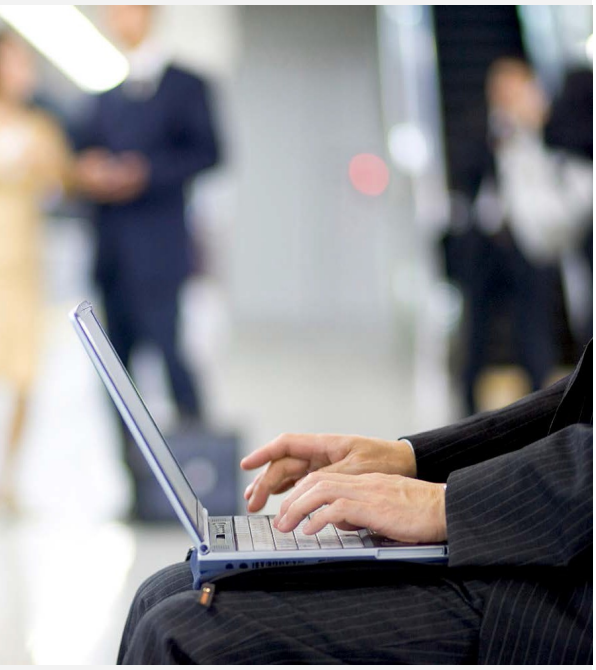
At-A-Glance



혜택

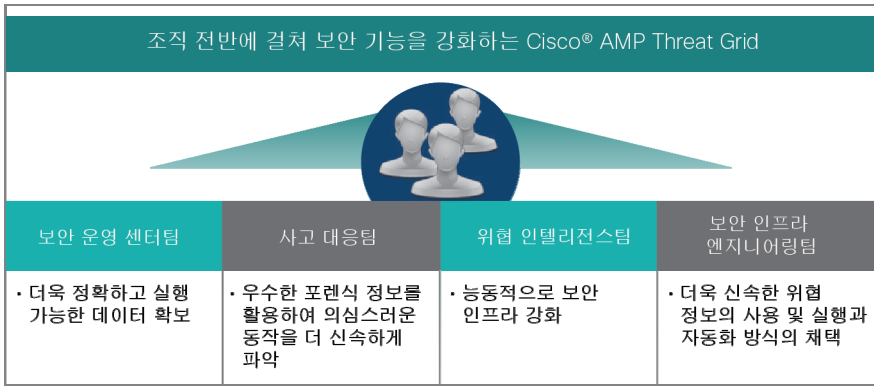
- 기존 보안 기술 및 리소스로 **지능형 공격 방어**
- **보안** 및 대응팀의 **효율성 향상**
- **더욱 신속한 보안 위반 발견 및** 보안 사고 **대응**

"AMP Threat Grid는 지능형 사이버 공격 대처를 위한 조직의 컨텍스트 기반의 정확한 악성코드 분석과 위협 인텔리전스 활용 방식에 혁신적인 변화를 일으키고 있습니다."

Jon Olstik,
ESG Group

Cisco Advanced Malware Protection Threat Grid

그림 1. 보안팀에서 Cisco AMP Threat Grid를 활용하는 방법



다수의 일반 악성코드 및 지능형 악성코드 공격에 시달리는 기업이 늘고 있습니다. 다수의 보안 전문가 또는 IT 관리자는 가장 먼저 처리해야 할 최고 위험도의 공격에 우선 순위를 부여하는 것은 고사하고 공격을 효과적으로 식별하는 것에서조차 어려움을 겪고 있습니다.

이제 걱정하지 마십시오. Cisco® AMP(Advanced Malware Protection) Threat Grid로 통합 악성코드 분석 및 위협 분석 기능을 메일 게이트웨이, SIEM(security information and event management), GRC(governance, risk management, and compliance) 플랫폼과 같은 기존 네트워크 및 보안 인프라에 통합하였습니다. 대규모의 고정 및 동적 악성코드 분석 솔루션을 활용하여 시기적절하고 실행 가능한 컨텍스트 기반의 인텔리전스를 확보하여 악성코드를 식별하고 감소시킬 수 있습니다.

Cisco AMP Threat Grid는 세계 각처에 구축되어 보안 운영 센터 및 사고 대응팀이 더 효과적이고 일관성 있는 조치를 취하는 데 기여하고 있습니다(그림 1).

악성코드와의 전쟁에서 꼭 필요한 두 가지 무기: 통합 악성코드 분석 및 위협 인텔리전스

Cisco AMP Threat Grid는 컨텍스트 기반 분석을 통해 거의 실시간으로 공격을 정확하게 식별합니다. 이 제품은 수백만 개의 파일을 분석하고 그 결과를 이미 분석된 수억 개의 다른 악성코드 아티팩트와 비교하여 연관성을 찾아냅니다. 고객은 악성코드 공격, 캠페인, 그 분포를 종합적으로 파악할 수 있습니다.

다음 단계

Cisco AMP Threat Grid for Cloud에 대한 자세한 내용은 http://www.cisco.com/content/en/us/products/security/amp-threat-grid-cloud/index.html을 참조하십시오.

Cisco AMP Threat Grid Appliance에 대한 자세한 내용은 http://www.cisco.com/content/en/us/products/security/amp-threat-grid-appliances/index.html을 참조하십시오.

Cisco AMP Threat Grid로 다음과 같은 혜택을 누릴 수 있습니다.

- 주요 행동 지표를 파악하고 위협 점수를 산정하여 지능형 공격에 대해 더욱 신속하게 우선 순위를 부여하고 복구
- 팀에서 우선 순위에 따라 신속하고 효율적으로, 자신 있게 대응하도록 지원
- 악성코드 차단 기능을 자동화하여 더 신속하게 탐지하고 대응
- 고급 피드를 SIEM, 침입 탐지 시스템, 게이트웨이, 프록시 등의 기존 보안 인프라에 손쉽게 통합하여 더 신속하게 악성코드를 탐지하고 차단

Cisco AMP Threat Grid는 지능형 공격을 정확하게 탐지하고 방어합니다. 강력한 검색, 상관성 분석, 보고 기능으로 현재 및 과거의 악성코드 아티팩트, 지표, 샘플에 대한 자세한 정보를 제공합니다. 상세 분석 보고서에는 네트워크 트래픽 및 아티팩트를 포함한 모든 악성코드 샘플 활동이 포함되어 있습니다.

C45-733452-00 12/14