Cisco Umbrella

Cisco Umbrella Tech Update

Mikael Grotrian
Consulting Systems Engineer

Cisco Umbrella

Cloud security platform

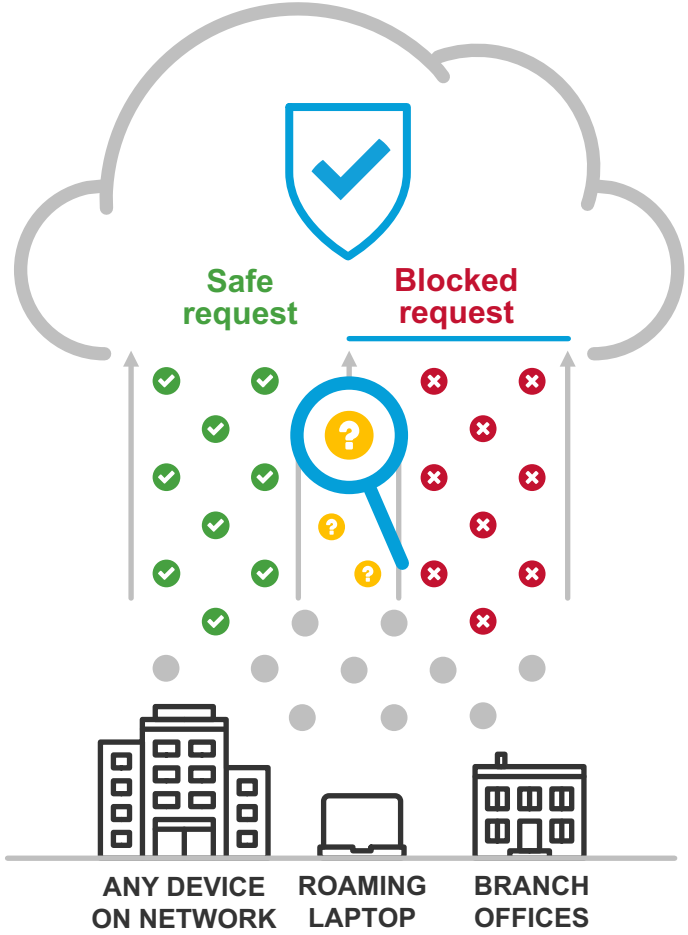
Built into the foundation of the internet

Intelligence to see attacks before launched

Visibility and protection everywhere

Enterprise-wide deployment in minutes

Integrations to amplify existing investments



ENFORCEMENT

Built into foundation of the internet

Destinations

Original destination or block page

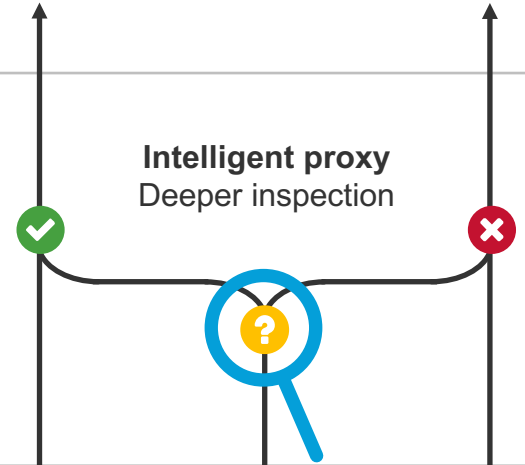
Safe
Original destinations

Blocked
Modified destination

Security controls

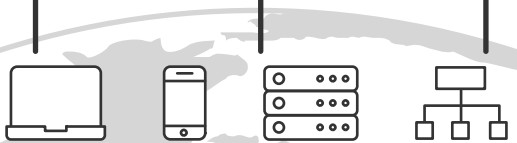
- DNS and IP enforcement
- Risky URL inspection through proxy
- SSL decryption available

Intelligent proxy
Deeper inspection



Internet traffic

On and off-network

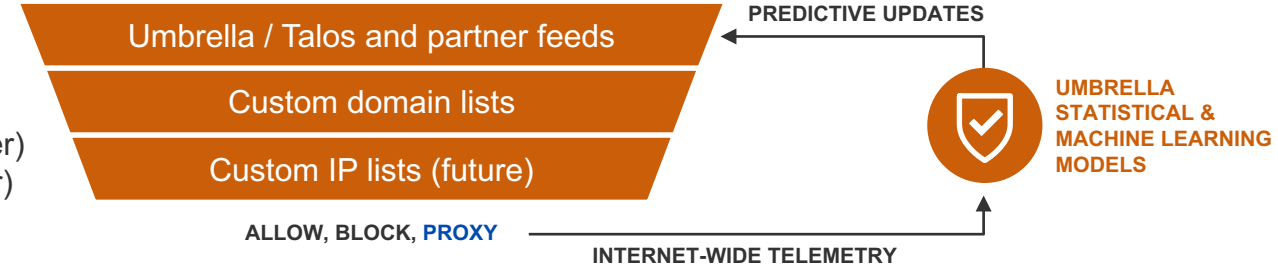


Cisco Umbrella

Breadth to cover all ports and depth to inspect risky domains

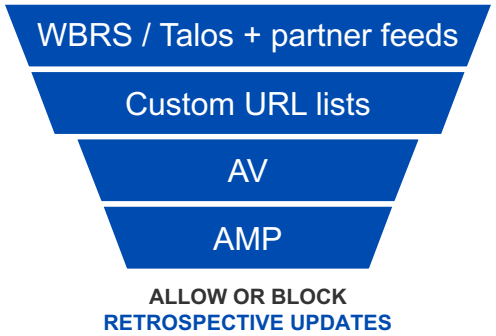
DNS and IP layer

- Domain request
- IP response (DNS-layer) **or** connection (IP-layer)



HTTP/S layer

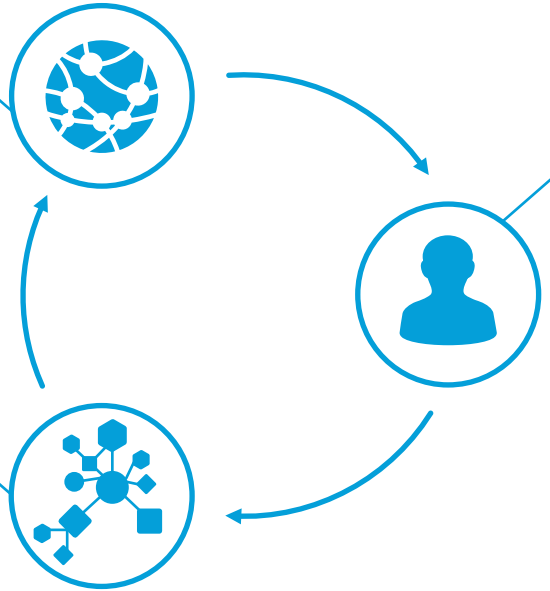
- URL request
- File hash



Intelligence to see attacks before launched

Data

- Cisco Talos feed of malicious domains, IPs, and URLs
- Umbrella DNS data — 100B requests per day



Security researchers

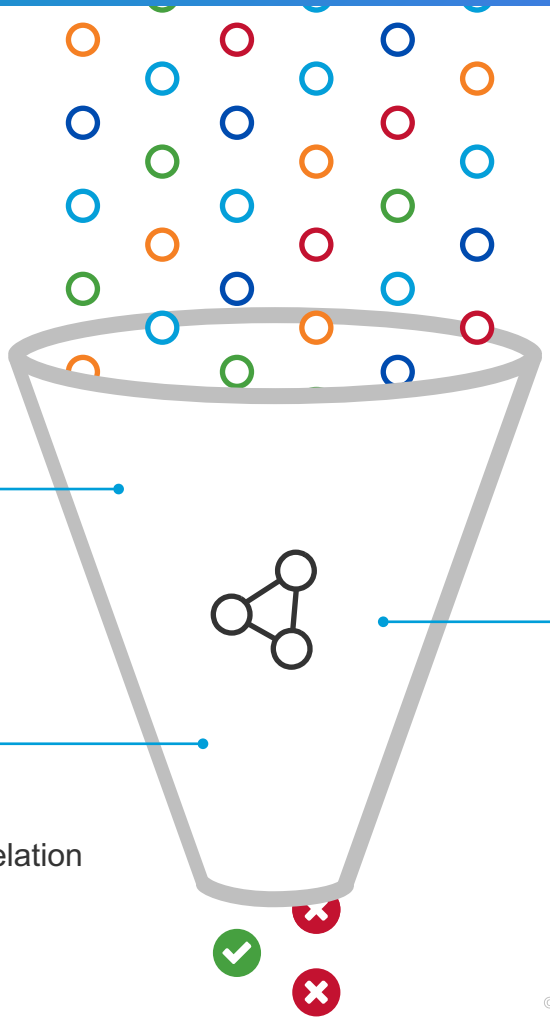
- Industry renown researchers
- Build models that can automatically classify and score domains and IPs

Models

- Dozens of models continuously analyze millions of live events per second
- Automatically uncover malware, ransomware, and other threats

INTELLIGENCE

Statistical models



2M+ live events per second

11B+ historical events

Guilt by inference

- Co-occurrence model
- Geo-location model
- Secure rank model

Guilt by association

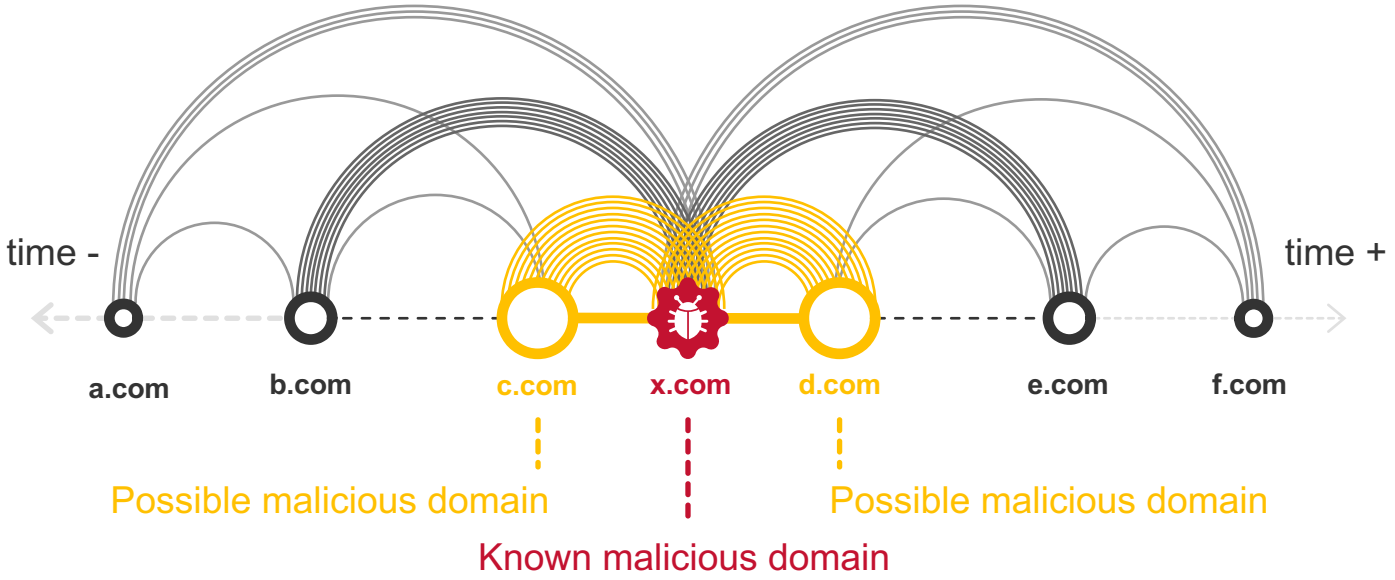
- Predictive IP Space Modeling
- Passive DNS and WHOIS Correlation

Patterns of guilt

- Spike rank model
- Natural Language Processing rank model
- Live DGA Detection

Co-occurrence model

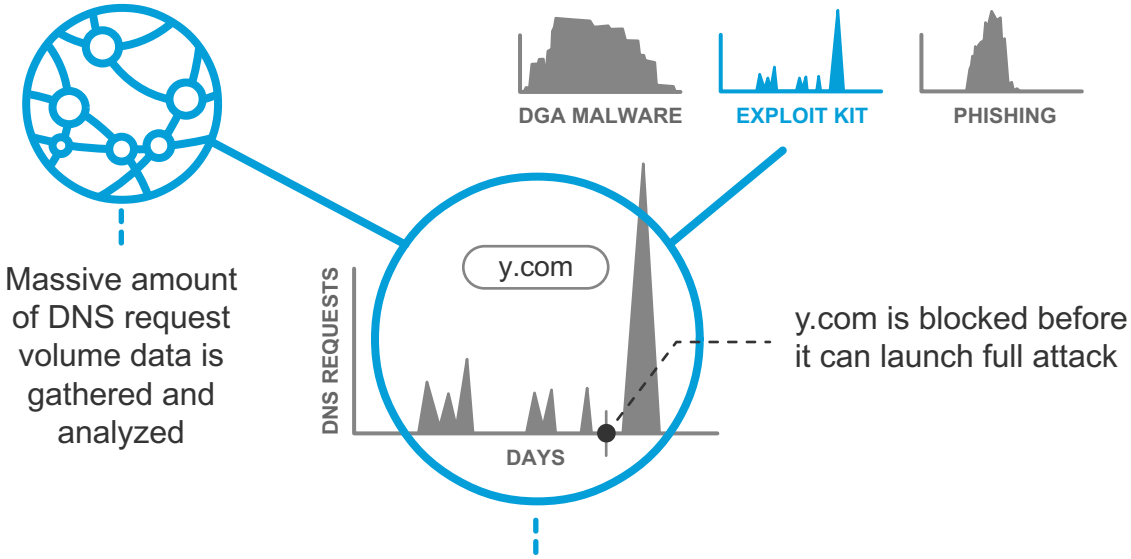
Domains guilty by inference



Co-occurrence of domains means that a statistically significant number of identities have requested both domains consecutively in a short timeframe

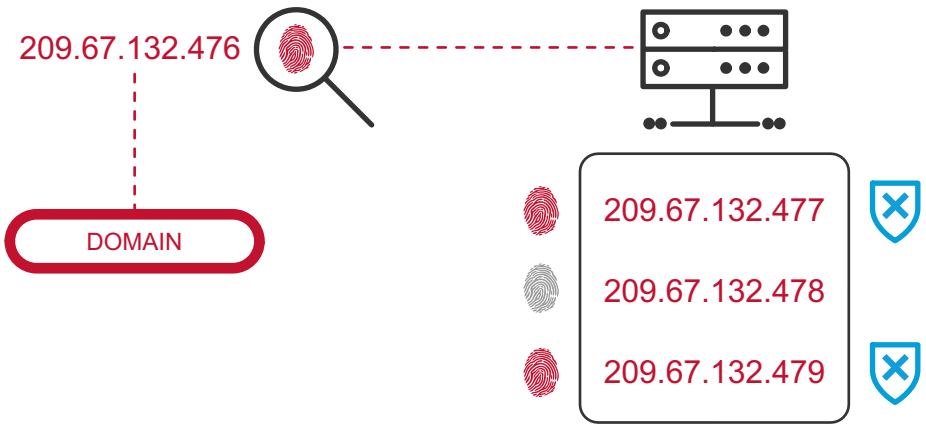
Spike rank model

Patterns of guilt



Predictive IP Space Monitoring

Guilt by association



Pinpoint suspicious domains and observe their IP's fingerprint

Identify other IPs – hosted on the same server – that share the same fingerprint

Block those suspicious IPs and any related domains

IP geo-location analysis

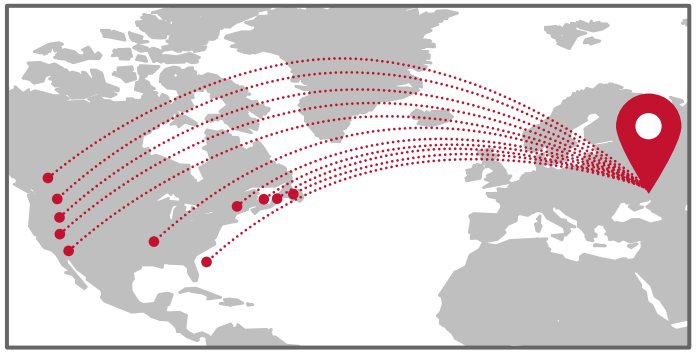
Host Infrastructure

Location of the server
IP addresses mapped to domain

Hosted across 28+ countries

DNS Requesters

Location of the network and off-network device
IP addresses requesting the domain

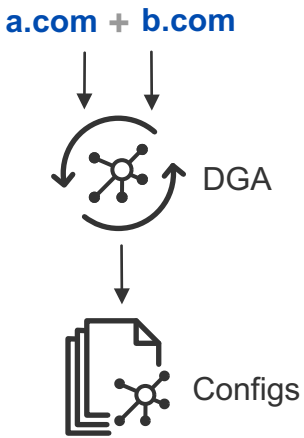


Only US-based customers
requesting a .RU TLD

‘Live DGA Prediction’ automated at an unparalleled scale

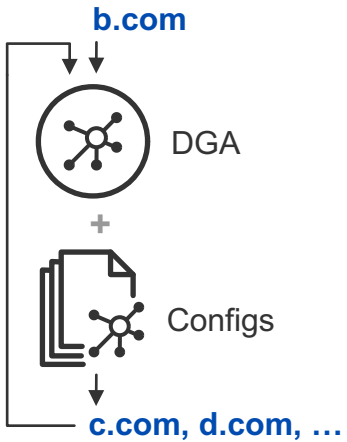
Live DNS log stream

Identify millions of domains, many used by DGAs and unregistered



Automate reverse engineering

Combine C2 domain pairs and known DGA to identify unknown configs



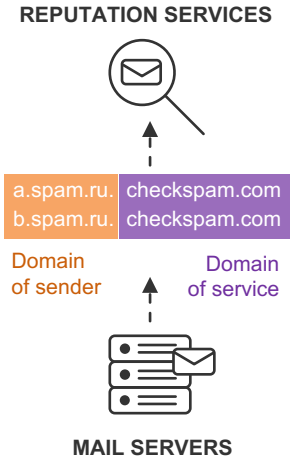
Predict 100,000s of future domains

Combine newly-identified configs with DGA to identity C2 domains continuously

Automate blocking pool of C2 domains

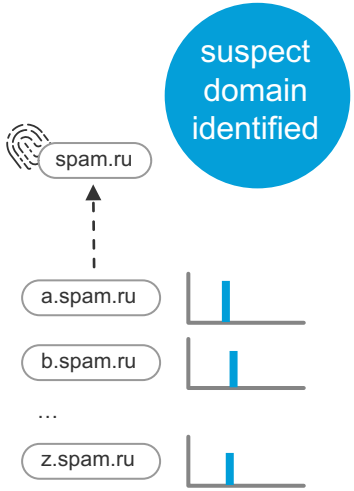
Used by thousands of malicious samples now and in the future

‘Sender Rank’ model: predict domains related to spammers



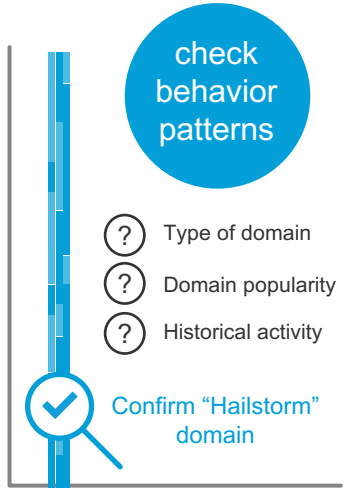
Identify queries to spam reputation services

85M+ DNS users are attacked by various spam campaigns and use reputation services



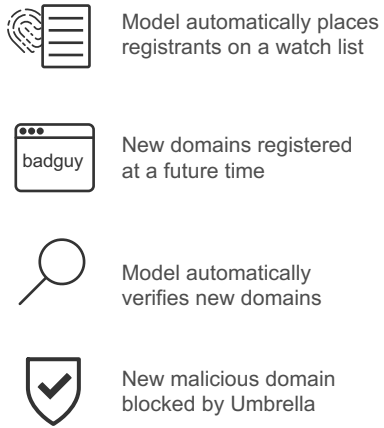
Model aggregates hourly graphs per domain

Short bursts of 1000s of “Hailstorm” spam uses many FQDNs, e.g. subdomains, to hide from reputation services



Model identifies owners of “Hailstorm” domains

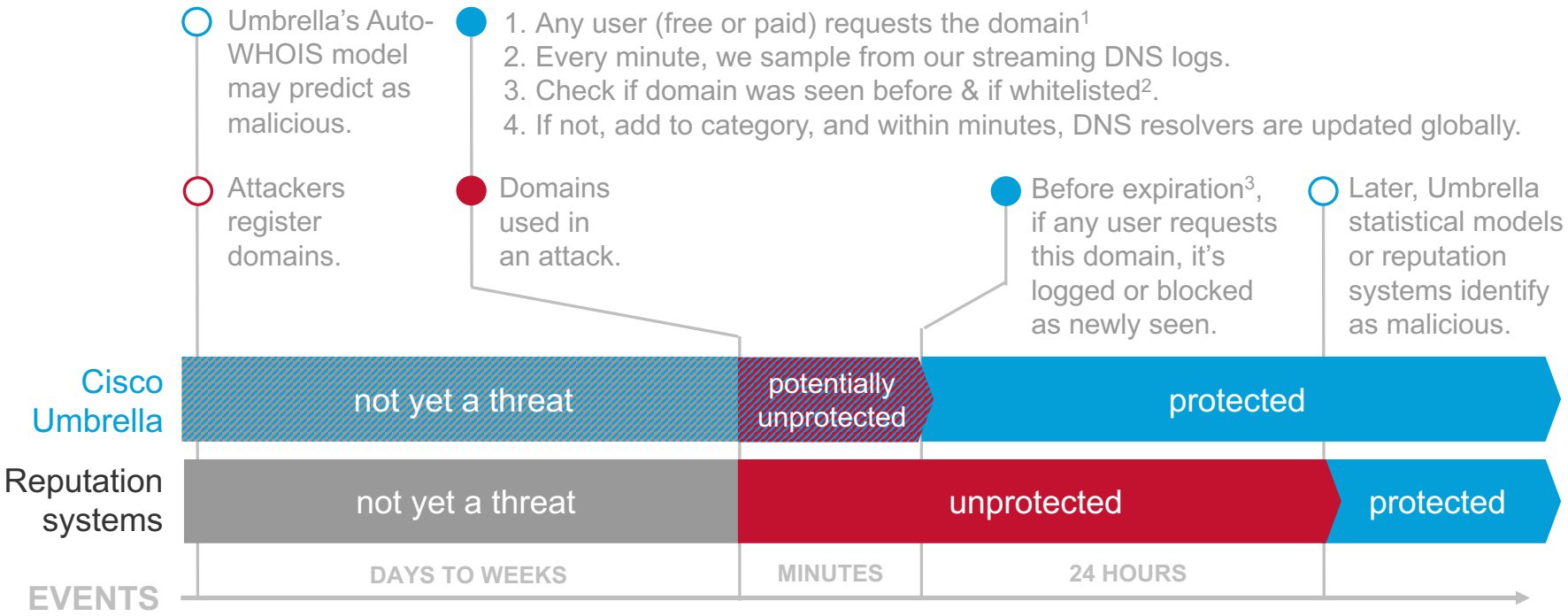
After confirmation, query WHOIS records to get registrant of sender domain



Block 10,000s of domains before new attacks happen

Attackers often register more domains to embed links in phishing or C2 callbacks in malware

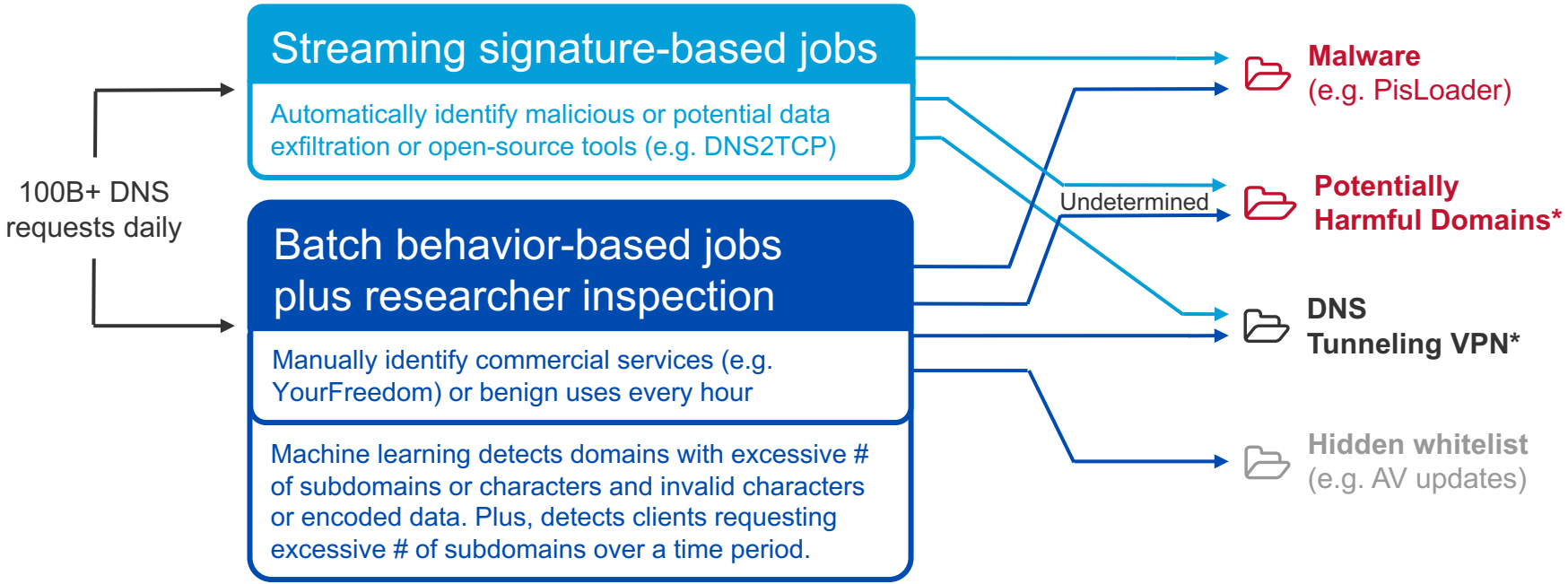
‘Newly Seen Domains’ category reduces risk of the unknown



Cisco Umbrella

1. May have predictively blocked it already, and likely the first requestor was a free user.
2. E.g. domain generated for CDN service.
3. Usually 24 hours, but modified for best results, as needed.

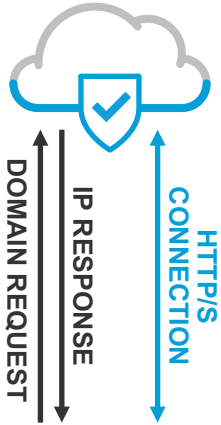
New analysis and categories to combat DNS tunneling



***NEW CATEGORIES:** These are allowed by default, but can be blocked. And domains in these categories may have already been categorized as Malware or Botnet (a.k.a. C2 callbacks) by many other Umbrella statistical models.

DEPLOYMENT

Enforcement and visibility per Umbrella identity



Securely embed identities within query using a RFC-compliant mechanism, differing granularity based on deployment

Web-based redirects transparent to user enable same identity for proxy

NETWORK VIA EGRESS IP FOR ALL DEPLOYMENTS

Umbrella deployments	Your DNS or DHCP server	Umbrella roaming client (RC)	+ Umbrella AD Connector	+ Umbrella virtual appliance (VA)	Umbrella API for network devices
Umbrella identities	N/A	Hostname (GA)	*Usernames with groups for RC and VA	Internal IPs	Network device names or VLAN IDs
		Internal IPs (LA)		Subnets	
		Usernames* (LA)		Usernames*	

*Indicates identity available with Umbrella AD Connector

On and off the corporate network

All ports and protocols

Open platform

Live threat intelligence

Proxy and file inspection

Discovery and control of SaaS

Opfølgning

- Tilmeld jer Virtual Updates + TechUpdates
- Tilmeld jer Cisco Live (Vegas + Barcelona)
- Talos
- Join Cisco Security
  - Youtube
    - Cisco Security
    - Umbrella
    - Talos
    - Chalk Talks
  - Demo Fridays

Cisco Umbrella