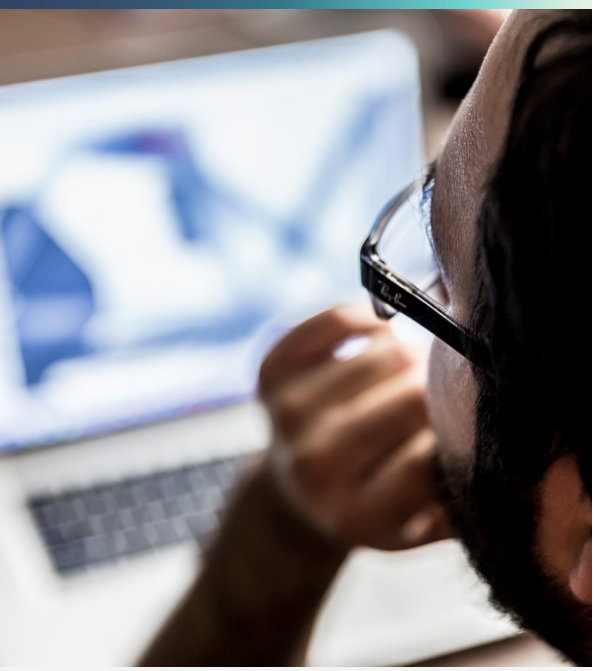
한눈에 보기



혜택

- **위협 가시성과 탐지 효과가 향상되어** IT 보안 팀이 네트워크 전체에 잠복해 있는 새로운 악성코드를 탐지
- **억제 시간이 단축되므로** 감염된 엔드포인트를 위협으로 간주하여 자동으로 빠르게 제거
- 시행을 위해 이미 구축된 Cisco 네트워킹 디바이스 사용을 지원하는 동시에 운영 오버헤드와 **악성코드 관련 비용 절감**

Rapid Threat Containment: Cisco FireSIGHT Management Center 및 Cisco ISE

사고 발생 전에 위협 차단

오늘날 지능형 악성코드는 갈수록 정교하고 은밀해지고 있으며, 속도도 빨라지고 있습니다. 보호가 취약한 디바이스가 IoT(Internet of Things)에서 급증함에 따라 공격 표면이 확장되고 있습니다. 대부분의 조직에는 이상 항목 탐지 기능이 이미 존재하는 만큼, 이제 공격자들은 탐지를 피하고 빠르게 이동하여 중요한 데이터를 빼내는 악성코드를 개발하고 있습니다. 때문에 IT, 보안 및 사고 대응 팀에 있어 효과적인 위협 탐지와 차단은 시간을 다투는 일이 되었습니다.

자동화와 확장성을 갖춘 가속화된 지능형 보안 기능이 필요합니다. 악성코드를 식별하기 위해 지속적으로 위협 인텔리전스를 업데이트하는 지능형 위협 센서가 있다고 가정해 보겠습니다. 이 센서는 감염된 엔드포인트를 빠르고 효율적으로 억제합니다. 이것은 Cisco® FireSIGHT® Management Center 및 ISE(Identity Services Engine) Rapid Threat Containment 솔루션과 함께 사용 가능한 두 가지 기능입니다.

여러 독립형 시스템을 대신하는 통합 솔루션

여러 벤더의 서로 다른 보안 시스템을 통합하는 것은 비용이 많이 들고 복잡합니다. 또한 통합한다고 해도 최신 위협 탐지 및 억제를 제공하지 않는 것이 일반적입니다. 운영 효율성을 향상하고 위협을 빠르게 탐지, 분석 및 억제하는 포괄적이며 긴밀하게 통합된 벤더 지원 솔루션이 필요합니다. Cisco 솔루션은 다음을 제공합니다.

- 네트워크 및 엔드포인트 센서를 사용하여 네트워크 전체에서 위협을 식별하는 우수한 자동 악성코드 탐지
- 위협 및 보안 침해 지표(IoC)에 대한 자동화된 분석 및 자격 부여로, 공격을 빠르게 이해하고 억제하기 위한 상황 가시성을 IT 보안 담당자에게 제공
- 지속적으로 업데이트되는 위협 인텔리전스로 지능형 악성코드에 대한 방어를 개선
- 퍼베이시브 네트워크 적용 기능으로 감염된 엔드포인트를 즉시 억제하거나 치료될 때까지 격리
- 이미 구축된 Cisco 네트워킹 디바이스와의 상호운용성

솔루션 지원

Rapid Threat Containment 솔루션은 Cisco 고객 서비스에서 테스트되고 문서화되며 지원됩니다.

Cisco FireSIGHT Management Center 소프트웨어 릴리스 5.4 및 pxGrid (Platform Exchange Grid) Integration Guide는 솔루션의 올바른 설계 및 운영을 구현하는 데 도움을 줍니다. http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html을 참조하십시오.

솔루션 기능은 표 1에 자세히 설명되어 있습니다.

표 1. 솔루션 기능

지능형 악성코드와 보안 침해 지표(IoC)에 대한 위협 센서는 업계 최고의 지능형 위협 탐지를 사용합니다.	다음과 같은 위협 센서를 구축할 수 있습니다. • 라이센스가 부여된 NGIPS(Next-Generation Intrusion Prevention System)와 Cisco AMP(Advanced Malware Protection)를 포함하는 Cisco ASA with FirePOWER™ Services NGFW(Next-Generation Firewall) • FireSIGHT NGIPS 어플라이언스 • Cisco AMP for Networks 어플라이언스 • Cisco NGIPS 가상화된 차세대 침입 탐지 서비스 • FireSIGHT on Cisco ISR(Integrated Services Router) 어플라이언스
위협 가시성은 네트워크의 위협에 대한 종합적인 보기와 빠르고 자동화된 의사 결정을 내리는 데 필요한 정보가 포함된 IT 보안을 제공합니다.	위협 가시성에는 자동화된 상황 분석 및 위협 자격을 통해 실행 가능한 인텔리전스를 제공하는 Cisco FireSIGHT Management Center가 포함되어 있습니다. IT 보안 팀에서는 Firepower Management Center를 통해 엔드포인트 보안 환경을 파악하고 모니터링합니다. Cisco 센서에 대한 지속적인 위협 인텔리전스 업데이트로 엔드포인트 인텔리전스를 강화합니다.
적용 자동화로 위협 탐지 시 감염된 엔드포인트를 빠르게 억제할 수 있습니다.	자동 적용을 지원하는 기술은 다음과 같습니다. FireSIGHT Management Center: 충분한 심각도의 위협 또는 침해 지표가 감지되면 FireSIGHT Management Center에서 Cisco ISE에 감염된 엔드포인트를 억제하도록 지시합니다. ISE: 이 솔루션은 라우터, 스위치, 방화벽 또는 무선 컨트롤러에 적용 지침을 자동으로 전달하여 감염된 엔드포인트를 억제합니다. 적용 옵션에는 다음이 포함됩니다. • Cisco TrustSec® 기술: 소프트웨어 정의 세그멘테이션은 감염된 엔드포인트를 억제하는 가장 효과적인 방법입니다. 감염된 엔드포인트가 연결된 네트워크 액세스 스위치 또는 컨트롤러에서 적용이 발생하거나 Cisco ASA(Adaptive Security Appliance), Cisco Web Security Appliance 또는 데이터 센터 스위치와 같은 다운스트림 디바이스에서 적용이 발생할 수 있습니다. • dACL(Downloadable Access Control List): Cisco ISE는 dACL 또는 명명된 ACL을 스위치 또는 컨트롤러에 전달하여 스위치 또는 무선 컨트롤러에서 디바이스를 차단하거나 억제할 수 있습니다. • VLAN: ISE는 감염된 디바이스를 격리된 VLAN으로 이동할 수 있습니다.

다음 단계

Cisco FireSIGHT Management Center 및 Cisco ISE에 대한 자세한 내용은 http://cisco.com/go/security를 참조하십시오.

C45-735770-01 10/15