Biedt de Cisco Web Security Appliance (WSA) bescherming tegen malware/spyware?

Inhoud

vraag

Biedt de Cisco web security applicatie (WSA) bescherming tegen Malware/Spyware?

Cisco Web Security Appliance (WSA) biedt de meest uitgebreide gateway-verdediging van de sector tegen spyware en webgebaseerde malware. Dit omvat alles van Adware (dat de meeste ondersteuningsproblemen veroorzaakt en aanzienlijke netwerkbronnen consumeert) tot kwaadwillende bedreigingen zoals Trojanen, browser Hijackers, browser Helper Objects, Phishing, Pharming, System Monitoring, Keyloggers, Worms, enz.

Belangrijkste differentiators van de oplossing van het Web van Cisco zijn:

1. Een geïntegreerde Layer 4 (L4) Traffic Monitor scant alle poorten met draadsnelheid, detecteert en blokkeert malware en telefoonhome-activiteit. Door alle 65.535 netwerkpoorten te volgen, stopt de L4 Traffic Monitor effectief malware die probeert poort 80 te omzeilen en voorkomt ook robuuste P2P- en IRC-gerelateerde activiteit.
2. Proxylaag-verwerking: De Cisco web security applicatie bevat ook een extreem hoge prestaties van Web proxy, samen met geïntegreerde caching en content Acceleration Services-functies. Het Cisco Web proxy-apparaat is gebaseerd op het eigen besturingssysteem van Cisco, AsyncOS, en kan ondersteuning bieden voor maximaal 100.000 gelijktijdige verbindingen tot 10x meer dan de traditionele UNIX-gebaseerde proxy-servers. Het zijn van een web proxy maakt het mogelijk om uitgebreide content inspectie te maken op de toepassingslaag - een cruciaal vereiste om de nauwkeurigheid te verzekeren tegen op internet gebaseerde malware.
3. De eerste Web Reputation Filters van de industrie voorzien in een krachtige buitenlaag van defensie. Leveraging SenderBase®, Cisco Web Reputation Filters analyseren meer dan 50+ verschillende Web traffic en netwerkgerelateerde parameters om de betrouwbaarheid van een URL nauwkeurig te evalueren. Geavanceerde security modelleringstechnieken worden gebruikt om elke parameter afzonderlijk af te wegen en een enkele score op een schaal van -10 tot +10 te genereren. Beheerder ingesteld beleid wordt dynamisch toegepast, op basis van reputatieschade.
4. Accelerated signatuur scannen met Dynamic Vectoring en Streaming Engine (DVS Engine). In tegenstelling tot oudere architectuuroplossingen die afhankelijk zijn van ICAP en een multibox plaatsing om het scannen van malware te verzekeren, heeft Cisco WSA de DVS Engine voor een geïntegreerde on-box scanoplossing geïntroduceerd. Dit innovatieve platform maakt gebruik van verfijnde objecten parsing- en vectortechnieken, samen met

stream scannen en verzegeling, wat leidt tot een 10x-scandoorvoersnelheid die hoger is dan de op ICAP gebaseerde oplossingen van de eerste generatie.

5. Het anti-Malware-systeem van Cisco dat door de industrie wordt geleid maakt gebruik van de DVS-motor en meerdere typen handtekeningen van Webroot om bescherming tegen de breedste verscheidenheid aan op internet gebaseerde bedreigingen te bieden. Deze bedreigingen kunnen variëren van adware, browser kapers, phishing en pharing aanvallen tot kwaadaardige bedreigingen zoals Trojanen, systeemmonitoren en Keyloggers. WSA biedt de grootste kwaadaardige signatuurdatabase van de industrie aan bij de poort.