XDR 구매자 가이드

XDR(확장 탐지 및 대응) 시장에서 전문가답게 길을 모색하는 방법

Contents

XDR(확장 탐지 및 대응) 이해하기

전 세계적으로 또 다른 보안 접근 방식이 필요한 이유는 무엇일까요?

오늘날의 하이브리드 멀티 벤더 및 멀티 벡터 환경에서는 복잡성이 가장 큰 과제입니다. 보안 팀은 비일관적으로 통합된 수십 개의 툴에서 운영을 실행하면서 계속해서 확장되는 에코시스템을 보호해야 합니다. 사물 인터넷(IoT)과 하이브리드 업무는 공격 표면의 확대로 이어졌습니다. 피싱, 악성코드, 랜섬웨어의 수가 매년 두 배, 때로는 세 배씩 늘어나고 있습니다. 동시에 기업들은 그 어느 때보다도 고도로 연결되어 있습니다. 한 회사에서 보안 침해를 당하면 그 회사의 공급업체, 파트너, 고객, 심지어는 경제부문 전체가 영향을 받기도 합니다.

이러한 새로운 뉴노멀에는 기업이 예측할 수 없는 위협이나 변화를 극복하고 더욱 강력하게 부상할 수 있도록 모든 측면의 무결성을 보호하는 역량인 보안 탄력성이 필요합니다. 또한 보안 팀에는 과거에 제공되었던 것 이상의 것이 필요합니다.

어떤 솔루션일까요?

위협이 점점 정교해지고 있으므로 자립형 포인트 보안 솔루션에 구축된 기존의 탐지 및 대응 모델만으로는 부족합니다. 이런 상황에서는 통합 보안 사고 탐지 및 대응 툴인 XDR(확장 탐지 및 대응)이 유용합니다. XDR 솔루션은 여러 보안 툴에서 텔레메트리를 자동으로 수집하고 연관성을 파악하고 분석을 적용해 악의적인 활동을 탐지한 다음 위협에 대응하고 이를 해결합니다. 효과적인 XDR 솔루션은 이메일, 엔드포인트, 서버, 클라우드 워크로드, 네트워크 등 모든 벡터에서 데이터의 상관관계를 파악하므로 포괄적입니다. 따라서 아무리 고도로 발달된 위협이 발생해도 환경 전체에 대한 가시성과 컨텍스트를 확보할 수 있습니다.

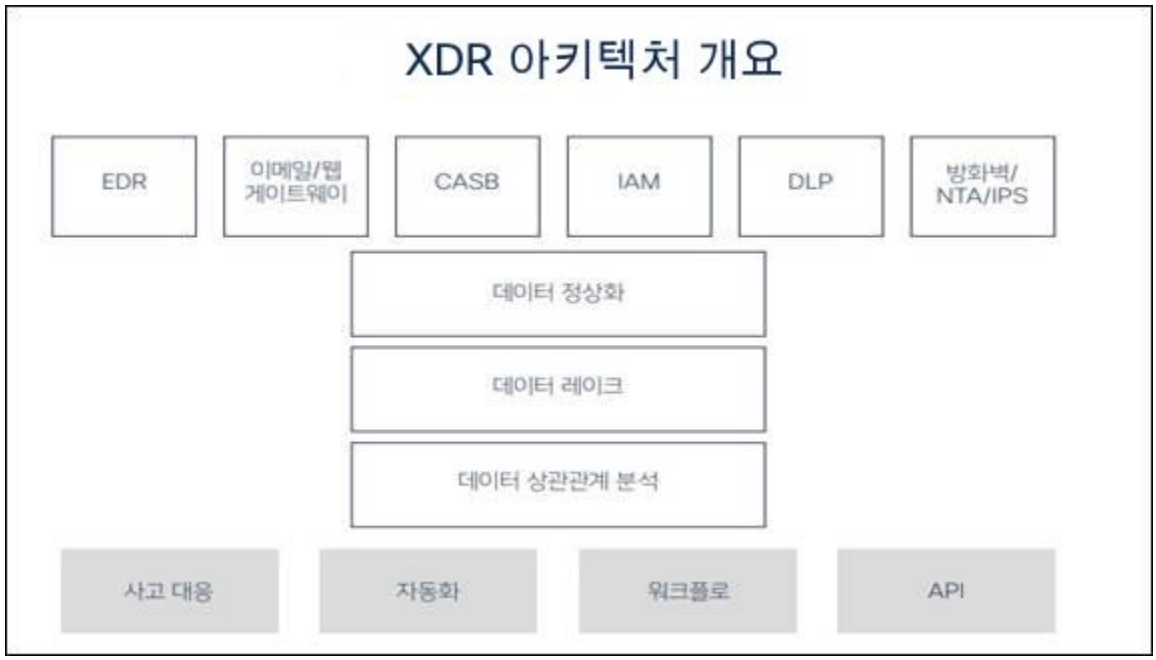
XDR을 사용해야 하는 이유는 무엇일까요?

첫째, XDR을 사용하면 네트워크, 클라우드, 엔드포인트, 이메일 등에서 이벤트 상관관계와 멀티 벤더 탐지를 통해 가장 정교한 위협도 탐지할 수 있습니다.

둘째, XDR을 사용하면 영향에 따라 위협의 우선순위를 지정할 수 있으므로 경보 피로가 줄어듭니다.

셋째, 작업 자동화를 통해 생산성을 높여주므로 SOC 리소스를 더욱 효율적으로 사용할 수 있습니다.

넷째, 보안 격차를 줄이고 실행 가능한 인텔리전스를 통해 다음 단계를 예측함으로써 보안 탄력성을 구축하는 데 도움이 됩니다.



XDR을 올바르게 구현하기 위한 5가지 핵심 요소

1. 필요한 곳 어디든 우선순위가 지정되고 실행 가능한 텔레메트리 제공

귀사에서는 경보의 바다에서 효율적으로 위협을 분류할 수 있습니까?

가시성의 폭과 인사이트의 깊이가 XDR의 기본 원칙입니다. 정교한 위협은 대부분 엔드포인트나 네트워크만을 공격하지 않습니다. 이메일, 엔드포인트, 네트워크, ID 관리, 샌드박싱, 방화벽 등 다양한 벡터를 공격합니다. 따라서 광범위한 텔레메트리와 고품질의 데이터를 제공하는 XDR 솔루션이 필요합니다.이러한 XDR 솔루션은 XDR 결과를 도출하고 환경에서 어떤 일이 벌어지고 있는지에 대해 종합적이고 완전한 뷰를 제공합니다. 하지만 인사이트를 수집하는 것뿐만 아니라 사고를 관리하는 것도 중요합니다. XDR이 약속하는 효과를 누리기 위해서는 이러한 인사이트의 우선순위를 지정해야 합니다. 위험 기반 우선순위 지정 기능(실질적인 위험이 가장 높은 사고에 우선순위를 둠)을 제공하는 XDR 솔루션을 사용하면 진정으로 중요한 사안에 신속하게 행동을 취할 수 있습니다. 또한 XDR 솔루션은 정보를 바탕으로 가장 효과적인 조치를 결정할 수 있도록 다음 단계도 제안해야 합니다.

주요 기능	관련 제품 영역
• 오탐으로 인한 노이즈를 최소화하는 효율성 및 정확성 • 환경 전체에서 경보 집계 및 상관관계 파악	EDR(엔드포인트 탐지 및 대응)
• 지속적인 실시간 네트워크 모니터링	NDR(네트워크 탐지 및 대응)
• 알 수 없는 악성코드 및 기타 정교한 네트워크 공격이 탐지되었을 때 컨텍스트와 함께 우선순위가 지정된 경보를 생성하는 고급 분석	XDR(확장 탐지 및 대응)
• 지속적인 실시간 이메일 위협 모니터링 및 자동 해결 우선순위 지정	이메일 보안

벤더에게 해야 할 질문

- 귀사의 솔루션은 당사의 환경 전체(엔드포인트, 디바이스, 네트워크) 전체에 어떻게 가시성을 제공합니까?
- 귀사의 솔루션은 인사이트를 어떻게 제공합니까? 귀사의 솔루션은 우선순위가 지정된 텔레메트리를 제공합니까?
- 귀사의 솔루션은 비즈니스 영향 및 위험에 따라 위협의 우선순위를 어떻게 지정합니까?
- 탐지에 어떤 종류의 위협 정보를 사용합니까? 그 정보는 어디에서 가져옵니까?
- 귀사의 솔루션에 사용하는 데이터 소스는 어떻게 검증합니까?
- 이 제품이 Wannacry, NotPetya, Turla와 같은 정교한 위협을 어떻게 처리합니까?

2. 벡터나 벤더와 상관없이 통합된 탐지 지원

귀사의 XDR 솔루션은 보안 투자가 조화를 이루어 효과를 내도록 지원합니까?

위협이 더욱 정교해지고 다양한 공격 벡터에 걸쳐 발생하므로 환경 전체를 일관적으로 탐지하는 것이 그 어느 때보다도 중요해졌습니다. 오늘날의 보안 팀은 보안 환경과 전 세계 공급망, 공격자, 디펜더의 에코시스템 내에서 엄청난 수준의 복잡성을 다루고 있습니다. XDR 솔루션을 사용하면 심각도와 영향에 따라 탐지를 집계하고, 상관관계를 분석하고, 우선순위를 지정하므로 보안 팀에 도움이 됩니다. 그러나 이를 위해서는 보안 스택이 조화를 이루어 작동해야 합니다. 개방적이고 확장 가능하며 클라우드를 중심으로 하는 XDR 솔루션을 선택하면 또 다른 복잡성을 추가하지 않고 환경 전체에서 통합된 탐지와 이벤트 상관관계 분석의 이점을 누릴 수 있습니다. 보안 스택의 각 구성 요소는 고유한 탐지 요소(네트워킹, 이메일, 방화벽 등)를 갖고 있는데, 이를 서로 조합하면 더욱 강력한 기능을 발휘합니다. XDR이 엔드포인트, 네트워크, 방화벽, 이메일, ID, DNS라는 여섯 개의 텔레메트리 소스를 모두 아울러 잠재적 위협을 종합적으로 시각화할 수 있어야 한다는 점을 고려해야 합니다. 귀사의 XDR 솔루션은 네이티브 백엔드-프론트엔드 통합을 통해 귀사의 전체 보안 스택과 손쉽게 통합되어야 합니다. 그래야만 벤더가 포트폴리오를 변경하거나 벤더를 변경하더라도 보안이 일관적으로 유지됩니다. 마지막으로, 보안 스택의 위협 탐지 기능을 최적화하려면 귀중한 로컬 컨텍스트를 제공하고 신뢰할 수 있고 정확한 위협 정보 판단을 내리는 XDR 솔루션을 살펴보는 것이 좋습니다.

주요 기능	관련 제품 영역
• 익스플로잇 기반 메모리 주입 공격 등 비정상적 엔드포인트 실행 프로그램 동작 탐지 및 차단 • MITRE ATT&CK 매핑을 통한 IoC(침해 지표) 파악 • 파일 평판 모니터링으로 엔트리 포인트에서 위협 탐지 및 격리 • 관리자가 위험에 따라 해결 우선순위를 지정하고 공격 표면을 줄일 수 있도록 환경에서 OS 취약성 식별	EDR(엔드포인트 탐지 및 대응), 취약성 관리
• 지능형 분석을 사용하여 알 수 없는 악성코드, 데이터 유출과 정책 위반 등의 내부자 위협 및 기타 정교한 공격을 빠르게 탐지 • 실시간으로 네트워크 공격 탐지 및 높은 신뢰도의 경보 제공	XDR(확장 탐지 및 대응), NDR(네트워크 탐지 및 대응)
• 평판 필터링으로 원치 않는 이메일 탐지 및 차단 • 소셜 엔지니어링, 사칭자 등 속임수 기반 이메일 공격 식별 및 방지	이메일 보안

벤더에게 해야 할 질문

- 귀사의 XDR 플랫폼이 당사의 기존 투자를 어느 정도 활용할 수 있습니까?
- 귀사의 XDR 플랫폼이 벤더와 상관없이 당사의 솔루션과 호환됩니까?
- 귀사의 솔루션들이 서로 기본적으로 통합됩니까?
- 귀사의 탐지 기술이 시장에 출시된 다른 제품보다 나은 점은 무엇입니까?
- 귀사의 솔루션으로 탐지할 수 있는 위협 종류는 무엇입니까? 귀사의 솔루션은 MITRE ATT&CK 프레임워크에 경보를 매핑합니까?

3. 빠르고 정확한 위협 대응 지원

위협을 식별하고 나면 얼마나 빠르고 자신 있게 위협에 대응할 수 있습니까?

네트워크, 엔드포인트, 이메일 등에서 얻은 인사이트를 통합하면 어떤 일이 일어났는지, 진행 상황은 어떤지, 위협을 해결하기 위해서는 어떤 조치를 취해야 하는지 더욱 정확히 이해할 수 있습니다. 한 위치에서 위협이 미치는 영향과 범위를 확인하고 클릭 한두 번으로 조치를 취할 수 있는 형태가 가장 이상적입니다. 효과적인 XDR은 호스트 격리, 모든 받은 편지함에서 악성 이메일 삭제 등 기본적으로 대응 및 해결 기능을 갖추고 있어야 합니다. 또한, XDR은 시간이 지나면서 팀이 보안을 발전시킬 수 있도록 자동화 기회를 제공하고 맞춤형 대응 조치를 쉽게 만들 수 있도록 지원해야 합니다.

주요 기능	관련 제품 영역
• 침해 후 신속하게 엔드포인트 위협에 대응	EDR(엔드포인트 탐지 및 대응)
• 몇 초 만에 네트워크 문제 또는 사고의 침입 경로 식별 및 격리	XDR(확장 탐지 및 대응), NDR(네트워크 탐지 및 대응)
• 실시간 클릭 시간 분석으로 악성 웹사이트 차단	이메일 보안

벤더에게 해야 할 질문

- 귀사의 제품은 어떤 대응 조치를 제공합니까?
- 한 위치에서 XDR 솔루션을 사용하여 엔드포인트에 해결 조치를 수행한 후 다른 위치로 확장할 수 있습니까?
- 귀사의 제품은 대응을 지원하는 기존의 보안 툴과 어떻게 통합됩니까?
- 귀사의 솔루션은 문제 해결을 어떻게 가속화합니까?
- 위협 알림에서 해결까지 대응 시간이 어떻게 됩니까(예: 피싱 공격의 경우)?

4. 간소화된 사용자 경험을 위해 하나의 조사 관점 제공

귀사에서는 위협 탐지, 대응, 해결을 하나의 인터페이스에서 관리합니까?

XDR 솔루션을 평가할 때는 보안 분석가의 경험을 고려하는 것이 중요합니다. 보안 운영 팀에서는 관리할 사항이 많기 때문에 수많은 툴과 콘솔로 업무 효율을 저하해서는 안 됩니다. 따라서 시스코에서는 분석가가 여러 보안 툴과 데이터 소스에 걸쳐 보안 데이터에 대한 통합된 뷰를 제공하여 위협을 더 신속하고 효과적으로 탐지하고 대응할 수 있도록 지원하는 XDR 솔루션을 권장합니다. 이러한 솔루션은 워크플로우를 간소화하고 보안 사고를 조사 및 해결하는 데 필요한 시간과 노력을 절약하는 데 도움이 됩니다. XDR 솔루션은 모든 위협 벡터와 액세스 포인트를 아우르는 전체 라이프사이클 대시보드를 제공해야 합니다. MITRE ATT&CK 같은 모델을 통해 위협 추적을 용이하게 함으로써 프로세스를 새로 접하는 사용자가 가설에 기반한 위협 추적에 쉽게 접근할 수 있도록 하고 다음 단계를 쉽게 예측하도록 해야 합니다. 고려해야 할 또 다른 요인은 디자인이 분석가 경험에 미치는 영향입니다. XDR 솔루션은 생산성을 높이고 주요 탐지, 조사, 대응 기능과 관련한 의사결정 시간을 단축해야 합니다. 또한 점진적인 공개를 통해 경보에 대해 더 효과적인 컨텍스트를 제공함으로써 초급에서 중급 수준의 분석가가 보안 운영 내에서 고급 수준의 작업을 수행하여 잠재적인 위협의 범위와 심각도를 빠르게 판단할 수 있도록 해야 합니다.

주요 기능	관련 제품 영역
• 모든 위협 벡터와 액세스 포인트를 아우르는 전체 라이프사이클 대시보드 제공 • IT 운영, 보안 운영, 네트워크 운영으로 확장되는 통합된 툴 세트 제공 • 하나의 통합된 위치에서 데이터, 애널리틱스, 자동화 액세스 및 관리	XDR(확장 탐지 및 대응)

벤더에게 해야 할 질문

- 귀사의 솔루션은 팀의 위협 추적 업무를 어떤 방식으로 지원합니까?
- 귀사의 솔루션은 SOAR, SIEM 솔루션 등 기존의 보안 기술과 어떻게 통합됩니까?
- 귀사의 XDR을 사용하여 위협의 영향력을 파악하고 보안 침해의 범위를 발견하고 단일 인터페이스에서 클릭 한 번으로 조치를 취할 수 있습니까?
- 귀사의 솔루션은 시스템/하위 시스템 액세스의 전체 또는 부분을 권한이 있는 그룹 및 개별 사용자로 제한하는 역할 기반 보안을 지원합니까?
- 당사의 모든 기존 보안 기술에서 텔레메트리를 중앙화하고 분석할 수 있습니까?
- 귀사의 솔루션은 사고 대응 워크플로우를 간소화하여 전반적인 조사 타임라인을 단축합니까?

5. 생산성을 높이고 보안 강화 태세를 제공

귀사의 XDR 솔루션은 더 적은 오버헤드로 위협 탐지와 대응 효율성을 높입니까?

회사의 보안 탄력성을 구축하는 데 있어 중요한 요소는 자동화와 오케스트레이션입니다. 보안 직원은 중요한 임무를 수행해야 합니다. 보안 위협이 발생했을 때 복잡하고 수동적이며 반복적인 워크플로우로 이들의 시간을 잡아먹을 수는 없습니다. 알림 발견, 알림 상관관계 분석, 신속한 대응 조치 우선순위 지정 및 수행 등과 같은 핵심 워크플로우를 자동화하여 생산성을 높이는 XDR 솔루션은 전체 라이프사이클에서 팀의 업무 부담을 줄여줍니다. 효과적인 XDR 솔루션은 명확한 의사결정과 조치를 제시하는 조사를 가능하게 함으로써 평균 대응 시간을 줄일 수 있어야 합니다. 이를 통해 분석가는 정책과 절차에 따라 자동화되고 일관적인 방식으로 대응할 수 있습니다. 이렇게 하면 보안 운영 팀이 여유 시간과 에너지를 더 전략적이고 사전 예방적인 보안 작업에 투자하여 회사의 보안 태세를 한층 더 강화할 수 있게 됩니다.

주요 기능	관련 제품 영역
• 발생률이 낮은 위협을 비롯한 자동 엔드포인트 위협 추적 • 관리자가 IoC(침해 지표)를 직접 작성하여 스캔 가능	EDR(엔드포인트 탐지 및 대응)
• 동작 분석을 바탕으로 한 인사이트로 예측형 네트워크 위협 해결	XDR(확장 탐지 및 대응), NDR(네트워크 탐지 및 대응)
• 이메일 위협 해결 우선순위 지정 자동화	이메일 보안

벤더에게 해야 할 질문

- 서드파티 통합 시 벤더가 API를 변경하면 자동화 스크립트가 깨집니까?
- 귀사의 솔루션은 들어오고 나가는 클라우드 기반 워크로드에 대한 모니터링을 어떻게 지원합니까?
- 귀사의 XDR 솔루션을 사용하려면 환경을 변경하거나 새로운 기술을 구축해야 합니까?
- 귀사의 XDR 솔루션은 서드파티 보안 기술과의 사전 구축 및 기본 통합을 제공합니까?
- 귀사의 XDR 솔루션은 사고 조사 및 해결에 필요한 분석가의 시간을 단축해 줍니까?
- 귀사의 XDR 솔루션은 탄력성 구축을 위한 정책 관리에 정보를 제공합니까?

Cisco XDR

XDR은 보안 탄력성의 중요한 구성 요소

오늘날에는 불확실성이 당연한 것입니다. 따라서 기업들은 재무에서 공급망까지 비즈니스의 모든 측면에서 탄력성을 구축하는 데 투자하고 있습니다. 그러나 보안 탄력성에 투자하지 않는다면 이 모든 노력은 소용이 없습니다. 보안 탄력성이란 위협과 중단으로부터 비즈니스를 보호하고 변화에 자신 있게 대응하여 역량을 한층 더 강화하는 것을 말합니다.

XDR은 비즈니스를 위한 보안 탄력성을 수용하는 중요한 구성 요소입니다. XDR을 제대로 사용하면 보안 팀이 영향별로 위협의 우선순위를 지정하고 위협을 더욱 빨리 탐지하고 대응을 가속화하도록 지원함으로써 보안 태세를 향상할 수 있습니다. 자동화와 오케스트레이션 기능이 이러한 프로세스를 촉진하여 보안 팀의 업무 부담을 줄여 주기 때문에 보안 팀은 가장 중요한 일에 집중할 수 있습니다.

Cisco XDR을 통한 보안 운영 간소화

시스코는 시중에서 가장 포괄적인 보안 포트폴리오로 XDR 분야를 선도하고 있습니다. 시스코에서는 미래에 보안에 대한 요구가 커질 것을 예측하고, 벤더나 벡터와 상관없이 모든 팀이 효과적인 보안을 간편하게 활용할 수 있도록 구성 요소를 통합함으로써 시중에서 가장 포괄적인 보안 포트폴리오를 만드는 데 적극적으로 투자했습니다. XDR 접근법을 구축하는 것은 하나의 프로세스이므로 포인트 솔루션이 포화 상태를 넘어선 업계에서 임시방편적인 보안을 이어가는 악순환을 끊어내야 합니다. 시스코에서는 Cisco XDR을 통해 탐지에서 대응까지 가장 짧은 경로를 가장 원활하게 제시하고자 했습니다.

SOC 전문가가 SOC 전문가를 위해 설계한 Cisco XDR은 보안 운영을 간소화하여 보안 분석가가 아무리 정교한 위협도 차질 없이 사전에 예방하고 탄력성을 유지할 수 있도록 돕습니다. Cisco XDR은 개방적이고 확장 가능한 클라우드 우선 솔루션이므로 기존 보안 투자를 활용하고 전체 환경에 걸쳐 보안을 통합적으로 탐지할 수 있습니다.

시스코는 고객의 자산 보호를 중요시합니다. 시스코 역시 고객의 고객이기 때문입니다. 시스코는 어떤 위협에서도 귀사의 전체 에코시스템을 보호하도록 지원하는 개방형 보안 플랫폼인 Cisco Security Cloud를 통해 보안 탄력성을 구축하는 귀사의 여정에서 협력하고자 합니다. 시스코와 함께 포괄적인 보안의 강력한 힘을 경험해 보세요.

미래의 보안 운영을 지금 바로 구축할 준비가 되셨나요?

Cisco XDR 살펴보기

XDR의 주요 요소 및 기능

XDR 벤더와의 대화 중에 이 테이블(9~10페이지)을 빠른 참조용으로 사용하세요.

핵심 요소	주요 기능	관련 시스코 제품
필요한 곳 어디든 우선순위가 지정되고 실행 가능한 텔레메트리 제공	• 완전 관리형 사전 예방적 위협 추적이 가능한 기본 내장 EDR(엔드포인트 탐지 및 대응) • 신속한 취약성 식별, 위협 점수 지정, 우선순위 지정, 해결을 지원하는 통합된 위협 기반 취약성 관리	Secure Endpoint
	• 지속적인 클라우드 활동 분석 • 동작 모델링 및 머신러닝 알고리즘을 비롯한 고급 분석 • 통합된 가시성 및 집계된 실행 가능한 인텔리전스를 제공하는 보안 인프라스트럭처의 단일 뷰	Cisco XDR
	• 실시간 클릭 시간 분석을 제공하는 고급 아웃브레이크 필터	Secure Email
벡터나 벤더와 상관없이 통합된 탐지 지원	• 비정상적 실행 프로그램 동작의 실시간 탐지 및 차단 • 실시간으로 엔드포인트에 고급 OS 쿼리 가능 • MITRE ATT&CK 프레임워크에 매핑되는 기본 내장 위협 추적	Secure Endpoint
	• 사용자, 디바이스, 위치, 타임스탬프, 애플리케이션 등의 컨텍스트가 다양하게 포함되어 있는 신뢰도 높은 알림으로 클라우드에서 실시간으로 공격 탐지 • 확인된 탐지로 위협 탐지 및 격리 • NDR로 비인가 엔터티 탐지 및 엔드포인트로 자동 격리 • 외부 호스트와 통신하는 내부 호스트 탐지 • 보다 효과적인 포렌식 조사를 위해 모든 클라우드 트랜잭션에 대한 완전한 감사 추적 제공 • 포트폴리오의 다른 XDR 솔루션과 기본 내장 통합 • 기본 내장, 사전 구축 또는 맞춤형 통합으로 서드파티 솔루션과 통합을 통해 연결된 백엔드 아키텍처 및 일관적인 프론트엔드 경험 제공 • 클라우드, 엔드포인트, 네트워크, 애플리케이션 전체에서 다른 기술과 기본 내장 통합(기타 서드파티 기술 포함)	Secure Network Analytics 및Cisco XDR
	• 안티 스팸, URL 관련 보호 및 통제, 고성능 바이러스 스캐닝, 아웃브레이크 필터, 도메인 기능 평판 스캐닝 • 임원진을 타게팅하는 BEC 공격을 예방하는 위조 이메일 탐지 • 자동 악성코드 분석 및 샌드박싱	Secure Email

핵심 요소	주요 기능	관련 시스코 제품
빠르고 정확한 위협 대응 지원(계속)	• 광범위한 고객층에 대한 전용 글로벌 SOC(보안 운영 센터)에서 얻은 위협 정보 및 인사이트로 상시 보호 이용	모든 Cisco Secure 제품
	• 모든 엔드포인트 활동에 대해 비정상 동작의 런타임 탐지 및 차단을 제공하는 지속적인 모니터링	Secure Endpoint
	• 프라이버시와 데이터 무결성을 유지하면서 암호화된 트래픽에서 위협 식별 및 분리 • 한 위치에서 '대응' 워크플로우 트리거 • 보안 제품 데이터 소스와 Talos®의 글로벌 위협 정보 및 API를 통한 서드파티 소스에서 컨텍스트 인식을 집계하는 위협 대응 • 포렌식 사고 조사 케이스북 제작	Cisco XDR
	• 잠재적 악성 링크의 실시간 분석을 통해 URL 기반 위협을 지속적으로 예방 • 실시간 Talos® 모니터링, 분석, 위협 정보를 지속적으로 활용하여 이전에 알려지지 않았던 위협 또는 갑작스러운 변경 식별	Secure Email
간소화된 사용자 경험을 위해 하나의 조사 관점 제공	• 하나의 뷰에 글로벌 인텔리전스를 수집하고 상관관계를 파악하여 위협 조사 가속화 • 맞춤형 대응 조치를 만들어 대응 시간 단축 • 여러 데이터 소스와 위협 정보를 결합하여 데이터 강화 자동화	Cisco XDR
생산성을 높이고 보안 태세를 강화할 기회 제공	• 발생률이 낮은 실행 파일의 자동 식별 및 위협 분석 • 맞춤형 IoC를 작성하여 전체 엔드포인트 구축에서 침해 후 지표 스캐닝	Secure Endpoint
	• 동작 모델링, 멀티 레이어 머신러닝, 글로벌 위협 정보 • 신규 디바이스 역할이 네트워크에 추가되면 자동으로 분류 • XDR 솔루션과 함께 조사하여 모든 위협 벡터 및 액세스 포인트에서 자동화 지원	Secure Network Analytics 및Cisco XDR
	• 동적 평판 분석을 자동으로 트리거하고 이메일 악성코드의 출처, 영향을 받은 시스템, 악성코드가 수행하는 작업 대한 가시성 제공 • 해결 인사이트를 바탕으로 인바운드 및 아웃바운드 이메일에 조치 수행	Secure Email
	• 일반적인 활용 사례에 맞게 사전 구축된 워크플로우를 사용하여 일상적인 작업 자동화 • 보안 운영 팀 간에 플레이북 공유 • 다른 보안 포트폴리오 솔루션에서 온 알림 자동 분류 및 우선순위 지정	Cisco XDR