical data about domains.

Cisco Umbrella