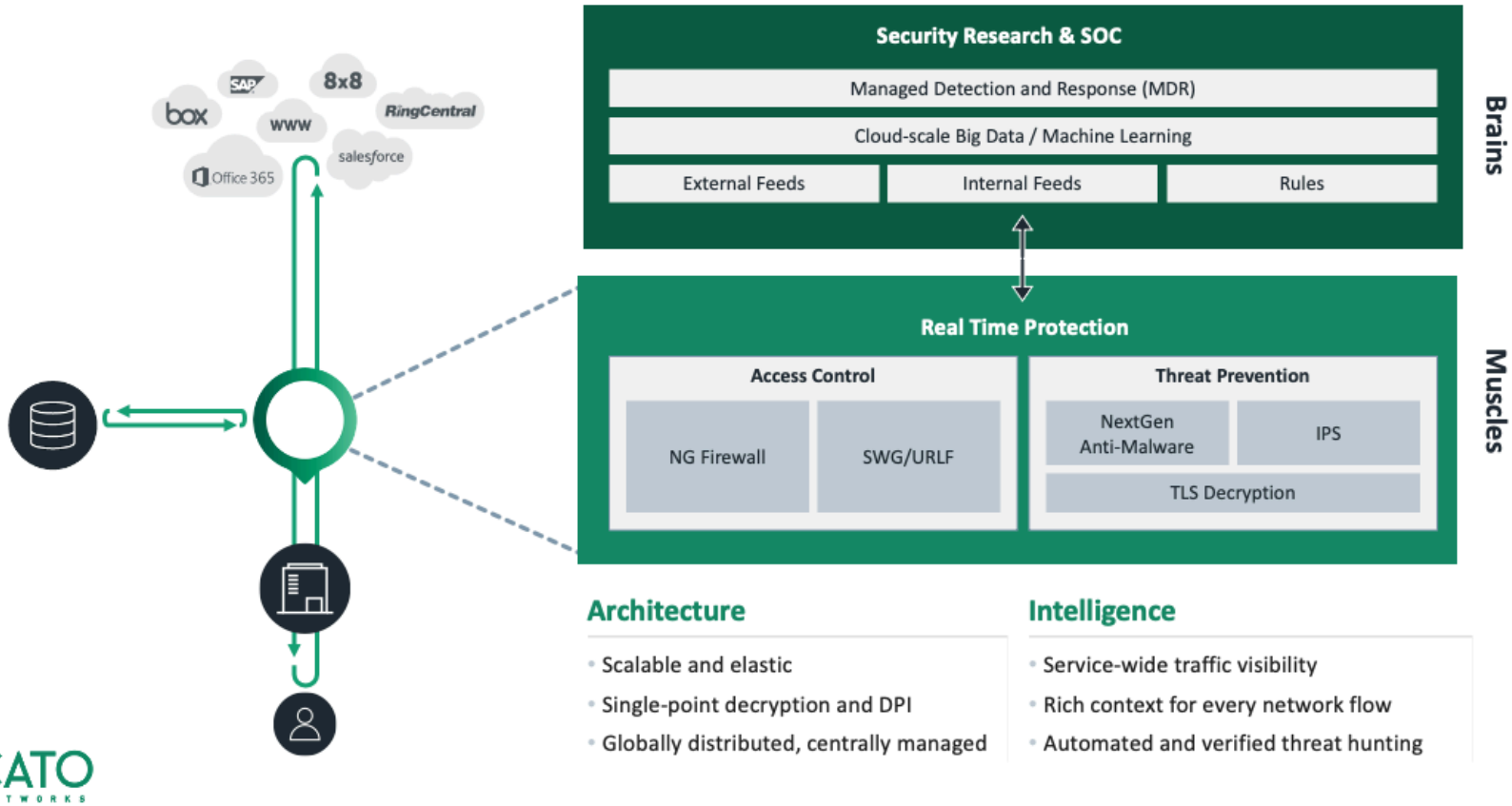
CATO NETWORKS

SOMMITA TECHNOLOGY GROUP, LLC

Security-as-a-Service Overview



The Cato Security-as-a-Service stack protects all traffic, WAN, Internet and Cloud against threats and attacks.

Architecture

We apply 2 set of engines: NG-firewall and Secure web gateway to control access to internal resources and external sites. And NG-anti malware and IPS to detect threats such as malware download and outbound malware communication. Cato maintains these engines for up-to-date protection, no upgrades or patches needed.

Cato's cloud-based architecture is scalable and elastic. Unlike edge appliances that are constrained by the volume of traffic they can protect, Cato leverages cloud-scale infrastructure to deliver enterprise-grade security across all traffic.

Because all WAN and Internet traffic flows through Cato, we can decrypt once and then apply the full security stack against the traffic – at line speed. If a customer chooses not to decrypt traffic the NG-FW and SWG still secure the traffic.

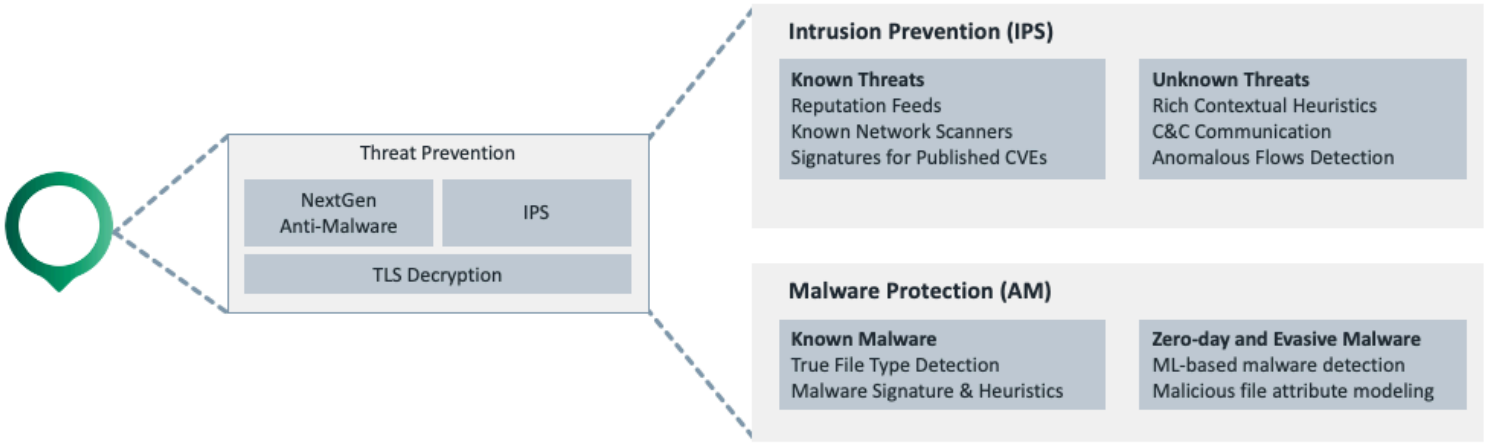
Lastly, Cato is globally distributed and centrally managed. Cato presents a single logical security engine that exists everywhere, so customers can set policies on logical business elements (people, locations, applications) without worrying about pushing these policies to the "right box".

Intelligence

Cato security is driven by real time intelligence.

Cato uniquely sees live traffic across hundreds of networks, including a trillion flows a day. Flows attributes are stored in our cloud-scale big data and provide rich context for our automated machine learning algorithms to analyze network activity.

Cato researchers use our vast database to detect suspicious flows, investigate them, and validate actual live threats on customer networks. This is the foundation for our managed detection and response service – yet another level of convergence that is going beyond products and network services.



Let's zoom into the threat prevention engine. It is comprised of 2 core engines:

The IPS (Intrusion Prevention System)

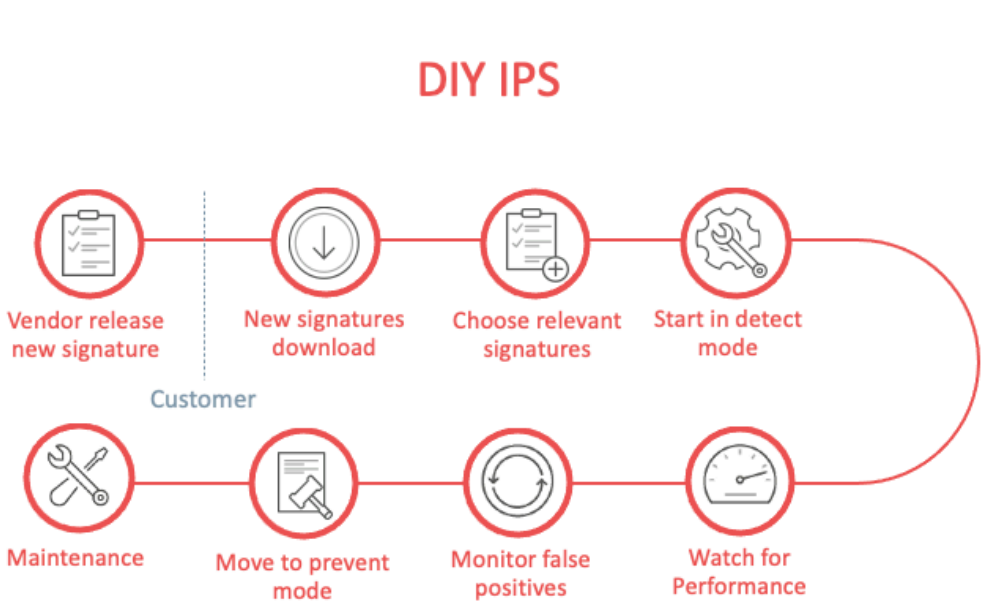
- All traffic, both inbound and outbound is processed by Cato's IPS. The IPS includes rules designed to protect against known threats and vulnerabilities, and real-time feeds that track malicious sites and servers. In addition, the IPS rules detect and prevent anomalous behavior based on flow context and characteristics.

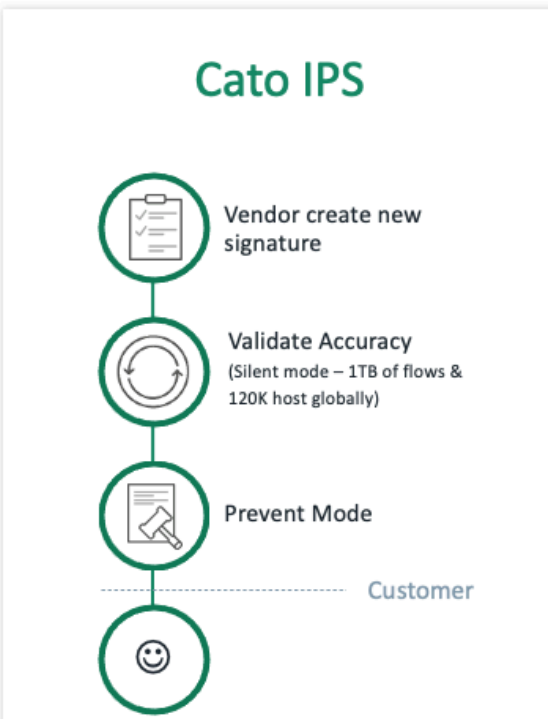
Malware Protection

- The malware protection leverages Cato full traffic visibility, to extract files from the stream.
- Each file goes through an analysis process to determine true file type and combat evasion tactics for executables masking as documents.
- The file is validated against known malware databases. This is the first layer of defense.
- The next layer, takes clean files, and run them though a machine-learning based engine, from SentinelOne, to detect malicious files based on their structural attributes. This is useful for example, against polymorphic encryption, that creates a stream of unique file signatures for the same malware file (a known tactic to evade signature- based malware protection). It can also work against zero-day malware by building a model of attributes associated with malicious files and comparing incoming files against that model.

This level of protection, as we discussed, is extended to all locations, users, and traffic and deliver cutting edge capabilities typically available only to very large enterprises.

DIY IPS vs. Managed IPS-as-a-Service





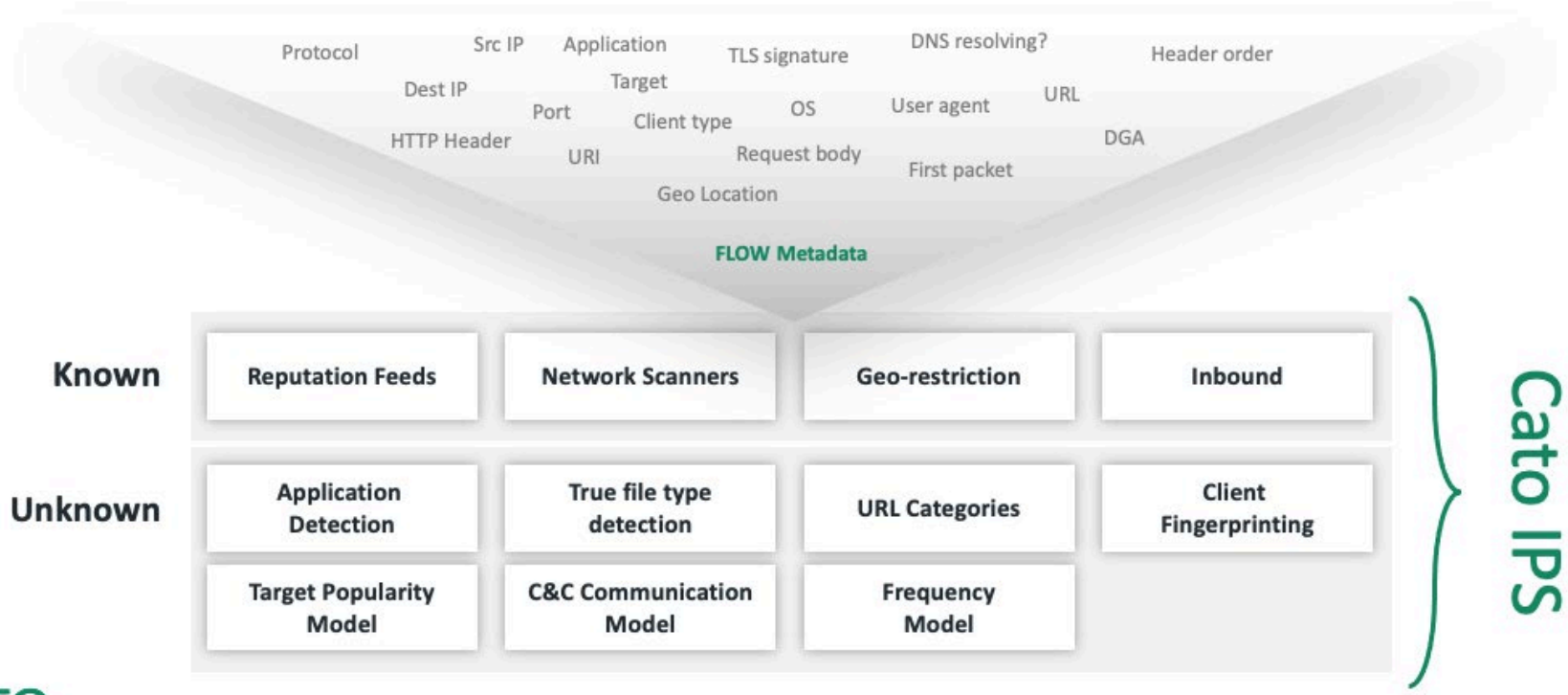
Why is managed IPS so important and unique?

Legacy IPS technology is simply unmanageable for most enterprises. IPS life cycle requires heavy involvement from IT. The IPS vendor distributes new signatures, IT needs to assess for relevance and performance impact, than test on live traffic for false positives and end user disruption, and only than deploy in full production. The resource impact causes many IT teams, to move IPS to detect mode, and essentially ignore the alerts it generates.

Here is how this entire process is eliminated with Cato. Our experts evaluate emerging threats and develop the rules to stop them. They test the rules in simulate mode on live traffic to ensure customers are not impacted and no false positives are generated before moving them to prevent mode. As a result, our IPS actually stops bad traffic without overloading IT.

Cato's IPS-as-a-Service with Context-Aware Protection

Analyze traffic in context to protect against known and unknown attacks



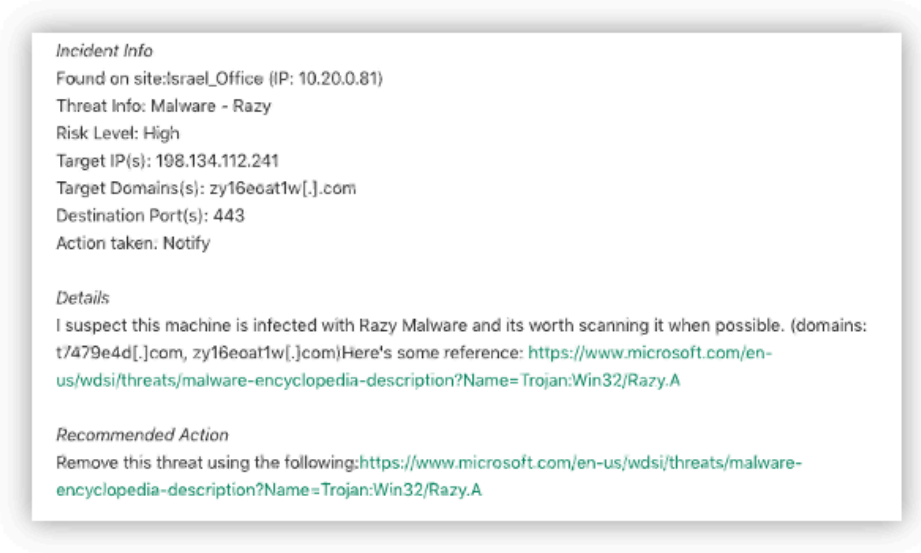
To understand more about the IPS let's understand how it works.

First, Cato IPS can access a very rich context of every flow as seen here. Beyond the obvious flow attributes like source and destination IP, it can access the HTTP header, the flow encryption algorithm, the type of client application, and the attributes of the target URL. For example, the URL category, age, and if it is machine or human generated).

All this context is rarely available to appliance-based IPS. The context is used by the Cato IPS rules to stop both known threats such as traffic from blacklisted IP or Geo and unknown threats by identifying anomalous or highly suspicious flows.

From Automated Prevention to Managed Detection and Response

- IPS is a threat prevention engine
  - It stops inbound threats and outbound malicious communication
- Endpoints can get infected
  - Locally through USB or when equipment is taken out of the enterprise network
  - And, yes, no protection is 100% bulletproof
- Cato managed detection and response service (MDR)
  - Daily analysis of the network to find compromised endpoints
  - Human expert verified
  - Guided remediation

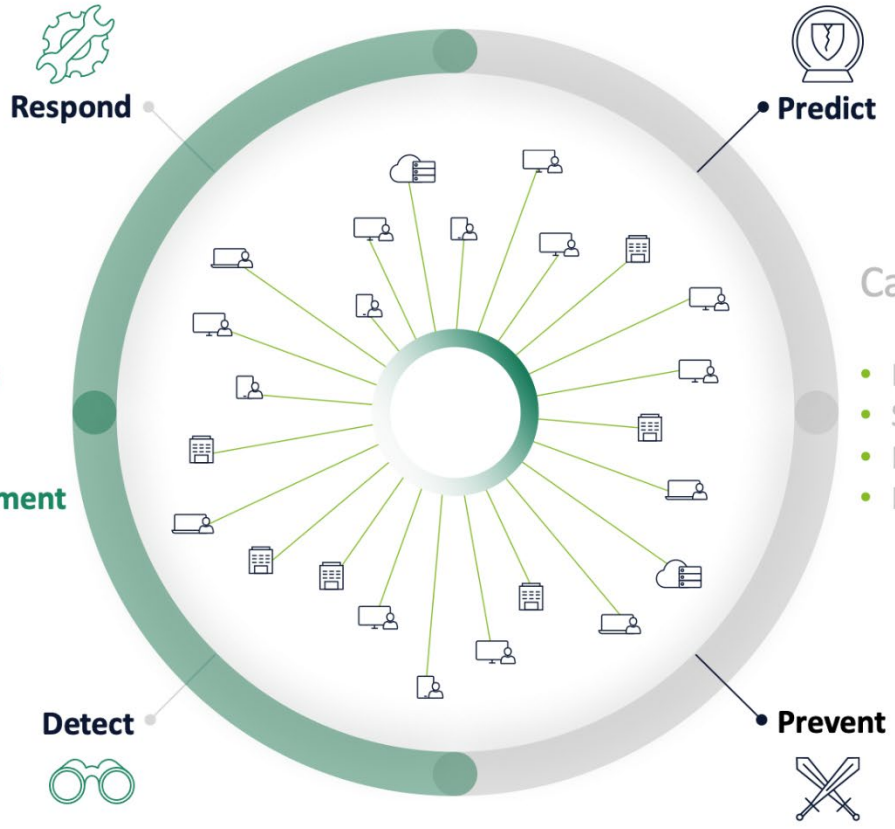


Beyond prevention there is detection.

IPS is threat prevention engine that will stop malicious inbound and outbound communication. But endpoints can still be infected by malware, which requires a different set of resources to detect, investigate, and remediate.
Cato offers a daily analysis service of your network to find compromised endpoints and assist in remediation. To the right is the type of notification Cato generates to let you know of what we are able to find.

Cato MDR

"Extra Pair of Eyes" to watch over the network



Cato MDR

- Zero-footprint Data Collection
- Automated Threat Hunting
- Human Verification
- Network-level Threat Containment
- Guided Remediation

Cato Prevention

- NGFW
- SWG/URL Filtering
- IPS as a Service
- NG-AV

Cato MDR: Monthly Report Sample (real MDR customer)

Investigations Audit

This shows conducted investigations details and conclusions performed by our team based on the network data in your business. Any incident here represent repetitive communication (most likely bot traffic) between a certain device and one or more targets. The concluded classification of this incident is highlighted in a matching color.

Total: 66

Incident ID	Timestamp	Site	Source Client	Target	Risk Level	Risk Type	Risk Name
a6442d73	2019-03-03 15:29:05	MONETT	10.100.10.95	www.mapsfrontier[.].com	low	pup	MapsFrontier
00bb31a3	2019-03-03 15:55:14	ENGLEWOOD	192.168.213.75	cdn2121.advancedmaccleaner[.].com	medium	pup	Advanced MAC Cleaner
f78d99e2	2019-03-03 16:52:30.288722	Radouane Kharibiche	10.41.98.29	ktv.kooora.ws	Inconclusive	Inconclusive	Suspicious activity
a41d1806	2019-03-04 13:42:48.661209	Rob Womble	10.41.70.24	rwiwqblifxge.pplt.com	Benign	App	pplt.com
43d5c2bf	2019-03-04 13:51:45.563054	PPLWSBRG1	10.10.10.176	joksmrjkawjcbn.hags.com	Benign	App	HAGS Global
e83a26e5	2019-03-04 13:58:11.846932	Rodney Holland	10.41.70.22	xorcboqmtv.pplt.com	Benign	App	pplt.com
ce1b03b7	2019-03-04 13:58:50.646415	SSI DFW	172.16.47.22	ecjoowxpyuef.pplt.com	Benign	App	pplt.com
73e51b77	2019-03-04 14:09:43.517006	ENGLEWOOD	192.168.213.68	pblxguuc.fxdqgxfynma.com	Benign	App	playtimeco.local
307cafe7	2019-03-04 14:10:14.877540	Jason Brucks	10.41.70.21	jqmomqkpecuijpl.pplt.com	Benign	App	pplt.com