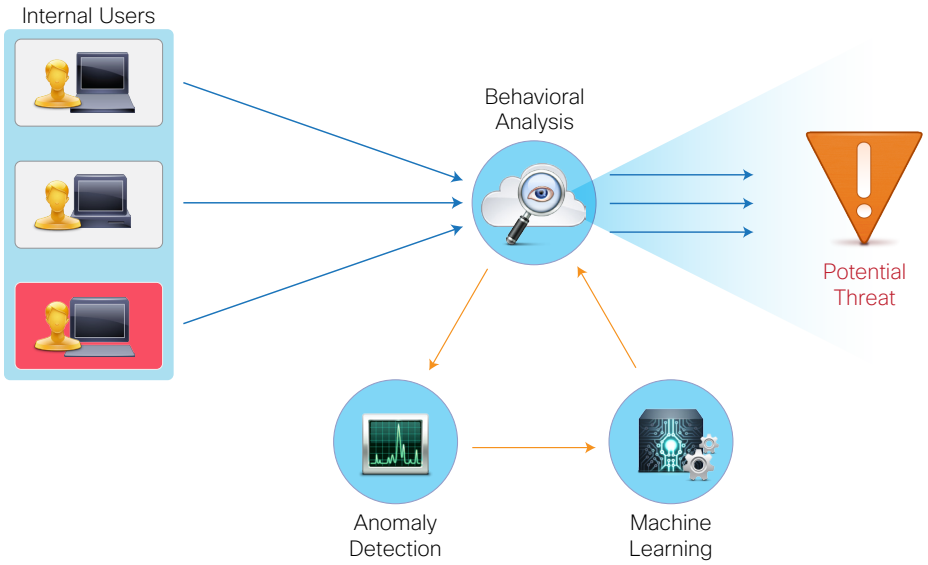
Cisco Cognitive Threat Analytics on Cisco Cloud Web Security

Cisco Cognitive Threat Analytics is a cloud-based solution that reduces time to discovery of threats operating inside the network. It addresses gaps in perimeter-based defenses by identifying the symptoms of a malware infection or data breach using behavioral analysis and anomaly detection.

Unlike traditional monitoring and incident response systems, Cisco Cognitive Threat Analytics is not dependent on manual rule sets, but instead relies on advanced statistical modeling and machine learning to independently identify new threats, learn from what it sees, and adapt over time.

Take advantage of Cisco Cognitive Threat Analytics with a simple add-on license to your Cisco Cloud Web Security solution. Reduce complexity while gaining superior protection that evolves with your changing threat landscape.

Figure 1. Threat Identication Through Behavioral Analytics Anomaly Detection



Evolving Threats, Lagging Security

Legacy preventative security measures are not enough to stop today's advanced threats. Mobile, cloud, and virtual technologies have disrupted the old security model, creating new attack vectors and all but eliminating the traditional network perimeter. Antimalware defenses must fight a never-ending and ultimately unwinnable battle to tag and identify every single exploit on the market. Even the most advanced methods are subject to evasive tactics that exploit weaknesses in point-in-time defenses.

At the same time, existing threat monitoring and incident response systems rely on a complex arrangement of manual rule sets to detect threats inside the network. These solutions require extensive setup times and constant tuning – a costly approach and largely ineffective when it comes to addressing new exploits and evasion tactics.

To deal with the ever evolving threat landscape, you need a different approach that lets you keep up with new and emerging threats.

Key Features of Cisco Cognitive Threat Analytics

- **Discovers threats on its own:** Cisco Cognitive Threat Analytics is not dependent on rule sets. Once you turn it on, the system will immediately begin looking for threats and will independently identify suspicious behavior that requires attention. No human intervention is required.
- **Focuses on symptoms of infection, not method of attack:** Many threat defense and antimalware solutions focus on catching threats by tagging and identifying each exploit's method of attack. Keeping up with the latest threats is impossible. Cisco Cognitive Threat Analytics takes a different approach. Instead of focusing on the method of attack, it looks for anomalous behavior that resembles the symptoms of an infection, regardless of how it got in. Specifically, Cisco Cognitive Threat Analytics analyzes traffic coming in and out of the secure web gateway. It evaluates individual user behavior and broader group context to create a baseline of normal activity. When it spots behavior that is outside the norm or is otherwise suspicious, it will investigate and make a determination as to whether the behavior constitutes a threat.

- **Fights threats with advanced algorithms and machine learning:** The science behind Cisco Cognitive Threat Analytics' unique approach to security – spotting the symptoms of an infection through behavioral analysis and anomaly detection – is rooted in a set of advanced algorithms and cutting edge techniques that were developed by a select group of scientists and engineers (formerly Cognitive Security, which was acquired by Cisco in 2013). They were developed over a 10 year period and include an advanced decision-making mechanisms that analyze multiple parameters and take in live traffic data; as well as machine learning capabilities that allow the system to learn and adapt from what it sees over time.

Benefits

- **Reduced time to discovery:** No matter how strong your defenses are, some malware will get through. Security strategies that focus on perimeter-based defenses and preventative techniques will leave attackers free to act as they please once inside your network. Cisco Cognitive Threat Analytics mitigates the scope of an infection by actively and continuously monitoring for threats that have penetrated your defenses. With its unique approach and advanced capabilities, it accurately identifies threats, and reduces the time to discovery in order to stop an attack before it spreads.
- **Security that evolves with the changing threat landscape:** When it comes to keeping up with the changing threat landscape, Cisco Cognitive Threat Analytics has a number of advantages over traditional solutions.

  First, it focuses on the symptoms of an infection, rather than the method of attack. While new exploits are constantly being released, it is far more challenging for attackers to infiltrate the network without leaving a trace. By focusing on the anomalous behaviors that indicate an infection, Cisco Cognitive Threat Analytics stands a better chance of consistently and reliably spotting new exploits.

  Second, because Cisco Cognitive Threat Analytics is not dependent on manual rule sets, it is not limited by preconceived notions, anchored in past events, or vulnerable to common decision-making biases. Instead, it relies on advanced statistical modeling and machine learning to make more accurate determinations and to improve decision making over time.

  Lastly, even as attackers devise new ways to avoid detection and cover their tracks, Cisco Cognitive Threat Analytics' adaptive capabilities allow it to respond to new threats as they emerge, in a way that manual rule sets can't.
- **Easy setup and maintenance:** Establishing and maintaining an exhaustive arrangement of manual rule sets can be complex, costly and time consuming. Cisco Cognitive Threat Analytics takes away the burden of setup and maintenance by eliminating the need for human intervention so that you can focus on investigating and preventing new incidents. You gain not only increased security, but also easy setup and reduced maintenance costs.

Why Cisco

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

To Learn More

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

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

C45-730900-01 03/14