ThreatAvert

Protect vital network assets and identify malware that impacts subscribers

Service providers recognize network security drives brand equity because it directly impacts subscriber satisfaction. Most threats rely on DNS to function, and new threats have been developed that specifically target critical DNS infrastructure. Providers need to rethink how to protect network resources and subscribers, especially as threats become more dynamic and diverse in a world where everything is connected.

Akamai SPS ThreatAvert evaluates DNS lookups in real time to detect and disrupt malicious activity. ThreatAvert targets threats that cause network outages or slowdowns, adversely impact the subscriber experience, or subvert other network protections, including:

- DNS-based DDoS that overwhelms resolvers with massive volumes of queries
- Bot malware that steals valuable personal data, or compromises consumer devices
- DNS tunnels that steal services by carrying other protocols inside DNS

Akamai SPS ThreatAvert is powered by Akamai's leading CacheServe DNS resolver, equipped with Global Intelligence Xchange (GIX) dynamic threat feeds. CacheServe is the gold standard for reliability — years of investment optimizing performance and numerous software enhancements ensure resilience and availability even in the face of massive spikes in DNS traffic. GIX is created by the Akamai Data Science team that processes more than 100 billion DNS queries, live streamed from around the world every day.

DNS Security Belongs in DNS Servers

DNS queries are a leading indicator of malicious activity because resolving the address of a malicious resource— C&C server, malware download, exfiltration site, etc. — is the first step in enabling most forms of malicious activity. DNS resolvers are an ideal place to embed intelligence to target threats because they see all the queries on a provider network. Malicious activity can be detected by matching incoming queries against entries on dynamic threat lists.

ThreatAvert scales in the DNS control plane, with far less cost, operational effort, and network impact than dedicated packet-processing solutions that scale with data plane traffic.

It's lightweight and efficient, and network traffic incurs no additional latency. Since it's network based, every device is covered, and clients and hosts don't require security software installation or updates.

Superior Accuracy, Depth and Breadth of Threat Coverage

Malware developers continuously innovate to maximize return on investment of their exploits. This means most threats are carefully designed to evade detection, and change rapidly so they can be sustained. The attack surface has also expanded to include a staggering variety of connected "Internet of Things" (IoT), so there's considerable diversity in the methods attackers use to achieve their goals.

Recognizing the subtlety and diversity of the threat landscape, Akamai's Data Science team has developed, implemented, and integrated key systems to analyze live-streamed DNS queries. Threat data from reputation lists, honeypots, and other third-party sources are incorporated in the process. Superior breadth and depth of threat coverage, accuracy, and agility come from investments in:

KEY HIGHLIGHTS

- Lightweight solution, scales to millions of subscribers, covers every device
- Leading data science delivers superior depth and breadth of threat coverage
- Continuously updated threat feeds maintain protection as exploits change
- Easy to read, real-time reports show threat status at a glance and link to details
- Efficient collection and scalable management of threat and telemetry data

ThreatAvert

- Patent-pending algorithms to instantly detect anomalous behavior (like DNS-DDoS), correlate disparate threats, and identify new bot Domain Generation Algorithms
- Advanced techniques for auto-whitelisting names to ensure "good" DNS queries are always protected
- Research staff with years of security experience and a deep understanding of malware and DNS data
- Worldwide network and data centers for real-time processing of live data streams

Precision Policies Block Bad Traffic, Protect Good Traffic

Precision Policies are incorporated into GIX feeds to manage unwanted DNS traffic. A broad and deep feature set allows fine-grained filtering to target malicious queries and protect (answer) legitimate queries:

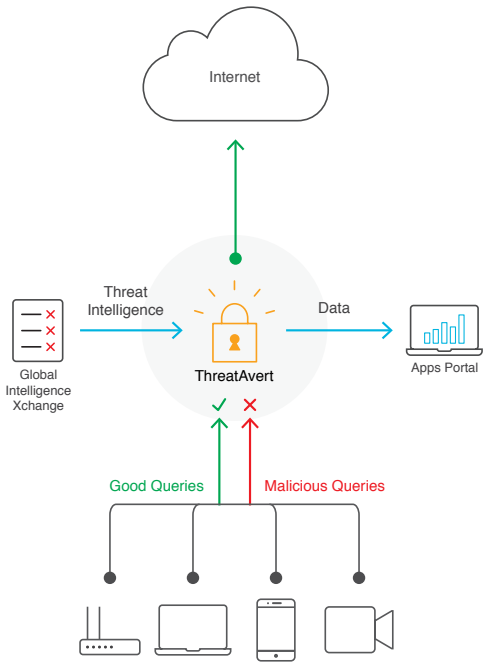
- Precision Policies can be applied to incoming queries or outgoing answers
- Filters or rate limits can be set based on: IP, Query Type, FQDN, or many other query parameters
- Filters or rate limits can use multiple query parameters along with logical operators: QTYPE AND FQDN, IP AND FQDN, etc.
- Filters or rate limits can match against GIX dynamic threat lists or operator-supplied lists
- Policies and threat lists can be combined: MATCH against BLOCKLIST and NOT on WHITELIST
- Multiple policy actions determine how queries are handled: drop, synthesize answer, answerwith truncate, NXD, NOERROR, and many more
- Policies can be combined and nested, making them even more powerful

Precision Policies can also be configured manually to address localized problems in a provider network.

Scalable Data Management, Rich Telemetry and Reporting

ThreatAvert incorporates a data management architecture based on open solutions that have been proven in the world's largest networks, delivering operational excellence at web scale and speed. Live-streamed data from ThreatAvert systems network-wide is aggregated and made available to reporting (described below) and other systems. The resilient architecture provides nonstop availability to power a nonstop customer experience. Optional connectors to open Big Data systems (Splunk, Hadoop) or purpose-built applications can be used to derive additional operational, security, and business insights.

ThreatAvert reports offer an instant assessment of security posture with an Executive Dashboard covering DNS queries blocked, peak DNS bandwidth saved, top malware in network, infected subscribers, and threat intelligence updates. An additional Security Dashboard provides graphs of DDoS and malware details. Successive layers of detail about malware and infected clients can also be obtained with a click. Custom dashboards and reports can be created in minutes to display security data in a user-defined format to meet unique operational requirements. Tag-based reports let operations staff configure views of their ThreatAvert topology to match their unique requirements.



The large data stream processed by Akamai experts offers a comprehensive picture of malicious activity across the Internet, as well as localized attacks.

Akamai