White Paper

Web Security: Protect Your Data in the Cloud

What You Will Learn

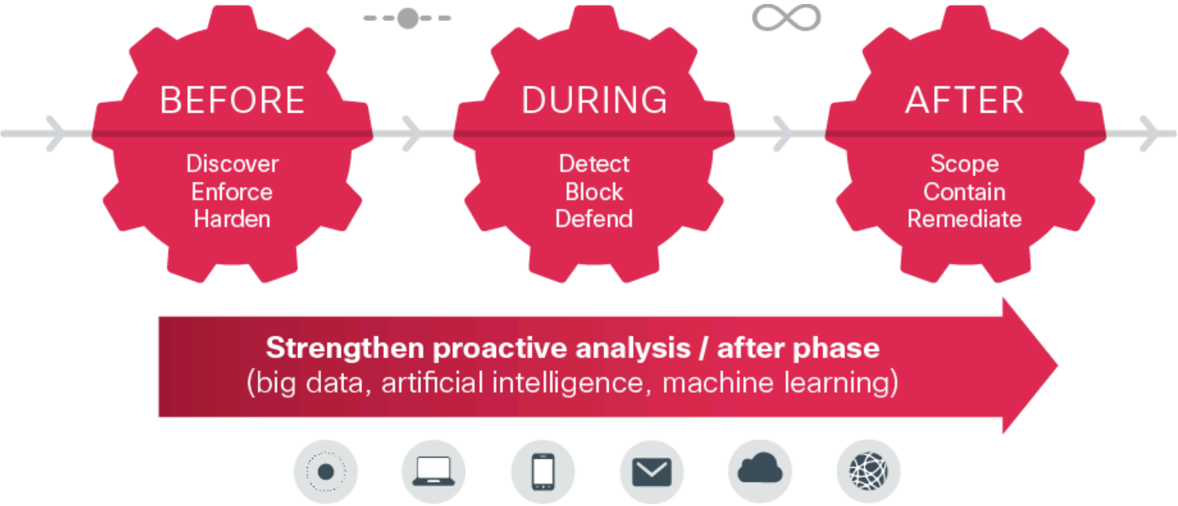
Security teams can't be everywhere, but the current landscape demands that organizations defend their data anywhere a threat can manifest itself. "Anywhere" includes networks, mobile devices, virtual environments, and the cloud or data center.

Today's threats are designed to penetrate every defense. Adversaries are actively working to understand what types of security solutions are deployed. And they are shifting to less visible, less detectable patterns of behavior. According to the *Cisco 2014 Annual Security Report*, most of these actors have one primary mission: stealing high-value data.

Meanwhile, the rise of the distributed enterprise, and the emergence of new business models such as cloud computing, mobility, and bring-your-own-device (BYOD) environments, have eroded the traditional security perimeter and are expanding the attack surface. Security teams are struggling to keep pace. They don't know how to prioritize which threats to investigate and are missing many threats they simply can't see.

It's easy to understand why preventive, point-in-time security solutions cannot provide adequate protection for modern businesses. Of course, no detection method is perfect, and inevitably some threats will be sophisticated and stealthy enough to penetrate all the layers of a defense. What is needed? Continuous and retrospective security designed to cover the entire attack continuum—before, during, and after an attack.

Figure 1. The Attack Continuum


BEFORE
Discover
Enforce
Harden
DURING
Detect
Block
Defend
AFTER
Scope
Contain
Remediate
Strengthen proactive analysis / after phase
(big data, artificial intelligence, machine learning)

Cisco Cloud Web Security Essentials

Cisco® Cloud Web Security (CWS) helps organizations meet the challenge of maintaining continuous security across the extended network. The solution provides industry-leading security and control for the distributed enterprise and offers the broadest set of deployment options available. A cloud-based version of Cisco Web Security, the Cisco CWS platform extends web security to mobile devices and distributed environments. It protects users through Cisco's worldwide threat intelligence, advanced threat defense capabilities, and roaming-user protection.

Cisco CWS features intuitive tools to create, enforce, and monitor inbound and outbound web policy, giving businesses complete control of how end users access Internet content. In short, Cisco CWS is a security perimeter in the cloud. It provides detailed context-aware policy control and enforcement. In addition, it:

- Dynamically blocks threats in real time
- Protects the network and users from undesirable web content
- Optimizes network resources by reducing bandwidth congestion
- Enables comprehensive reporting and monitoring of online activity
- Protects the organization from data leaks

Cisco CWS integrates with Cisco firewalls, branch routers, and client-based software to provide protection wherever users work. All traffic—whether it originates from the headquarters location, from branch offices, or from mobile or remote users—is routed through a global network of Cisco CWS data centers. Cisco CWS eliminates backhaul, speeds the deployment of web security, and helps to extend the value of existing Cisco investments.

With the recent acquisitions of the security companies Sourcefire and Cognitive Security, Cisco is now able to provide an enhanced version of Cisco CWS to thwart advanced malware threats, particularly in the "after" phase of the attack continuum, and to improve real-time threat detection in the "during" phase. Cisco offers this solution through an optional Premium subscription, described below.

Cisco CWS Premium

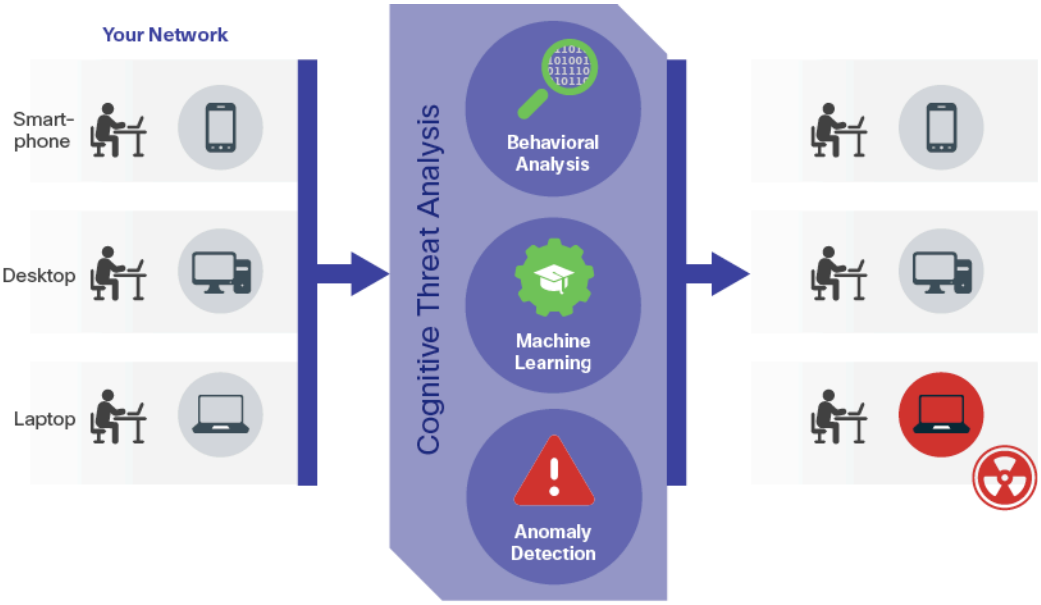
Cisco CWS Premium includes all of the features from Cisco CWS Essentials, but it also incorporates two innovative malware detection systems: Cognitive Threat Analytics (CTA) and Advanced Malware Protection (AMP). These systems automate the search for high-risk threats in an organization's web traffic. Cisco CWS Premium provides additional point-in-time protection, retrospective security, and continuous analysis to help organizations find and address the threats that matter most. And it reduces the time to the discovery of threats already operating inside their networks.

Security teams can now provide continuous web security that protects systems across the entire attack continuum. Following is a closer look at these two malware detection systems.

Cognitive Threat Analytics

Cognitive Threat Analytics, or CTA, developed by Cognitive Security, is a near-real-time network behavior analysis system. It uses machine learning and advanced statistics to spot unusual activity on a network: the symptoms of an infection. The solution is not dependent on rule sets, meaning no human intervention is required to "tune" the technology. Once CTA is enabled, it immediately begins looking for threats. Data is correlated in the cloud to enhance the speed, agility, and depth of CTA's anomaly detection capabilities.

Figure 2. Overview of CTA



CTA learns from what it sees. It adapts over time, identifying new command-and-control channels not previously detected by the security industry. It assesses the behavior of entities (for example, individual users) in the network and uses behavior modeling to predict how those entities should behave. CTA uses a long-term modeling of network behavior to correlate seemingly disparate activities. It then compares that correlated data to individual user behaviors across the specific customer network so it can detect threats more quickly.

It doesn't matter what a detected threat may be. If there is a discrepancy in expected behavior that is significant or sustained, CTA will flag it. CTA's actions are like those of a security team trying to identify a shoplifter before that person has a chance to steal: What is that person doing that is different from what other shoppers are doing? Carrying a big bag instead of pushing a shopping cart? Trying to exit through the back door instead of the front? Even though the suspicious behavior may turn out to be legitimate, it is worthy of investigation.

CTA spots anomalies and then directs security analysts toward potential problems, helping them to reduce their workload and prioritize threats. It also complements existing security technology from Cisco, making these solutions more accurate as well as more capable of detecting unknown or unusual behavior on the network. Cisco security capabilities are thus extended into the "after" phase of the attack continuum. Most important, CTA helps to provide security that evolves with the ever-changing threat landscape.

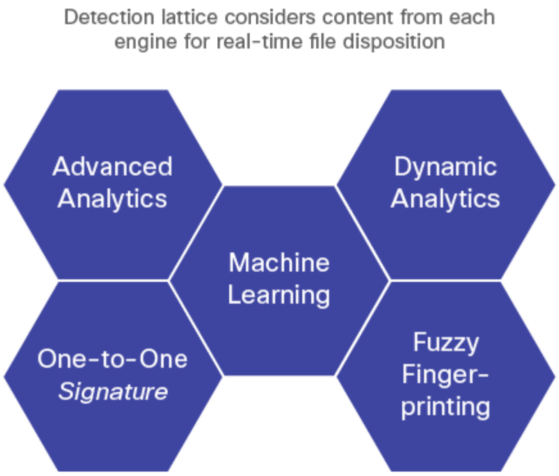
Advanced Malware Protection

The second detection system in Cisco CWS Premium is Advanced Malware Protection (AMP) from Sourcefire. AMP does not rely on malware signatures, which can take weeks or months to create for each new malware sample. Instead, it uses a combination of file reputation, file sandboxing, and retrospective file analysis to identify and stop threats across the attack continuum.

File Reputation

File reputation is the ability to look at databases of files to determine whether a file is “clean,” known to be malware, or unknown. AMP captures a “fingerprint” of each file as it traverses the Cisco CWS service and queries the collective cloud-based intelligence network of Cisco and Sourcefire to obtain a reputation verdict, or “score.” Using those results, AMP can then automatically block malicious files and apply administrator-defined policies. Figure 3 shows the different engines working in real time to detect advanced malware and determine file reputations.

Figure 3. Advanced Malware Protection



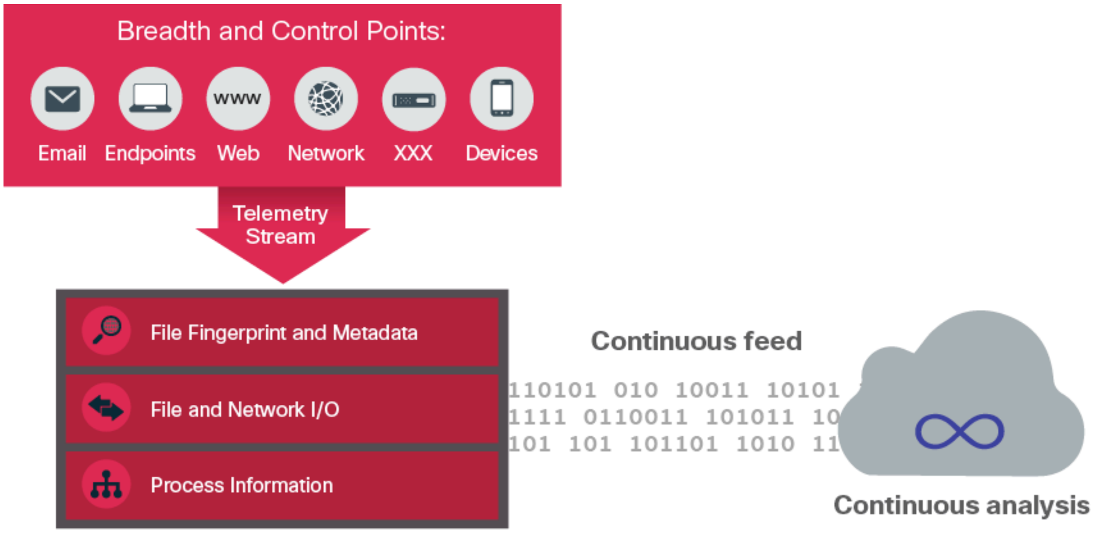
File Sandboxing

File sandboxing is a critical feature of AMP—and ultimately, of Cisco CWS Premium. With file sandboxing, AMP analyzes the unknown files traversing Cisco CWS. In a highly secure sandbox environment, AMP gleans precise details about a file’s behavior and then combines that data with detailed human and machine analysis to determine the file’s threat level. This information is then fed into the collective cloud-based intelligence network of Cisco and Sourcefire and used to dynamically update the AMP cloud data set. Active reporting allows security teams to view data-rich, easy-to-read reports about the analyzed files.

File Retrospection

Perhaps the most important aspect of AMP is its retrospective analysis capabilities, which give organizations the ability to “go back in time” to pinpoint when an outbreak occurred and then assess the damage. File retrospection provides continuous analysis of files that have traversed the security gateway, using real-time updates from the Cisco and Sourcefire cloud-based intelligence network.

Figure 4. AMP's Retrospective Analysis Process

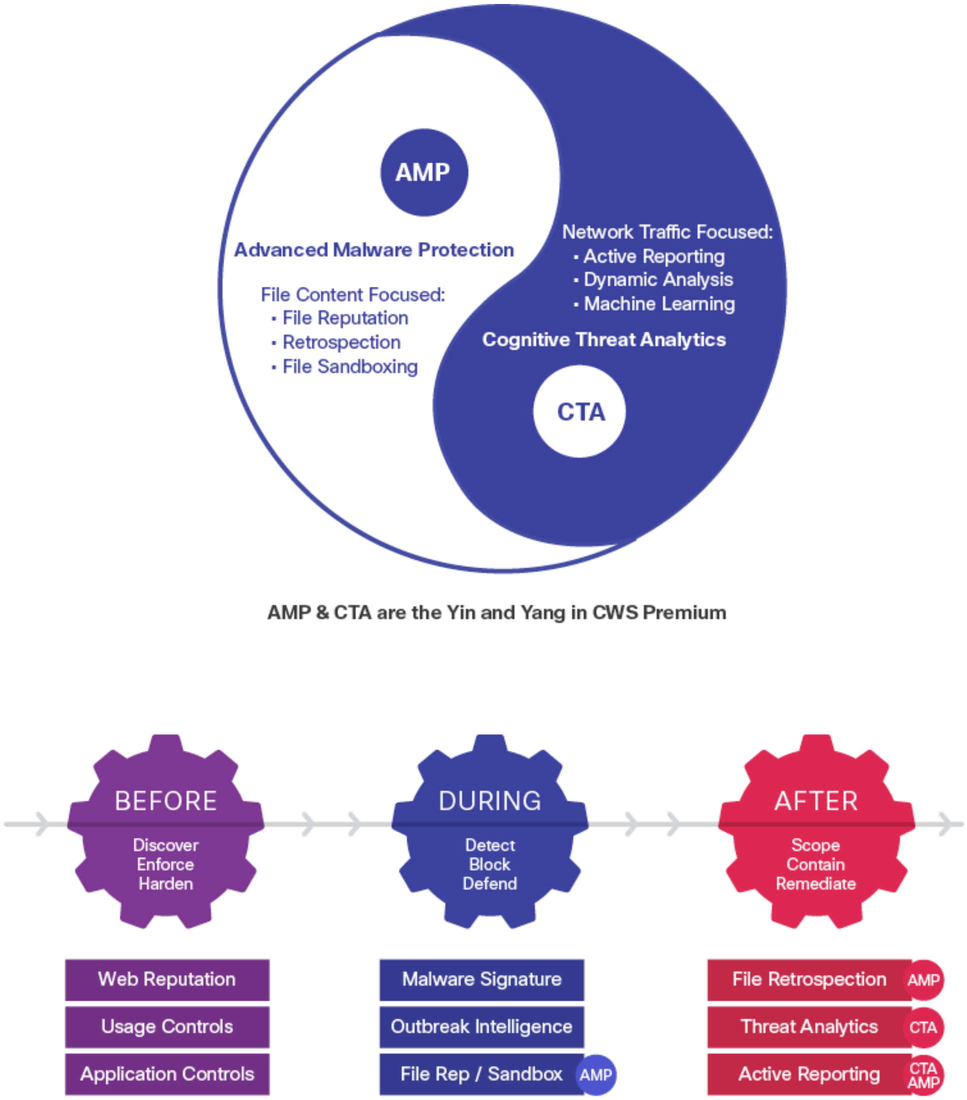


Sometimes retrospective analysis reveals that a file that was deemed "clean" when it passed through perimeter defenses is actually well-disguised, advanced malware. AMP will immediately alert the security administrator and identify which user on the network may have been infected and when. Security teams can address the attack quickly, before it has a chance to spread.

Conclusion

Cisco CWS Premium with CTA and AMP aligns with Cisco's strategy to help organizations address known and emerging security challenges. It helps them to detect, understand, and stop threats. Continuous analysis and real-time security intelligence are delivered from the cloud and shared across all security solutions to improve their efficacy. The combination of these three solutions helps organizations to identify new command-and-control channels not previously detected by the security industry and to address security challenges across the entire attack continuum.

Figure 5. CWS with AMP and CTA: Security Across the Attack Continuum



AMP & CTA are the Yin and Yang in CWS Premium

Before: Discover, Enforce, Harden

Cisco CWS delivers web reputation, usage controls, application controls (including those for microapplications), malware signatures, and outbreak intelligence to provide security both before and during an attack.

During: Detect, Block, Defend

AMP enhances security at the “during” phase of the attack continuum with its file reputation and file sandboxing capabilities. It automatically blocks malicious files and applies administrator-defined policies based on a file’s known reputation. It also analyzes unknown files traversing Cisco CWS and updates threat intelligence accordingly. These capabilities help security analysts prioritize threats to investigate.

After: Scope, Contain, Remediate

Both CTA and AMP enable continuous analysis and remediation in the critical “after” phase of the attack continuum. CTA provides real-time network behavior analysis to identify anomalous behavior in the network. AMP’s file retrospection, meanwhile, addresses the problem of malicious files passing through perimeter defenses. AMP’s active reporting capabilities provide visibility into the reputation and behavior of files that have entered the network. Security teams can more easily identify and assess the scope of attack and remediate quickly.

The machine learning that occurs with CTA and AMP in the “after” phase is then used to enhance the near-real-time detection capabilities that Cisco CWS Premium applies during an attack.

For More Information

To find out more about Cisco CWS Essentials and Cisco CWS Premium, go to http://www.cisco.com/go/cws.

For more information on CTA, see http://www.cisco.com/go/cognitive.

For more on AMP, visit http://www.cisco.com/go/amp.

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 C11-732714-00 09/14