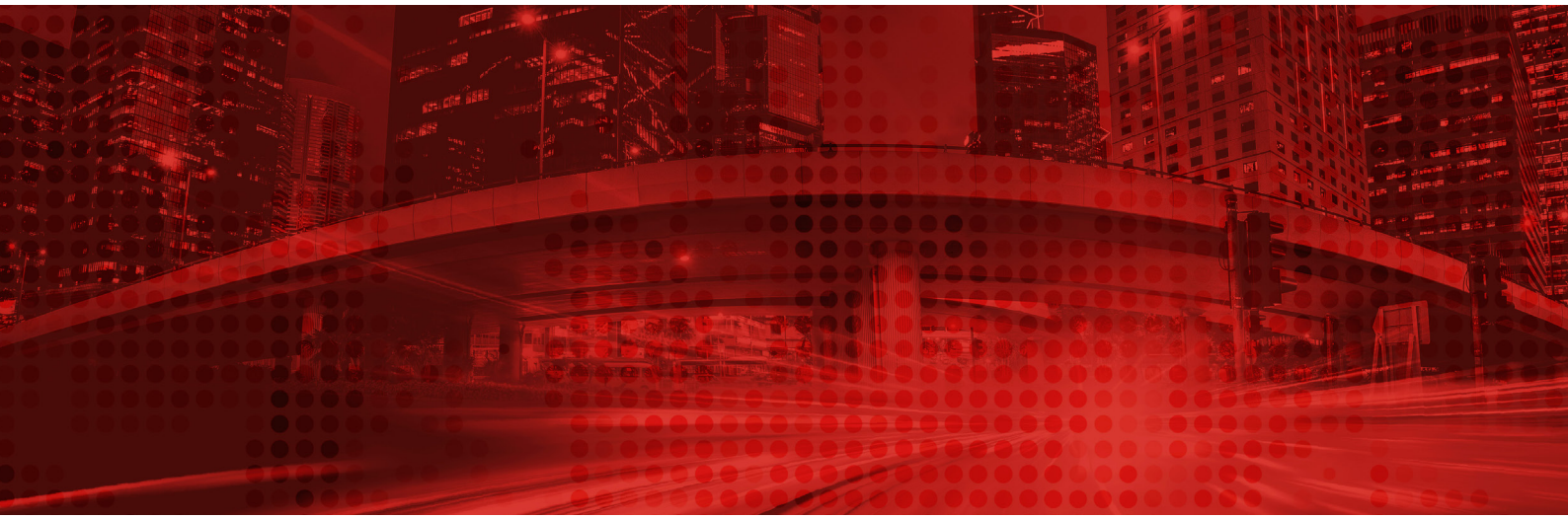
RSA® FRAUDACTION™ 360



소개

온라인 채널은 오늘날 직면하고 있는 혁신적인 글로벌 통합 범죄 네트워크를 경험한 적이 없습니다. 범죄자들은 마음껏 사용할 수 있는 최첨단 기술을 보유하고 있으며 정교한 지하 경제를 운영합니다.

- 피싱이 지속적으로 증가
- 더 정교하고 쉽게 구할 수 있게 된 트로이 목마
- App Store에 침투하는 악성 모바일 애플리케이션
- 가짜 비즈니스 페이지로 가득 찬 소셜 미디어

현재까지 RSA® FraudAction™은 다음과 같은 작업을 수행했습니다.

- 200만 건 이상의 사이버 공격 차단
- 전 세계적으로 10억 건 이상의 사이버 공격 식별
- 수억 건의 손상된 자격 증명 복구

살펴보기

탐지에서 차단까지 피싱, 트로이 목마, 악성 모바일 애플리케이션 및 소셜 미디어 위협에 대한 완벽 보호

최신 온라인 위협을 비롯해 부정 행위 동향에 대한 인텔리전스 보고서 및 피드

온라인 보고 포털인 RSA FraudAction 대시보드를 통한 상세 공격 보고서 액세스

이러한 다양한 유형의 공격들이 점점 더 서로 밀접하게 연관되기 때문에 공격을 막는 것이 무엇보다 중요합니다. 트로이 목마의 경우 종종 모바일 애플리케이션 구성 요소를 가지고 있으며, 소셜 미디어는 사이버 범죄자가 소비자를 속이기 위해 만든 가짜 비즈니스 페이지의 새로운 안식처가 되었습니다.

부정 행위를 완벽하게 방지하기 위해 조직은 여러 공급업체(다양한 서비스 지표, 예산 요구 사항, 다른 공급업체에 의해 다른 위협 요소에 대한 서비스가 제공됨으로 인한 여러 비즈니스 관계)를 관리하거나 하나의 위협 요소만 선별하여 다른 것보다 우선적으로 관리해야 합니다. 하나만 선별하는 경우 특정 공격 유형에 취약하다는 위험을 감수해야 합니다.

RSA FRAUDACTION 360

오늘날의 복잡한 공격 체계를 방어하기 위해, RSA FraudAction 360은 모든 위협 요소를 포괄적인 외부 위협 관리 서비스에 결합하여 피싱, 트로이 목마 공격, 악성 애플리케이션 및 소셜 미디어 위협으로부터의 부정 행위를 완벽하게 방지합니다. 또한 고객은 사이버 범죄에 대한 정보를 제공하는 인텔리전스 보고서를 통해 새로운 위협에 대해 심도 있게 파악할 수 있습니다.

외부 위협 완화

포괄적인 서비스를 사용하면 조직은 다음을 수행할 수 있습니다.

- 더 적은 사내 리소스로 외부 위협 관리
- 위협 요소를 남기지 않고 완벽하게 부정 행위를 방지
- 24X7 부정 행위 방지 작업에 대한 단일 공급업체의 예산만 관리 가능

RSA FraudAction 360 외부 위협 관리 서비스는 다음과 같은 구성 요소를 제공합니다.

- 피싱 방지
- 트로이 목마 방지
- 악성 모바일 애플리케이션 방지
- 소셜 미디어 위협 차단
- RSA FraudAction Cyber Intelligence 데이터 피드 및 보고서 선택

피싱 방지

RSA FraudAction은 피싱 공격을 탐지하고 최소화합니다. 이 서비스는 조직이 공격을 받을 때 대응하고 공격을 받은 후에는 자세한 포렌식 수행을 지원하도록 설계되었습니다.

모니터링 및 조기 탐지

RSA에 새로 등록된 도메인과 고객의 웹 로그를 모니터링을 포함해 여러 초기 탐지 전략을 사용합니다. RSA FraudAction의 탐지 리소스를 통해 RSA의 분석가는 고객의 남용 사서함을 포함하여 하루에 수십억 개의 URL을 검사하고, 의심스러운 URL을 자동으로 발견하고 수동으로 검증할 수 있습니다.

실시간 알림 및 보고

의심스러운 URL이 위협으로 확인되면 고객은 즉시 알림을 받고 RSA FraudAction 대시보드를 통해 실시간으로 최신 위협 정보 및 상태를 모니터링할 수 있습니다. 또한 온라인 보고 포털은 업계 및 지역 동향뿐만 아니라 차단에 걸리는 기간도 제공합니다.

독점 사이트 차단 네트워크

RSA는 모바일 브라우저 및 주요 데이터 보안 공급업체 및 ISP의 고객을 포함해 모든 주요 인터넷 브라우저 사용자에 대한 차단 피드를 통해 전 세계 웹 트래픽의 96% 이상을 보호하는 1차 방어선입니다. 공격이 확인되는 즉시 피싱 사이트의 실시간 피드를 이러한 조직에 전송하여 탐지 후 몇 분 이내에 피싱 사이트를 차단할 수 있습니다.

피싱 사이트 차단

RSA는 전 세계의 16,000개 이상의 다양한 호스팅 기관과의 오랜 관계 및 다국어 역량을 통해 글로벌 규모로 신속하게 부정 사이트를 차단할 수 있습니다. 현재까지 RSA는 187개 이상의 국가에 호스팅된 100만 개 이상의 부정 사이트 차단에 관여했습니다.

트로이 목마 방지

RSA FraudAction은 트로이 목마 공격으로 인한 피해를 탐지하고 최소화합니다. 이 서비스는 멀웨어 보안 위협을 포착하고, 공격이 발생할 때 대응하며, 공격에 이용된 온라인 리소스에 대한 최종 사용자 액세스를 차단하여 보안 위협을 최소화하도록 설계되었습니다.

식별 및 분석

RSA FraudAction은 높은 수준의 탐지를 위해 파트너 네트워크를 형성했습니다. 이 네트워크는 소비자 안티바이러스 회사, 인텔리전스 운영 및 인터넷 게이트웨이를 비롯해 여러 기술 분야의 조직을 포함합니다.

RSA FRAUDACTION 위협 보고서

RSA FraudAction 360 고객은 부정 행위 동향, 새로운 사기 수법, 음지에서 제공된 새로운 사이버 범죄 툴 및 서비스와 같은 인텔리전스에 대한 위협 보고서를 받습니다.

RSA FraudAction 위협 보고서는 부정 행위자가 타겟 조직에게 사용하는 현금 인출 방법 또는 기타 방법 등 현재 부정 행위자가 사용하고 있거나 새로 발견된 취약성을 고객에게 알립니다.

RSA FraudAction 파트너가 멀웨어를 탐지하면 조사를 위해 트로이 목마의 정보가 RSA AFCC(Anti-Fraud Command Center)로 전송됩니다. 전문 분석가는 정적 분석 및 동적 분석을 수행하여 트리거, 통신 지점 및 기타 데이터를 비롯해 감염된 시스템에서 트로이 목마의 작동 방식을 밝혀냅니다. 가능한 경우, 유출된 최종 사용자 자격 증명을 복구 시도를 위해 트로이 목마의 드롭 지점을 모니터링합니다.

차단

RSA는 고객을 대신해 각 공격의 감염 지점에 연결된 부정 사이트를 차단합니다. 부정 사이트가 발견하고 이를 분석한 다음 RSA AFCC는 ISP, 웹 호스팅 시설 및 도메인 등록 공급업체와의 상호 작용을 통해 정지 명령 절차로 사이트 차단을 시작합니다.

악성 모바일 애플리케이션 방지

RSA FraudAction은 조직이 악성 또는 허가되지 않은 불법 모바일 애플리케이션에 대응함으로써 부정 행위로 인한 손실을 줄이도록 지원합니다. 이 서비스는 주요 App Store를 모두 모니터링하고 조직의 고객 기반을 표적으로 하는 애플리케이션을 탐지하며, 허가되지 않은 애플리케이션을 차단하여 모바일 애플리케이션 부정 행위로 인한 조직의 평판 훼손과 재정적 손실 발생의 위험을 줄입니다.

모니터링 및 탐지

이 서비스는 모바일 App Store에 지속적으로 가시성을 제공하여 조직에 사전 예방적인 온라인 방어를 제공합니다. App Store에 대한 지속적인 모니터링을 통해 조직은 잠재적인 위협을 미리 예측하고 승인되지 않은 애플리케이션이 나타나는 즉시 인식할 수 있습니다.

악성 애플리케이션 차단

탐지 및 차단 승인 후 RSA는 악성 애플리케이션 제거를 시작합니다. 해당 서비스를 통해 고객은 자신의 조직을 나타내는 애플리케이션을 제어할 수 있어, 조직에서 발행 및/또는 승인한 애플리케이션만 애플리케이션 마켓에서 사용하도록 할 수 있습니다. 또한 해당 서비스를 통해 악성 애플리케이션이 App Store 내에서 노출되고 인기를 얻기 전에도 고객 및 수억 명의 온라인 모바일 애플리케이션 사용자가 피싱, 멀웨어 및 기타 무단 애플리케이션에 액세스하지 못하게 막을 수 있습니다.

고객 피드백

> “RSA FraudAction을 구축해 피싱 공격을 무력화하는 데 걸리는 시간을 몇 주에서 단 몇 시간으로 단축할 수 있었습니다. 또한 부정 행위를 효과적으로 방지함으로써 수백만 코루나에 달하는 손실 비용을 막을 수 있었습니다. 이는 우리에게도 좋은 소식이지만 무엇보다 고객에게 가장 반가운 소식일 것입니다.”

Large European FI

소셜 미디어 위협 차단

소셜 미디어는 조직의 브랜드 및 관련 서비스 오퍼링을 클라이언트와 엮어 주는 통합 통신 패브릭으로 떠올랐습니다. 새로운 소셜 스레드를 통해 위협 요소가 등장하자, 사이버 범죄자는 소셜 미디어 페이지를 남용하여 부정 행위를 저지르거나 부정 행위 계획에 착수했습니다. 조직은 수작업인 사내 옵션으로 위험 관리에 대한 요구를 해결하기 위해 소셜 미디어를 비롯한 디지털 채널 전반의 위험을 지속적으로 모니터링해야 합니다.

RSA FraudAction은 소셜 미디어 페이지에 대한 가시성을 제공하고 조직이 승인된 비즈니스 페이지와 잠재적으로 위험한 페이지를 구분할 수 있도록 설계되었습니다. 소셜 미디어 모니터링을 통해 RSA FraudAction은 조직을 대상으로 하거나 조직 및/또는 계열사로 행세하며 클라이언트를 속이려는 부정한 활동에 직접 연결된 페이지를 식별합니다. RSA FraudAction을 통해 조직은 심각하고 오래 지속되는 피해가 발생하기 전에 소셜 미디어 부정 행위 위협을 신속하게 해결할 수 있습니다.

RSA FRAUDACTION CYBER INTELLIGENCE

RSA FraudAction Cyber Intelligence는 사이버 범죄 동향에 대한 자세한 분석 정보와 비밀리에 이루어지는 전 세계 사이버 범죄의 부정 행위 수법 및 작업에 대한 심층적인 조사 결과를 제공합니다.

RSA FraudAction Cyber Intelligence 계층 1 서비스에서 제공되는 무료 피드와 보고서는 추가 비용 없이 RSA FraudAction 360에 포함됩니다. 이러한 위협 보고서와 데이터 피드는 다른 백엔드 시스템에 쉽게 통합될 수 있습니다.

RSA FRAUDACTION 360 INTELLIGENCE 제공 서비스:

- **IP 피드:** 프록시/SOCKS 및 RDP와 같은 위험성이 높은 IP로 구성된 일일 목록
- **이메일 피드:** 유출된 기업의 개인 직원 이메일 주소 및 스팸 이메일의 일일 목록
- **뮬 계정 피드:** RSA 인텔리전스 분석가가 복구한 뮬 계정으로 구성됨
- **아이템 드롭 피드:** 도난당한 카드로 구매한 품목을 "재배송 운반책"이 받는 실제 우편물 "배달지" 주소로 구성됨
- **신용 카드 피드:** 음지에서 추적되는 유출된 신용/직불 카드의 상세 정보로 구성됨
- **분기별 뉴스레터:** 글로벌 피싱 통계 및 트로이 목마 통계뿐만 아니라 지난 분기에 보고된 경향에 대한 개요
- **위협 보고서:** 사이버 범죄의 새로운 공격 방법 및 동향에 대한 조사 결과 보고서

RSA FRAUD & RISK INTELLIGENCE SUITE 소개

RSA® Fraud & Risk Intelligence Suite는 조직이 소비자 대상 디지털 채널 전반에 걸친 위험을 관리하여 매출을 극대화하고 부정 행위로 인한 손실을 최소화하도록 지원합니다. 이 제품군은 비즈니스 중심의 보안 솔루션으로 꾸려진 RSA 포트폴리오의 일부로서 통합된 가시성, 자동화된 분석 정보 및 조율된 작업에 따라 디지털 위험을 관리하는 통합된 접근 방식을 제공합니다. RSA는 전 세계 수백만 명의 사용자를 보호하고, Fortune지 선정 500대 기업의 90%가 넘는 기업이 성장하고 혁신 변화에 지속적으로 적응할 수 있도록 지원합니다. 자세한 내용은 rsa.com/ko-kr을 참조하시기 바랍니다.