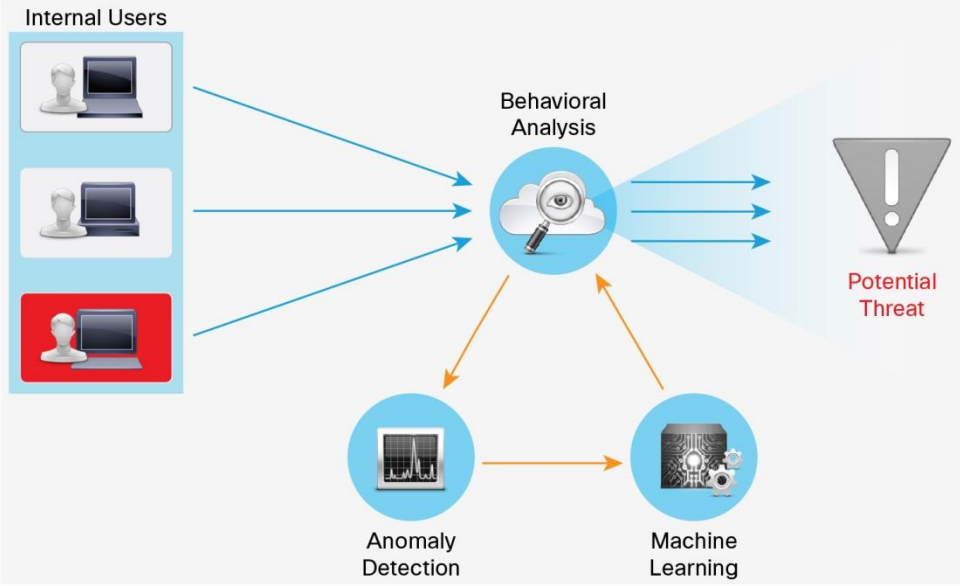
Cisco Cognitive Threat Analytics

Cognitive Threat Analytics (CTA) enhances web security with breach detection and analytics to stop threats in the network

Online threats have become increasingly sophisticated, targeted attacks are on the rise, and cybercriminals launch their campaigns through a variety of vectors. They can serve up malvertising and deploy exploit kits that install rootkits. They can establish a botnet presence within your infrastructure. Once cybercriminals establish a foothold, more than 90 percent of their threats use the web. There, they can establish channels for command-and-control communications and exfiltrate sensitive information.

Analyzing more than 10 billion web requests daily, Cisco® Cognitive Threat Analytics finds malicious activity that has bypassed security controls, or entered through unmonitored channels (including removable media), and is operating inside an organization's environment. Cognitive Threat Analytics is a cloud-based product that uses machine learning and statistical modeling of networks. It creates a baseline of the traffic in your network and identifies anomalies. It analyzes user and device behavior, and web traffic, to discover command-and-control communications, data exfiltration, and potentially unwanted applications operating in your infrastructure (Figure 1).

Figure 1. How Cognitive Threat Analytics Works



Features and Benefits

Feature	Benefit
User and device behavior	Cognitive Threat Analytics analyzes the traffic generated by each user and device. It correlates the data with the organization's broader context to find anomalous traffic associated with command-and-control communications. This automated analysis is critical to the successful identification of threats that use web-based communication to attack organizations.
Confirmed intrusions	Most security technologies provide alerts that require investigation. Cognitive Threat Analytics provides notification of the confirmed threats operating inside your organization so that you can take immediate action without further investigation.
Machine learning	Cognitive Threat Analytics uses machine learning and statistical modeling to independently identify new threats, learn from what it sees, and adapt over time, providing continuous breach identification.
Anonymous traffic monitoring	Cognitive Threat Analytics analyzes all forms of web traffic, including HTTPS and Tor. It provides an exceptional view into the anonymous and encrypted communications that channels attackers use and other security technologies are blind to.
Endpoint Integration	CTA is integrated with Cisco AMP for Endpoints. This integration allows users to gain visibility into devices where a connector cannot be installed, such as personal devices or critical servers, and see results from both systems in one place and act on them on the AMP for Endpoints console, reducing time to detection of new threats.

Identification of Compromised Devices

A cloud-based software as a service (SaaS), Cognitive Threat Analytics requires no additional hardware or software to be deployed. It analyzes web logs and immediately begins to look for threats. It will independently identify suspicious behavior that requires attention. No human intervention is required. On average, Cognitive Threat Analytics detects new threats in 2-3 hours, and will find 45 breached devices in a 5000-employee company each week.

Advanced Analytics

Cognitive Threat Analytics' patent-pending algorithms look at network communications from the inside out, evaluating behavior to create a baseline of normal activity. When it spots behavior that is outside the norm or is otherwise suspicious, it will investigate it and notify you when anomalous and malicious activity occurs. This automated analysis is critical to the successful identification of threats that use web-based communication to attack organizations.

Integrated Threat Intelligence

To provide a comprehensive view of the threat, CTA is integrated with Cisco AMP Threat Grid. When CTA independently detects command-and-control communication in the web channel, it queries the AMP Threat Grid database and correlates the indicators of compromise with the millions of malware artifacts seen by AMP Threat Grid to identify the malware that caused the anomaly.

Automated Response

Using Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII), Cognitive Threat Analytics integrates with existing security monitoring technologies, including Security Information and Event Management (SIEM) platforms. Organizations can integrate and automate their response with an established workflow.

Rapidly Detect Breaches

Cognitive Threat Analytics can spot attacks that are trying to establish themselves in your network as they reach out to command-and-control servers. By identifying confirmed breaches we eliminate the need for investigation and provide actionable intelligence to immediately remediate the threat.

Table 1. Detection & Analytics Engines

Engine	What It Does
Data exfiltration	Analyzing more than 10 billion web requests per day, Cognitive Threat Analytics uses statistical modeling of an organization's network to identify anomalous web traffic and pinpoint the exfiltration of sensitive data. CTA recognizes data exfiltration even in HTTPS encoded traffic, without any need to decrypt transferred content.
Domain Generation Algorithm (DGA)	Attackers generate an arbitrary number of domain names to avoid detection and blacklisting of hosts that provide malware. CTA recognizes malicious and obfuscated domain names generated from words, analyses the frequency of communication, information content of the headers and hundreds of other features we observe on each HTTP/HTTPS request.
Exploit Kit	Analyzing web requests allow CTA to uncover infections by exploit kits from 1) visiting an infected web page, 2) redirect to domain hosting Exploit Kit, 3) unknowing download by user, 4) successful exploitation, 5) download of malicious payload.
Tunneling through HTTP/S requests	Attackers often try to exfiltrate sensitive data, including credentials, using HTTP/HTTPS requests themselves. CTA uses multiple IOCs including global statistics and local anomaly scores to reliably distinguish malicious tunneling from benign use of the technique.
Command and Control (C2) Communication	CTA combines a wide range of data including statistics collected on internet-wide level to host-specific local anomaly scores. Combining of these indicators inside the statistical detection algorithms allows us to distinguish C2 communication from benign traffic and from other malicious activities. CTA recognizes C2 even in HTTPS encoded or anonymous (TOR) traffic, without any need to decrypt transferred content, detecting a broad range of threats.

Licensing

Licenses are available in 1-, 3-, and 5-year terms. They can take the following forms:

- Simple add-on license to Cisco Cloud Web Security
- Simple add-on license to Cisco Web Security Appliance
- Standalone Cognitive Threat Analytics service for third-party web proxy, such as Blue Coat ProxySG

Reduce complexity while gaining superior protection that evolves with the changing threat landscape with Cognitive Threat Analytics.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

Why Cisco

As the largest provider of network infrastructure and services in the world, Cisco is positioned to deliver advanced security solutions that reduce time to discovery and mitigate the scope of an attack inside the network. Taking advantage of Cisco's global footprint and visibility to network traffic running on Cisco infrastructure, Cognitive Threat Analytics focuses on symptoms of infection—not method of attack—to deliver superior protection and evolve with the changing threat landscape. Cognitive Threat Analytics is available as a simple add-on license to Cisco Cloud Web Security, Web Security Appliance, and as a stand-alone solution that can be integrated with existing security solutions.

To Learn More

Find out more at http://www.cisco.com/go/cognitive.

Evaluate how Cisco products will work for you with a Cisco sales representative, channel partner, or systems engineer.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-736557-01 06/16