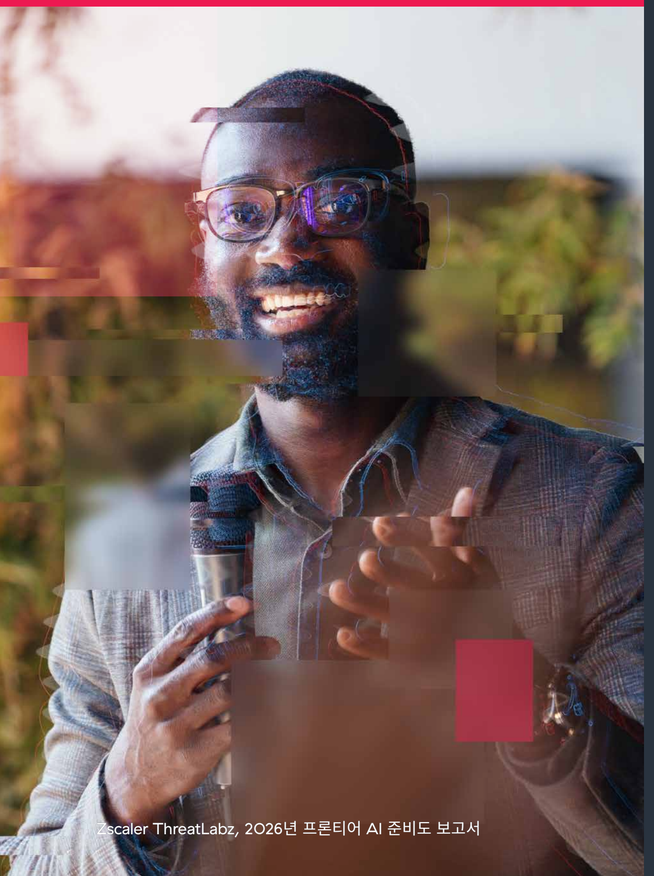
zscaler™

ThreatLabz 2026:
프론티어 AI 준비도 보고서



목차



요약 보고서 3

수치로 보는 현황 5

평가 대상 조직 6

위협 전망 7

방법론 9

주요 분석 결과 10

새로운 공격 체인:
프론티어 AI가 작은 틈들을 자율적으로
연결하여 단일 공격 시퀀스를 만드는 방법 15

사례 증거:
진행 중인 세 개의 조직 16

구현 현실성:
90일 스프린트에 실제로 필요한 조치 18

권장 사항 19

©2026 Zscaler, Inc. 모든 권리 보유.

핵심요약

작년에 우리는 유명한 AI 기업 중 한 곳으로부터 전화를 받았습니다. 우리는 이들이 자율적인 보안 테스트를 실행하도록 조정된 프론티어 AI 모델을 출시했다는 소식을 방금 접했습니다. 그 전화를 계기로 우리는 조직들이 이러한 자율 공격에 대비할 수 있는 준비도를 점검하도록 돕는 여정을 시작하게 되었습니다. 우리는 그 성능만큼이나 결과에 놀랐습니다.

주목할 점은 프론티어 AI를 기업 환경에 직접 적용하지 않고, 먼저 자체 인프라에서 테스트를 진행한 후, 그 결과를 바탕으로 현재 제공하는 평가 프로그램을 개발했다는 것입니다.

목표는 단순히 보안상의 허점을 지적하는 데 그치지 않고, 조직이 새로운 위협에 대비하면서 보안을 강화할 수 있는 부분을 구체적으로 보여주는 것입니다. 우리 모두는 함께 배우고 있으며, 이러한 결과는 단순한 경고가 아니라, 우리 모두가 회복력을 전반적으로 향상할 수 있는 방법을 공유하는 교훈이 되기를 바랍니다.

Zscaler는 대부분의 기업이 운영하는 하이브리드 및 레거시 환경과 달리 클라우드 네이티브 아키텍처를 사용하기 때문에 실제 모델에서 사용되는 것과 동일한 프론티어 테스트 방법을 활용하고, 유사하게 효과적인 모델과 TTP를 사용하여 기업 환경에서 공격자가 어떻게 작동하는지 모방했습니다. 이를 통해 우리는 우리와 같은 아키텍처가 아닌 기업 인프라의 운영 현실에 맞춰 평가 프로그램을 구축하고 조정할 수 있었습니다.

주요 시사점: AI에 대한 성공적인 대응은 단순히 AI를 더 많이 활용하는 것이 아니라, 설계 단계부터 악용될 수 있는 경로를 차단하는 아키텍처를 구축하는 것입니다.

글로벌 기업들은 프론티어 AI 기반 사이버 공격에 대비하지 못하고 있지만, 그 이유는 대부분의 사람들이 생각하는 것과는 다릅니다. 위험은 AI가 이전에는 결코 발견되지 않았던 특이한 취약점을 찾아내는 데 있는 것이 아닙니다.프론티어 모델은 모든 조직이 이미 알고 있는 명백한 취약점들을 활용하여 기계처럼 빠른 속도로 완벽한 공격 경로를 만들어낼 수 있다는 것입니다. 대부분의 아키텍처는 애초에 그런 용도로 설계되지 않았으며, 인간이든 도구든 AI를 앞지르려는 시도는 영원히 패배하는 싸움입니다. 아키텍처만이 유일한 승리 요소입니다. 다행스러운 점은 올바른 제로 트러스트 아키텍처를 구축하면 대부분의 기업이 생각보다 훨씬 더 높은 수준의 복원력을 확보할 수 있다는 것입니다.

프론티어 AI 준비도 평가 프로그램은 특정 유형의 공격자, 즉 기계처럼 빠른 속도로 작동하며 자율적으로 정찰, 취약점 연결, 그리고 측면 이동이 가능한 프론티어 AI 모델에 대한 조직의 복원력을 측정합니다. 이러한 공격자를 “프론티어 AI”라고 부르는 이유는 기존의 스캐너나 심지어 인간 분석가조차도 비슷한 속도로 재현할 수 없는 방식으로 공격 표면 전반에 걸쳐 추론할 수 있기 때문입니다. 실제 운영 환경에서 진행된 병렬 테스트에서, 프론티어 모델은 높은 신호 대 잡음비와 근거 있는 맥락을 바탕으로 한 추론 능력을 보여주었으며, 공격 연결망 발견에 있어 강력한 시너지 효과를 발휘했습니다. 이러한 능력은 이론적인 것이 아니라 이미 입증되었습니다.

©2026 Zscaler, Inc. 모든 권리 보유.

2026년 상반기에 평가된 수백 개의 기업 조직(금융 서비스, 의료, 제조, 에너지 및 8개 추가 산업 분야의 포춘 500대 기업 포함)에서 프론티어 AI 준비도 점수의 평균은 100점 만점에 37점이었습니다. 거의 모든 조직(91%)이 공개적으로 접근 가능한 AI 인프라를 보유하고 있었으나, 그 중 어느 곳(100%)도 신원 기반 접근 제어 시스템을 갖추고 있지 않았습니다. 게다가, 어떤 조직도 보안 스택이 설계대로 작동하는 데 필요한 만큼의 암호화된 트래픽을 검사하지 않았습니다. 일반 기업들은 자체 네트워크를 통해 전송되는 데이터의 64%를 사실상 파악하지 못하고 있었으며, 방어 기능을 보유하는 것과 실제로 운영하는 것 사이의 괴리를 해소한 기업은 전무했습니다.

가장 시급하게 대두되는 격차는 앞서 언급한 구조적 문제점을 더욱 악화시키고 있습니다. 평가 대상이 된 기업 모두에서 AI 거버넌스는 초기 단계에 머물러 있습니다. 코파일럿, 추론 API, MCP 엔드포인트, 섀도 AI 게이트웨이 등 AI 관련 요소들이 보안 프로그램이 흡수하고 관리할 수 있는 속도보다 훨씬 빠르게 확산되고 있습니다.

이는 프론티어 AI 위협에 대한 준비도를 강화할 수 있는 중요한 기회를 제공합니다. 분석 결과, 조직의 거의 3분의 1이 핵심 요충지에 디셉션 전략을 확대 적용함으로써 보안을 크게 향상시킬 수 있는 것으로 나타났습니다. 이와 마찬가지로, 침입 방지 기능을 전체 시행 모드로 전환하고, 애플리케이션 계층 이상 탐지를 통합하며, 세그멘테이션 정책을 개선하는 것은 SOC 경고 정확도와 전반적인 방어 태세를 향상하는 데 있어 구체적이고 영향력 있는 조치입니다.

보안 책임자들은 본 보고서를 이사회 차원의 논의를 이끌어낼 계기로 삼아야 합니다. 대상 조직 평균인 37점에서 5대 방어 축 모두가 프론티어 AI급 공격에 대응해 운영 효과성을 발휘하는 임계점인 73~98점 사이의 프론티어 AI 준비도 점수를 달성하는 것은 90일 이내에 가능합니다. 이를 위해서는 세 가지 경영 조치가 필요합니다. (1) 이사회 보고를 통해 기업의 의무 사항으로 프론티어 AI 복원력을 확립하고, (2) 내부 경영진의 합의와 전담 스프린트 역량을 확보하며, (3) 듀얼 트랙 스프린트를 실행하여 휴면 상태의 제어를 활성화하고 모든 AI 표면을 동시에 통제합니다.

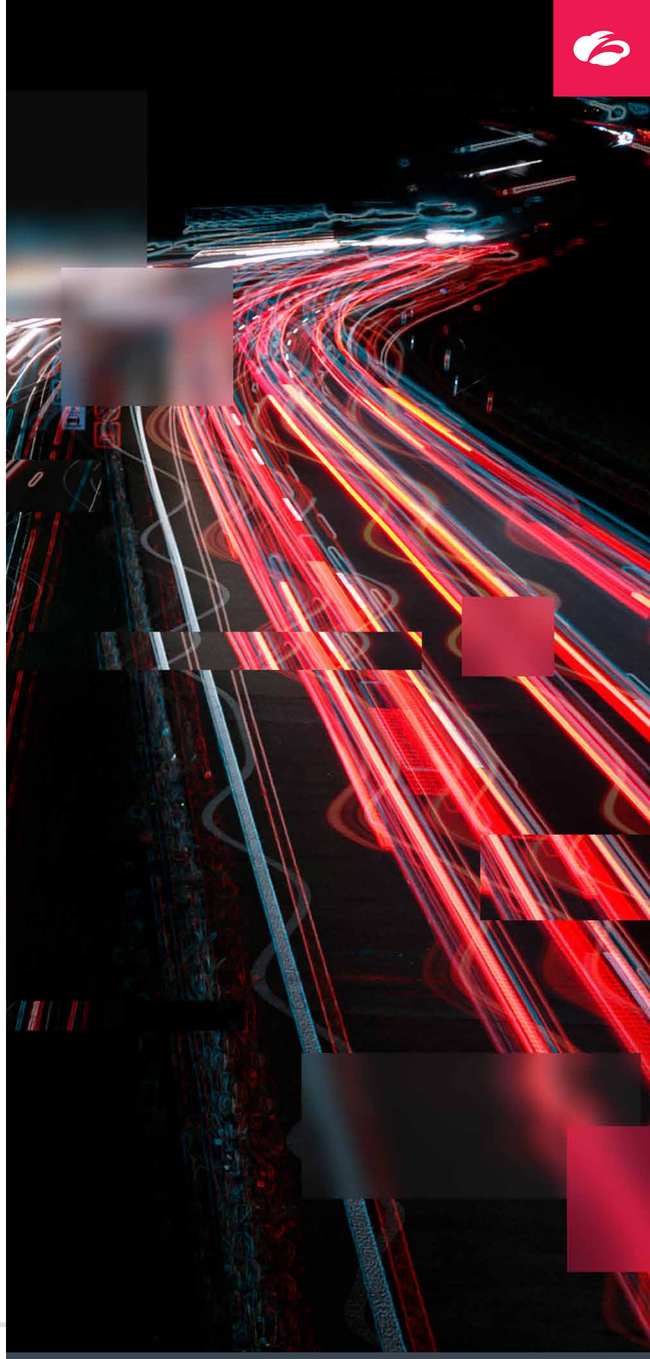
운영상의 출발점은 모든 조직에게 동일합니다. 즉, 이미 가지고 있는 것부터 시작하는 것입니다. 전략적 출발점은 거버넌스입니다. 어떤 조직도 현재 취약한 보안에 노출되는 것을 감수하지 않고서는 AI 접근 보안을 미룰 수 없습니다.



DEEPEN DESAI,
Zscaler의 사이버보안 총괄 부사장



GEORGE MOSER,
Zscaler의 글로벌 부사장 겸 CXO 인 레지던스 총괄



©2026 Zscaler, Inc. 모든 권리 보유.

수치로 보는 현황

100% AI에 대한 신원 기반 인증 기능을 갖추고 있지 않습니다.

91% 해당 인프라를 외부 공격에 완전히 노출시키고 있습니다.

100점 만점에 37점입니다. 최저점은 17점이며 최고점은 60점입니다.

SSL 검사율 **0.4%에서 68.1%까지 다양하며 평균은 약 36%입니다**. 이는 인라인 보안 제어(DLP, IPS, 샌드박싱, AI 이그레스)를 통해 적절한 보안 수준을 확보하는 데 필요한 70% 검사율에 훨씬 못 미치는 수치입니다.

최악의 피해 범위 시나리오에서 가장 높은 권한을 가진 ID가 접근할 수 있는 **애플리케이션은 483,250개**

대표적인 와일드카드 관련 사례로, 195개의 와일드카드 도메인에서만 **108,033건** 애플리케이션이 노출되었습니다. (와일드카드는 정책에서 여러 도메인이나 경로를 한 번에 나타내기 위해 사용하는 “*” 또는 앞에 붙는 “.” 같은 기호로 관리 효율성을 높이지만, 적절하게 제어되지 않으면 공격 표면을 급격히 넓힙니다.)

10개 조직 중 9개 조직 VPN 어플라이언스를 외부에 노출하고 있습니다. 각각의 어플라이언스는 사전 인증 공격 표면이 되며, 프론티어 AI 모델은 이를 기계처럼 빠른 속도로 탐지할 수 있습니다.

750개 이상의 자산 인터넷에 연결된 인프라에서 CISA가 지정한 취약점을 가지고 있으며, 이는 적극적인 탐색을 통해 확인되었고, 평가 당시 해당 취약점이 실제 환경에서 활발하게 사용되고 있었습니다.

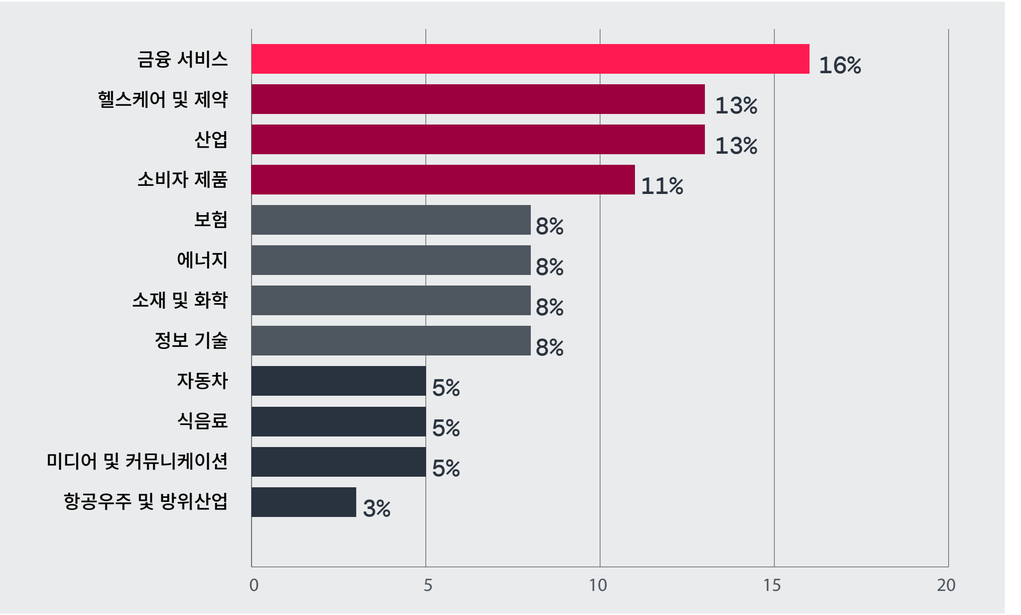


©2026 Zscaler, Inc. 모든 권리 보유.



평가
대상 조직

본 보고서의 분석 결과는 2026년 상반기 동안 수백 개의 기업을 대상으로 실시한 프론티어 AI 준비도 평가를 기반으로 합니다. 32%는 포춘 500대 기업입니다.해당 그룹은 다음과 같은 구성으로 12개 산업 분야에 걸쳐 있습니다.



평가 대상 조직은 주로 수만 개의 인터넷 검색 가능 자산을 보유한 대기업이었습니다. 인터넷에서 검색 가능한 자산에는 인증 없이 공용 인터넷에서 접근할 수 있는 모든 시스템, 애플리케이션 또는 엔드포인트가 포함됩니다.

©2026 Zscaler, Inc. 모든 권리 보유.



위협 전망

프론티어 AI 모델은 기업의 취약점을 기계처럼 빠른 속도로 식별하고 연결하는 능력을 입증했습니다.

위의 분석 결과는 현재 상황, 즉 2026년 상반기에 대상 집단 전반에서 관찰된 상황을 설명합니다. 아래의 위협 전망은 활성화 시점이 중요한 이유를 설명합니다. 이러한 상황을 악용하는 공격자의 역량은 기업의 일반적인 운영 주기보다 훨씬 빠르게 발전하고 있습니다. 아래의 각 추세는 하나 이상의 평가 결과를 직접적으로 뒷받침합니다.

Zscaler의 프론티어 모델 테스트 프로그램에서 프론티어 AI급 모델은 내부 정보가 없는 블랙박스, 소스 코드, 컴파일된 바이너리 및 정적 파일 포함한 화이트박스, 부분 또는 전체 시스템 콘텍스트 포함한 그레이박스의 세 가지 모드에서 평가되었습니다. 이러한 테스트를 통해 프론티어 AI 모델은 근거 있는 콘텍스트가 제공될 경우, 신호 대 잡음비가 높은 엔터프라이즈 환경에서도 추론 능력을 발휘하고, 인간 분석가와 기존 스캐너가 놓쳤던 다단계 공격 경로를 일관되게 식별할 수 있음이 독립적으로 확인되었습니다. 실제 운영 환경 전반에 걸쳐 근거 있는 컨텍스트는 공격 경로 탐지 능력을 크게 향상시키는 요소임이 입증되었습니다.

이번 독립적인 검증을 통해 1번부터 6번까지의 분석 결과에서 확인된 구성상의 격차가 자율적으로 작동하는 프론티어 AI 모델에 의해 활용될 수 있으며, 현재의 프론티어 모델들이 평가 대상 집단 전반에서 관찰된 바와 같이 이러한 특정 조건들을 활용할 수 있다는 것이 확인되었습니다.

AI 기반 취약점 발견은 2027년까지 새로운 익스플로잇의 등장 속도를 매우 빠르게 할 가능성이 높습니다

취약점 악용까지 걸리는 평균 시간이 마이너스로 전환되었습니다. 이제 자동 패치 시스템이 구축되어 있더라도 기업 환경 전반에 패치가 배포되기 전에 취약점이 악용되고 있습니다. 이러한 문제는 구조적인 것으로, 악용 시점이 기업의 변경 관리 시스템이 적응하는 속도보다 훨씬 빠르게 단축되고 있기 때문입니다.

평가 대상 집단 전체에서 확인된 바와 같이, KEV 및 EPSS 점수가 1.0에 가깝거나 그 수준인 인터넷 공개 자산의 경우, 정보 공개와 실제 악용 사이의 시간 간격이 몇 시간으로 단축되었습니다. 정기적인 유지보수 기간에 패치를 적용하는 조직은 복구 주기 동안 알려진 취약점을 악용하는 공격에 직면할 가능성이 매우 높습니다.

©2026 Zscaler, Inc. 모든 권리 보유.

향후 12~18개월 동안 AI 공격 표면 확장은 거버넌스 프로그램의 대응 속도를 앞지를 가능성이 높습니다

AI 거버넌스가 전 세계적으로 부재한 것은 AI 도입 속도와 보안 프로그램 적응 속도 사이에 구조적인 격차가 존재함을 반영합니다. 개발팀, SaaS 공급업체 및 사업부는 보안 검토 없이 코파일럿, 추론 엔드포인트 및 MCP 인터페이스를 배포하고 있습니다. 관찰된 확산 속도를 기준으로 볼 때, 통제되지 않은 AI의 면적은 통제가 실효성 있는 수준에 도달하기 전에 두 배로 늘어날 가능성이 높습니다. 대응을 지연하는 조직은 평가 기간 내에 악용당할 가능성이 높습니다.

신원 도용을 통한 측면 이동은 제로 트러스트 환경에 대한 주요 사후 공격 기법이 될 가능성이 매우 높습니다

무작위 분석 결과에 따르면 신원 도용이 가장 손쉬운 경로인 것으로 나타났습니다. 프론티어 AI급 공격자는 기존의 네트워크 공격보다 자격 증명 탈취를 우선시할 가능성이 매우 높습니다. 단 하나의 신원으로 수천 건의 지원서를 받을 수 있어 그에 따른 보상은 엄청납니다. 세션 만료 기한이 없고 기기 보안 태세 검증 기능이 없는 조직은 거의 확실히 첫 번째 공격 대상이 될 것입니다.

암호화된 트래픽 사각지대는 AI 기반 데이터 탈취의 주요 유출 경로가 될 가능성이 높습니다

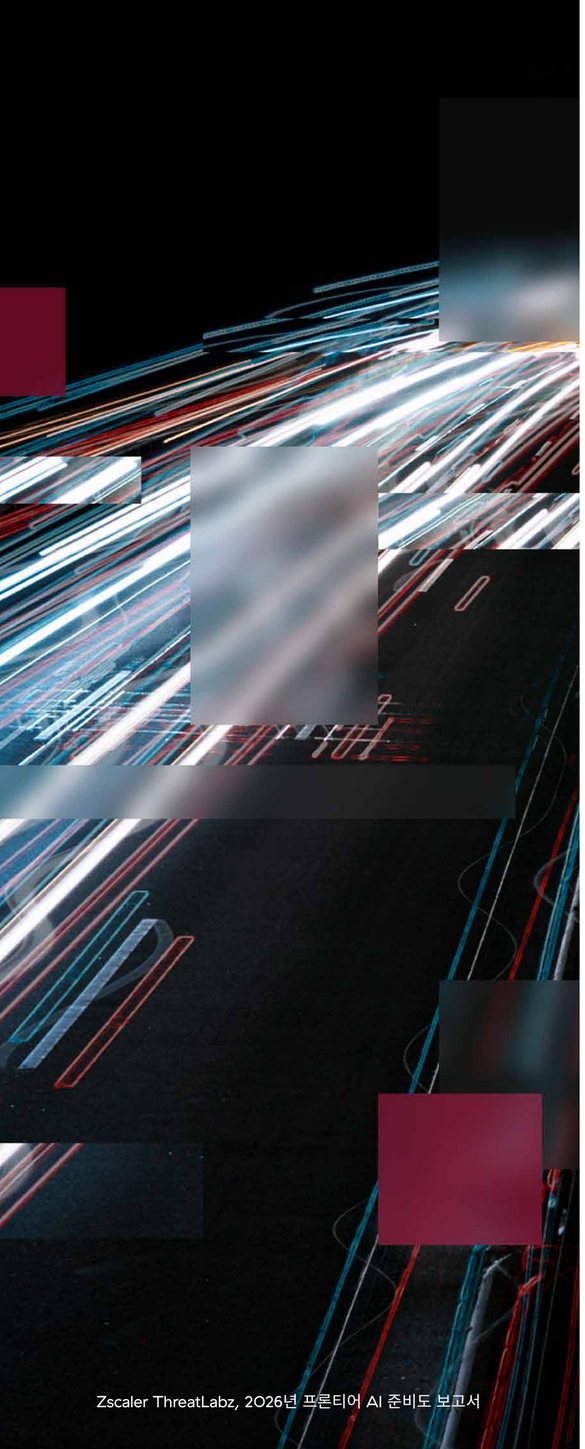
프론티어 AI는 암호화된 API 호출, 모델 상호 작용 또는 클라우드 트래픽 내에 민감한 데이터를 인코딩할 수 있습니다. 합법적으로 보이는 패턴을 생성하는 AI 도구와 이를 검사할 수 없는 보안 체계가 결합되어 고대역폭의 은밀한 데이터 유출 채널이 만들어집니다. 이는 이미 악용되고 있을 가능성이 높으며, 앞으로 더욱 심화될 것이 거의 확실합니다.

자율적인 익스플로잇 체이닝은 최초 접근부터 완전한 시스템 장악까지 걸리는 시간을 몇 분으로 단축시킬 가능성이 높습니다

노출된 VPN 어플라이언스, KEV 취약점, 와일드카드 세분화 및 비활성 탐지 기능이 결합되어 AI 공격자가 아무런 대응 없이 정찰 단계에서 광범위한 내부 접근 단계로 나아갈 수 있는 환경이 조성됩니다. 데이터에 따르면 이러한 전체 체인 현재 대다수 집단에 대해 실행 가능합니다. 엔드투엔드 방식으로 작동하는 자율 도구는 향후 12개월 이내에 고도화된 사용자들에게 제공될 가능성이 높습니다.



©2026 Zscaler, Inc. 모든 권리 보유.



방법론

프론티어 AI 위협 검증

우리는 통제된 환경과 실제 기업 맥락에서 OpenAI GPT-5.5 및 Anthropic Claude Opus 4.8을 활용했습니다. 우리가 "프론티어 AI급"이라는 용어를 사용하는 이유는 특정 모델보다는 자율적인 다단계 추론, 도구 사용, 맥락에 기반한 검색, 그리고 자기 주도적 활용 순서 결정과 같은 역량 임계값이 더 중요하기 때문입니다. 현재 또는 미래의 모델을 불문하고 해당 임계값 이상인 모든 모델은 이 평가에서 측정하는 적대자 유형을 나타냅니다.

이와 동시에 Zscaler는 블랙박스(내부 정보 없음), 화이트박스(소스 코드, 컴파일된 바이너리, 정적 파일), 그레이박스(부분 또는 전체 시스템 콘텍스트)의 세 가지 모드를 사용하여 내부 테스트 프론티어 모델 테스트를 수행했습니다. 이러한 테스트를 통해 프론티어 AI 모델이 실제 맥락에 기반하여 작동할 때 기업 환경에서 높은 신호 대 잡음비 추론 성능을 달성한다는 것이 확인되었습니다.

점수 산정 체계

각 조직은 프론티어 AI 위협 모델을 사용하여 5가지 방어 요소에 걸쳐 가중치가 부여된 100점 만점의 종합 점수를 받았습니다. 주요 요소는 공격 회피(25점, 25%), 피해 반경 제한(25점, 25%), AI 활용 관리 (20점 20%), 데이터 보호 (20점 20%), 그리고 디셉션 및 디코이(10점, 10%)입니다. 점수 산정 시 제어 권한 소유 여부와 운영 활성화 상태 모두를 평가했습니다.

데이터 소스

평가는 외부 공격 표면 관리(EASM), AI 기반 취약점 우선순위 지정, AI별 표면 탐색, 개인 액세스 구성 검토, 그리고 가능한 경우 검사 범위, 정책 시행 및 인증 상태를 다루는 인라인 원격 측정 데이터 등 여러 범주의 입력 자료를 활용했습니다.

평가 모델

Opus 엔진은 포괄적인 EASM 가시성을 기반으로 분석 결과를 검증하고 우선순위를 지정하여 조치가 필요한 악용 가능한 문제를 파악하고, 후보 집합을 평균 84%, 가장 복잡한 경우에는 92%까지 개선했습니다. 또한 복구 ROI별로 CVE 점수를 재조정하고, 분석 결과를 CISA KEV와 상호 참조하며, 검증된 공격 표면 전반에 걸쳐 다단계 악용 경로를 식별했습니다.

본 평가의 범위(및 제외 사항)

본 평가는 외부 공격 표면 노출 정도와 보안 제어 구성 상태를 평가합니다.
본 평가는 SIEM 규칙 수준에서의 SOC 탐지 효율성, 사고 대응 준비 상태, ID 공급자 보안 상태 또는 엔드포인트 탐지 범위를 평가하지 않습니다. 해당 점수는 AI 기반 공격자가 실효성 있는 통에 부딪히지 않고 침투, 이동 및 유출할 가능성을 반영합니다. 이는 전체적인 보안 태세 점수를 나타내는 것은 아닙니다.

결정적으로, 프론티어 AI급 공격은 정찰에서 데이터 유출까지의 킬 체인을 단 몇 분으로 단축할 수 있어, 고도화된 SOC조차 대응할 수 없는 시간이며, 인간의 개입 전에 구성상의 허점을 악용할 수 있을 만큼 빠릅니다.

©2026 Zscaler, Inc. 모든 권리 보유.

주요 결과

분석 결과 1

기업은 몇 가지 간단한 단계를 통해 기존의 AI 방어 기능을 극대화할 수 있습니다

조직은 실용적인 사이버 위생 수칙을 통해 보안을 크게 강화할 수 있습니다.

활성화 기회는 광범위합니다. 조직의 64%는 고품질 탐지 기능을 강화하기 위해 라이선스를 취득한 디셉션 플랫폼을 도입할 준비를 마쳤습니다. 조직의 15%는 침입 방지 시스템을 모니터링 모드에서 완전 시행 모드로 전환할 준비가 되어 있습니다. 18%는 추가 사이트로 확장 가능한 인증 기능을 갖추고 있습니다.조직은 구성 최적화만으로도 100점 만점에 73점에서 98점 사이의 목표 점수를 달성할 수 있습니다. 대상 조직의 평균 초기 점수인 37점을 기준으로 볼 때, 이는 개별 항목의 점수가 대폭 향상된 것을 의미합니다.

이것이 AI급 위협에 중요한 이유는 완전한 보안 조치가 적용되지 않은 상태에서 작동하는 보안 도구는 기계처럼 빠른 속도로 공격하는 공격에 대한 저항력을 약화시킵니다.

분석 결과 2

AI 거버넌스는 조직 규모나 관리 범위와 관계없이 평가 대상 기업 모두에서 초기 단계에 머물러 있습니다

본 분석 결과는 보편적으로 나타납니다. 평가 대상 조직의 100%가 AI에 대한 신원 기반 인증이 부족하고, 91%는 AI 엔드포인트를 공개적으로 노출하고 있습니다. AI 거버넌스 핵심 요소별 평균 점수는 20점 만점에 2.1점(최대치의 10.5%)이었습니다. 해당 집단에서 가장 높은 점수는 20점 만점에 3점이었습니다.

노출 정도는 상당합니다. 인터넷에 노출된 MCP 엔드포인트와 인증되지 않은 챗봇 또는 코파일럿을 포함하여 공개 AI 엔드포인트가 전체 대상 조직에서 흔하게 발견되었습니다. 관찰된 가장 심각한 사례에는 공용 인터넷에 노출된 심각한 수준의 GenAI 게이트웨이가 포함되었습니다.

이러한 격차는 개발팀, 사업부 및 제3자 공급업체가 AI 인터페이스를 배포하는 속도가 보안 프로그램의 적응 속도를 앞지르기 때문에 발생합니다. AI 거버넌스는 미래의 과제가 아닙니다. 이는 모든 평가 대상 조직에서 현재 악용 가능한 취약점이며, 관리되지 않는 공격 표면 중 가장 빠르게 증가하는 범주입니다.

©2026 Zscaler, Inc. 모든 권리 보유.

분석 결과 3

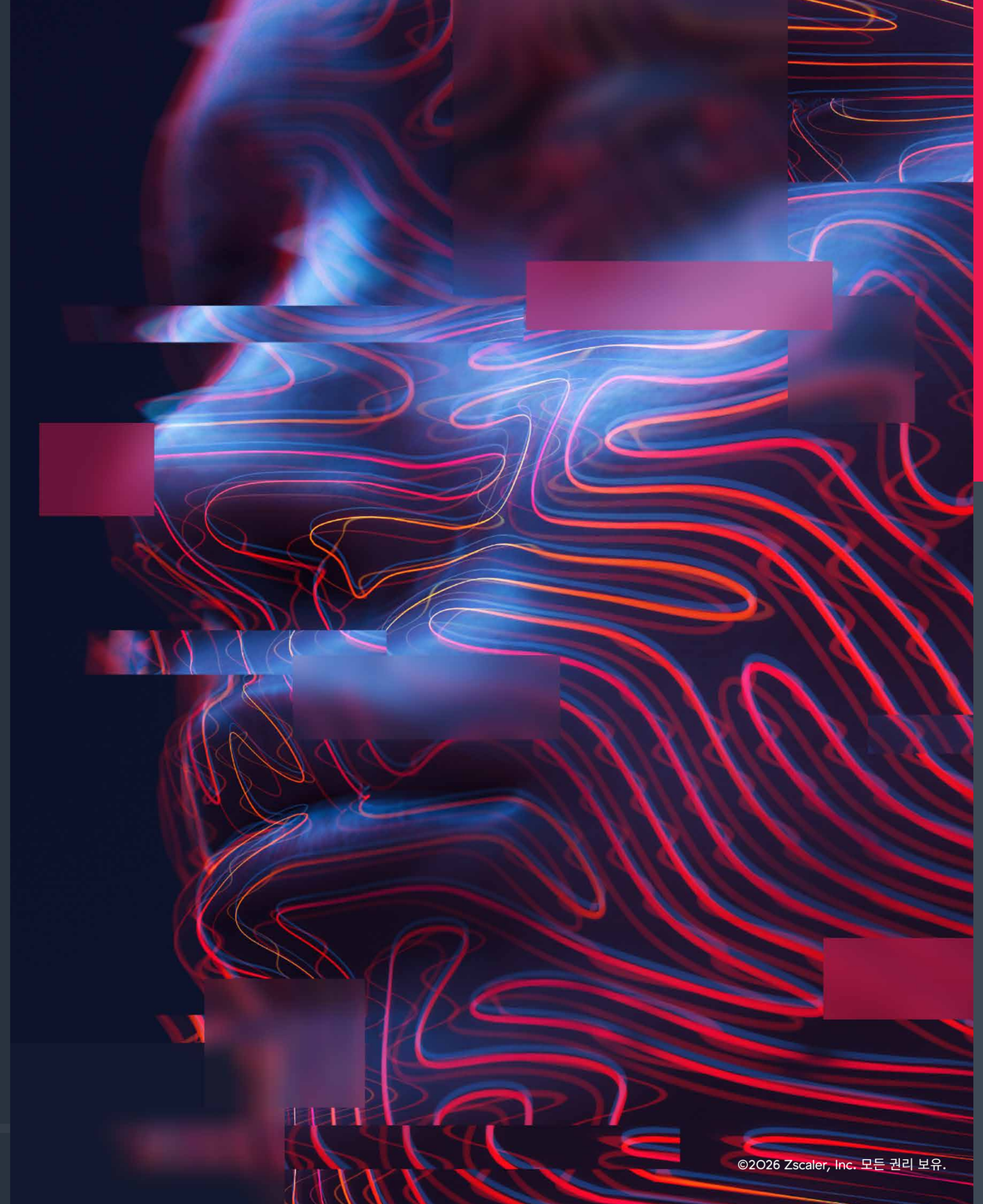
암호화된 트래픽에 대한 제한적인 검사는 대부분의 트래픽에 걸쳐 배포된 보안 제어의 효과를 저하시킵니다

암호화된 트래픽 검사는 오랫동안 보안 운영의 우선순위였습니다. AI 기반 위협이 존재하는 상황에서는 완벽한 검사 범위 확보가 매우 중요합니다.프론티어 AI 모델이 데이터를 유출할 경우, 암호화된 채널, 특히 AI API 호출, 클라우드 스토리지 업로드, 그리고 합법적인 트래픽 패턴과 섞이는 모델 간 통신을 사용할 가능성이 매우 높습니다.검사되지 않은 트래픽 내에서 활동하는 적은 인라인 제어 시스템에 감지되지 않습니다.이로써 암호화된 트래픽 검사는 운영상의 모범 사례에서 AI급 위협에 대한 기본적인 요구 사항으로 격상됩니다.

일반적으로 기업은 암호화된 트래픽의 약 36%를 검사합니다. 어떤 조직도 활성 인라인 보안 통제(DLP, IPS, 샌드박싱, AI 이그레스)를 거치는 암호화 트래픽 비율이 최적의 보안 범위를 달성하기에 충분한 수준으로 정의된 본 평가의 70% 적격 검사 기준을 충족하지 못했습니다.최악의 경우, 암호화된 트래픽의 99.6%가 보안 인프라를 전혀 검사받지 않고 거칩니다.

암호화된 트래픽에 대한 검사가 이루어지지 않으면 DLP, IPS, 샌드박싱, AI 기반 트래픽 관리와 같은 인라인 보안 제어가 무력화되어 조직은 데이터 유출 및 멀웨어 유포와 같은 심각한 위협을 감지하지 못하게 됩니다. 사이버 위협의 86% 이상과 모든 AI 모델 상호 작용이 암호화된 채널을 사용한다는 점을 고려할 때, 포괄적인 트래픽 검사는 AI급 공격에 대한 방어에 필수적인 전제 조건입니다.

근본 원인은 기술적인 문제가 아니라 운영상의 문제입니다. 대다수의 조직은 선택적 검사 모델(기본값은 “검사 안 함”)을 사용합니다. 해당 조직 전반에서, 조직들은 특정 트래픽 범주에 대한 검사를 비활성화하는 ‘다른 정책 우회’ 또는 ‘검사 안 함’ SSL 규칙에 자주 의존합니다. 영향을 받은 조직들 사이에서 이러한 우회 규칙의 수는 2개에서 51개까지 다양했습니다.



©2026 Zscaler, Inc. 모든 권리 보유.

분석 결과 4

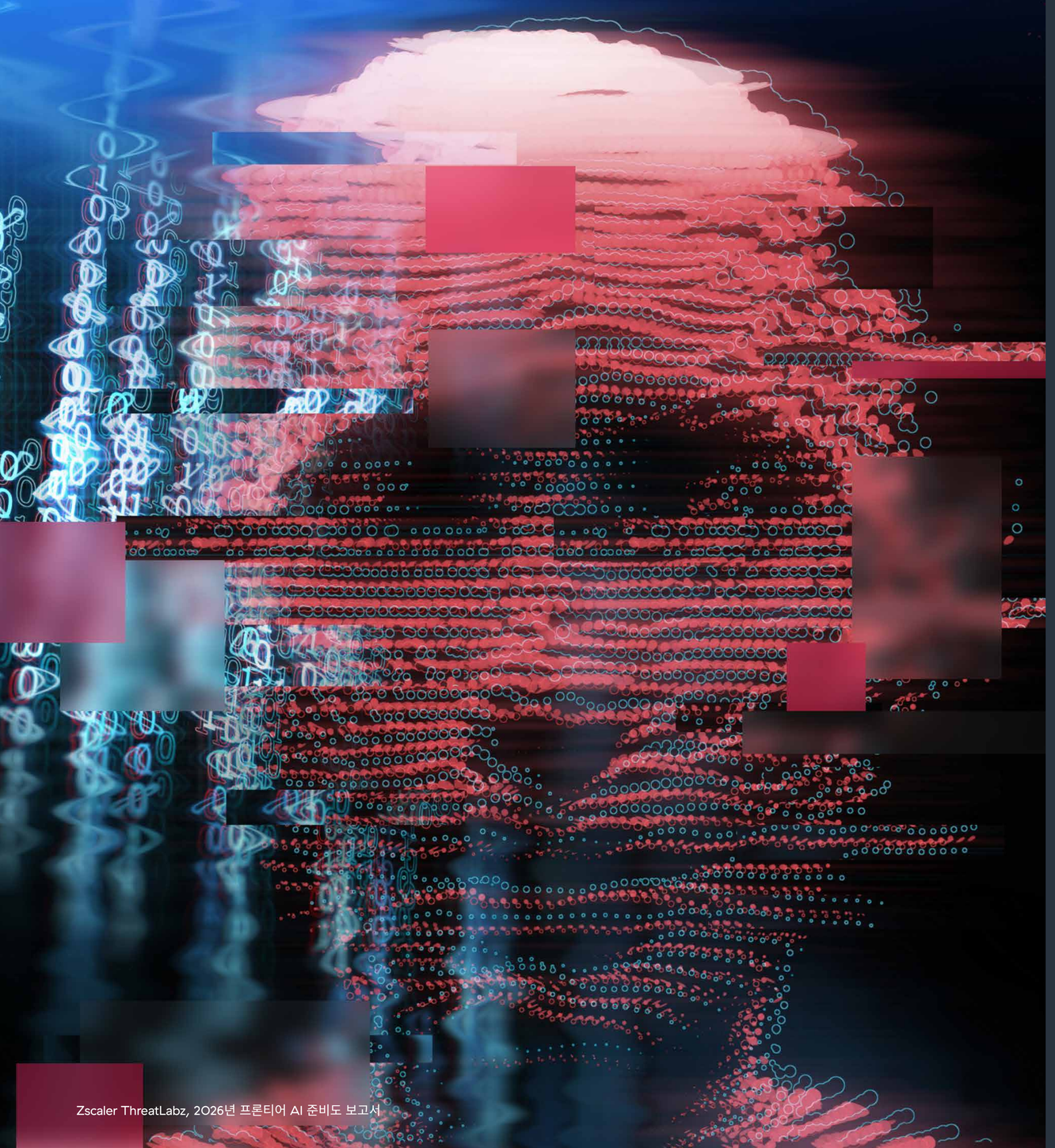
평가 대상 환경은 아직 필요한 속도로 AI 기반 공격을 탐지하거나 방지하도록 구성되어 있지 않습니다

네 번째 분석 결과는 디셉션, IPS, 이상 탐지 및 세션 모니터링을 포함한 보안 제어 구성이 AI급 공격에 최적화되어 있지 않아 조직이 차단할 수는 있지만 식별할 수 없는 위협에 노출되는 심각한 탐지 격차를 보여줍니다. 결과적으로 프론티어 AI급 공격은 SOC에 감지되지 않으며, 디셉션, IPS, 행동 이상 또는 세션 시간 초과에 대한 트리거가 없으므로 침해의 첫 징후는 내부 탐지보다는 외부 알림일 가능성이 높습니다.

- **디셉션(조기 경보 시스템):** 조직의 64%는 핵심 영역까지 확장되지 않은 디셉션 플랫폼을 보유하고 있습니다. 현재 구성으로는 측면 이동 공격자가 탐지 장치에 걸리지 않을 것입니다. 디셉션은 고정밀 디코이를 사용하여 측면 이동을 즉각적이고 자동화된 방식으로 차단함으로써 AI 기반 공격에 대해 효과적이고 시그니처에 독립적인 탐지 기능을 제공합니다.
- **침입 방지(인라인 차단):** 조직의 15%는 침입 방지 시스템을 완전 시행 모드로 전환하여 방어력을 강화할 수 있는 분명한 기회가 있습니다. "다른 정책 우회" 규칙이 활성화된 경우 대부분의 트래픽은 평가되지 않았습니다. 암호화된 채널을 통해 전송되는 알려진 익스플로잇은 검사되지 않고 차단되지 않은 채 통과했습니다.
- **애플리케이션 계층 이상 탐지(행동 신호):** 여러 조직에서 아직 인라인 규칙을 구성하지 않았습니다. 와일드카드 탐색량에 대한 이상 탐지가 이루어지지 않았습니다. 단일 사용자가 수천 개의 애플리케이션에 순차적으로 액세스하는 경우 경고가 발생하지 않을 가능성이 매우 높습니다.
- **세션 및 ID 모니터링(침해 차단 트리거):** 여러 조직에서 만료 시간 없이 구성된 인증 시간 초과로 인해 손상된 세션이 무기한으로 유효한 상태로 유지될 수 있습니다. 한 조직에서는 18개의 액세스 규칙 중 어느 것에도 장치 상태 확인이 포함되어 있지 않았습니다. 탈취당한 자격 증명은 재인증을 트리거하지 않고 몇 주 동안 작동할 수 있었습니다.
- **프론티어 AI급 공격이 SOC에 미치는 영향은 매우 클 것으로 예상됩니다.** SOC는 아무것도 감지하지 못합니다. 디셉션 트리거도 없고, IPS 경고도 없으며, 행동 이상 징후도 없고, 세션 시간 초과도 발생하지 않습니다. 침해 사실을 처음 알게 되는 시점은 내부 탐지보다는 외부 알림일 가능성이 매우 높습니다.



©2026 Zscaler, Inc. 모든 권리 보유.



분석 결과 5

광범위한 분할로 인해 프라이빗 접근 플랫폼이 측면 이동 고속도로로 변질되었습니다

분석 결과, ZTNA를 사용하는 조직의 64%가 의도한 것보다 더 많은 애플리케이션을 노출할 수 있는 와일드카드를 과도하게 사용하는 구성을 가지고 있는 것으로 나타났습니다. 한 사례에서는 단 195개의 와일드카드 도메인만으로 10만 8천 개 이상의 애플리케이션에 접근할 수 있게 되어, 단일 사용자가 해당 환경의 매우 광범위한 영역에 접근할 수 있는 가능성을 초래했습니다. 이러한 구성은 온보딩을 간소화하기 위해 배포 또는 마이그레이션 중에 도입되는 경우가 많지만, 환경이 확장됨에 따라 유지되어 원래 의도했던 범위를 넘어 접근 권한이 확장될 수 있습니다. 정기적인 검토와 개선이 없다면, 와일드카드 기반 정책은 최소 권한 원칙을 훼손하고 피싱이나 세션 탈취와 같은 방식으로 신원 도용의 영향을 확대할 수 있습니다.

여러 조직에서 인증 시간 제한을 “없음”으로 설정하여 이 문제를 더욱 악화시키고 있습니다. 침해된 세션은 무기한으로 유효한 상태로 유지됩니다. Limit Blast Radius에서 가장 높은 점수(25점 만점에 14.4점)를 받은 조직조차도 여전히 와일드카드 구성을 유지했습니다. 점수가 낮은 조직들은 사실상 세분화가 되어 있지 않았습니다.

이러한 패턴은 프라이빗 액세스 환경이 제로 트러스트 아키텍처가 시행하도록 설계된 최소 권한 분할을 아직 반영하지 못하고 있음을 의미합니다. 대규모 신원 도용이 가능한 프론티어 AI급 공격자에 맞서, 와일드카드 중심의 구성은 평가된 환경에서 가장 효과적인 측면 이동 경로를 나타냅니다.

©2026 Zscaler, Inc. 모든 권리 보유.

분석 결과 6

기업의 3분의 1 이상이 인터넷에 연결된 인프라에 알려진 취약점을 그대로 보유하고 있습니다

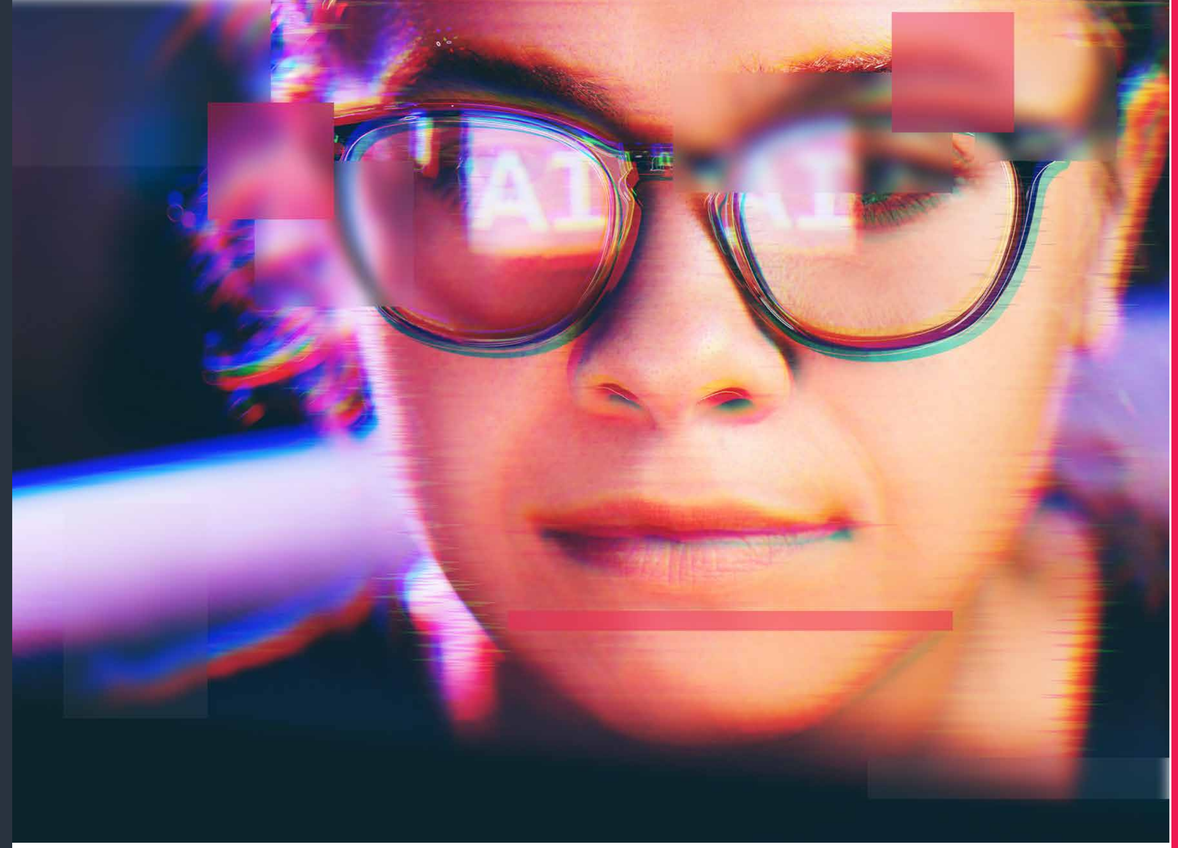
이러한 취약점이 지속되는 이유는 알려지지 않았기 때문이 아니라, 개선 작업이 유지보수 기간, 변경 관리 요구 사항 및 인프라 종속성과 같은 운영상의 현실과 경쟁해야 하기 때문입니다. 대상 조직 중 절반 이상(53%)이 인터넷에 노출된 자산에 대한 CISA 알려진 취약점(KEV)에 대해 개선 권고를 받았습니다. 능동적 탐색 결과, 기업의 3분의 1 이상에서 외부 경계 시스템에 실제로 악용 가능한 KEV가 존재하는 것으로 나타났습니다.

그 결과, 방어자가 취약점을 신속하게 해결할 수 있는 속도와 공격자가 취약점을 파악하고 악용할 수 있는 속도 사이의 격차가 점점 커지고 있습니다. 공격자들이 AI를 활용하여 취약점을 발견하고 악용 속도를 높임에 따라, 취약점 노출 가능 기간은 더욱 단축될 가능성이 높습니다.

대상 조직 대다수에서 3건의 CVE가 발생했습니다. 모두 CISA의 알려진 악용 취약점 목록에 있습니다.모두 능동적 탐색을 통해 확인되었습니다.

- **CVE-2024-38475(Apache mod_rewrite):** EPSS 점수 0.9988~0.9997
- **CVE-2021-40438(Apache mod_proxy SSRF):** EPSS 점수 0.9999~1.0000
- **CVE-2023-44487(HTTP/2 Rapid Reset):** EPSS 점수 0.999

고도화된 체계를 갖춘 조직에서조차 이러한 문제가 지속되는 것은 운영상의 현실을 반영합니다. 웹 계층 인프라, 특히 Apache와 F5/NGINX, 이는 종종 표준 패치 자동화 범위를 벗어나며 변경 기간 전반에 걸쳐 수동 조정이 필요합니다.



현재 노출된 취약점은 알려진 취약점을 반영하지만, 조직 경계 내에 알려진 KEV를 보유하고 있는 경우, 기존에 이루어진 보안 조치가 완료되기 전에 동일 시스템에서 아직 공개되지 않은 취약점이 악용될 위험에 직면할 수 있습니다.

다섯 번째 분석 결과는 이러한 위험을 더욱 증폭시킵니다. 패치가 적용되지 않은 인터넷 연결 자산은 각각 사전 인증 진입점을 나타내며, 단일 ID로 수십만 개의 애플리케이션에 접근할 수 있는 환경에서는 악용된 CVE 하나로 인해 영향을 받는 서버를 훨씬 넘어 접근 권한이 확장될 수 있습니다.

우선 순위 조치는 외부 공격 표면 관리를 통해 자산 가시성을 지속적으로 유지하고, 중개된 액세스를 통해 발견 가능한 공격 표면을 줄이고, 악용 가능성 기반 우선순위 지정을 통해 비즈니스상 정당한 노출 자산에 대한 탐지-분류-패치 주기를 단축하고, 복구 기간 동안 자율적인 가상 패치를 사용하는 것입니다.

©2026 Zscaler, Inc. 모든 권리 보유.

새로운 공격 체인:_

프론티어 AI는 어떻게 작은 틈들을 자율적으로 연결하여 하나의 공격 시퀀스를 만들어내는가?

이러한 결과는 단지 몇몇 사례에 불과한 것이 아닙니다. 그들은 더 광범위한 공격 체인의 연결 고리를 강화하고 있습니다.개별적으로는 각각 해결 가능한 격차이지만, 이러한 격차들이 모두 합쳐지면 개별적인 분석 결과에서 나타나는 것보다 훨씬 더 큰 문제점이 드러납니다.

맥락에 기반한 프론티어 AI 모델은 패치가 적용되지 않은 CVE, 아직 시행되지 않은 IPS, 와일드카드 구성, 관리되지 않는 AI 엔드포인트, 검사되지 않은 이그레스 경로와 같은 조건을 자율적으로 식별하고 순서대로 배열하여 인간의 개입 없이 기계 속도로 연속적인 익스플로잇 경로로 만들 수 있습니다. 기존 스캐너와 침투 테스트는 이러한 복합 경로를 비슷한 속도로 드러내지 못합니다.다음 순서는 평가된 환경 전반에 걸쳐 검증되었습니다.

1 단계: 인터넷 스캔을 통해 노출된 VPN 어플라이언스(500대 이상 중 1대)를 식별합니다. 웹 계층에서 CVE-2024-38475(Apache) mod_rewrite, EPSS 0.9997을 식별합니다.

2 단계: 사전 인증 취약점을 악용합니다. 자격 증명 없이 초기 접근 권한을 획득합니다. IPS가 비활성화되어 있습니다. 경고가 생성되지 않습니다.

3 단계: 침해당한 VPN 인프라에서 자격 증명을 수집합니다. 유효한 단일 기업 ID를 확보합니다.

4 단계: 프라이빗 액세스 플랫폼에 인증합니다. 와일드카드 구성을 통해 17,000개 이상의 애플리케이션에 액세스할 수 있습니다. 타임아웃은 "없음"으로 설정되어 있습니다. 장치 상태 확인은 수행하지 않습니다.

5 단계: 컴퓨터 속도로 애플리케이션을 탐색합니다. 경로에 디셉션용 디코이가 없습니다. SOC는 경고를 감지하지 못합니다.

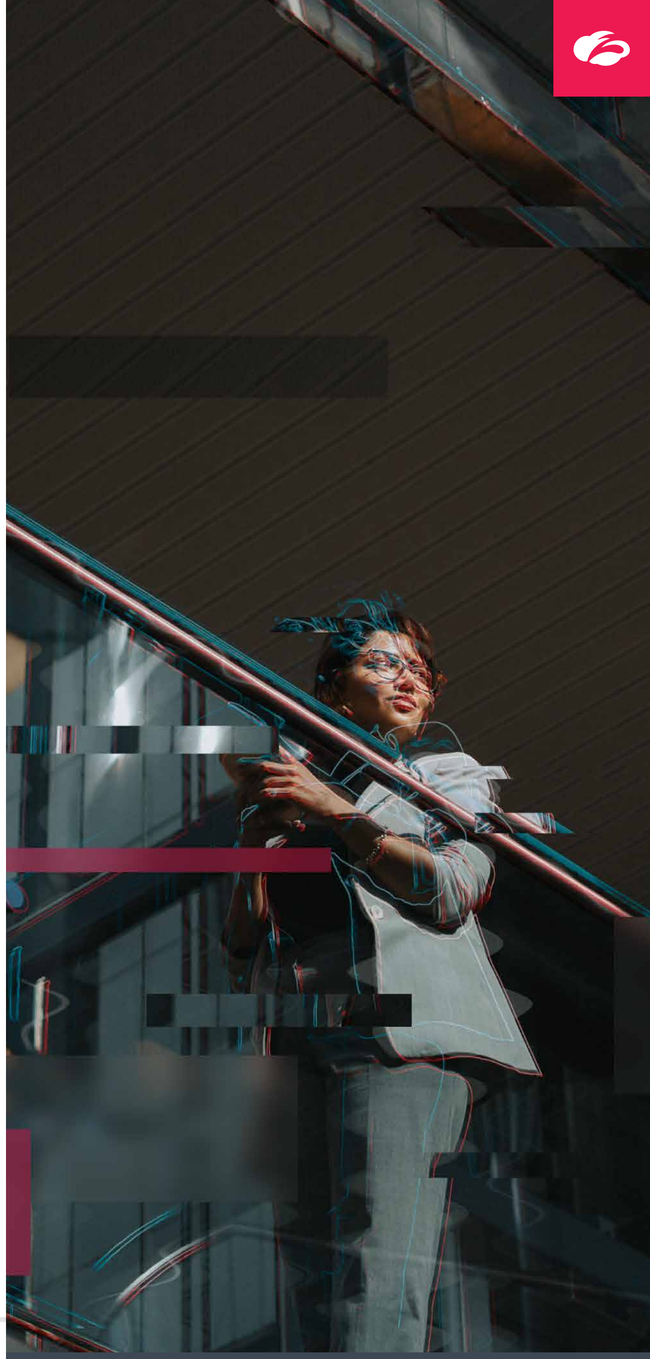
6 단계: 추가 인증 없이 접근할 수 있는, 거버넌스가 적용되지 않은 AI 추론 엔드포인트(300개 이상 중 1개)에 도달합니다. 모델의 텍스트 창을 통해 독점 데이터를 조회할 수 있습니다.

7 단계: 암호화된 채널을 통해 데이터가 유출됩니다. 트래픽의 3분의 2는 검사되지 않습니다. DLP는 유출 트래픽을 감지할 수 없습니다. 경고가 생성되지 않습니다.

초기 스캔부터 데이터 유출까지의 총 소요 시간:
내부 공격자 테스트 결과, 기업 AI 시스템은 첫 번째 치명적인 오류가 발생하기까지 평균 16분밖에 걸리지 않았습니다.

Zscaler의 프론티어 모델 테스트 프로그램
(프런티어 AI급 모델 및 GPT 5.5, 세 가지 모드 전반: 내부 정보 없음, 소스 코드 접근, 일부/전체 시스템 컨텍스트), 이러한 연쇄 추론 능력이 검증되었습니다. 그라운디드 컨텍스트 하니스를 사용하면 프런티어 모델이 기존 스캐너나 인간 분석가는 같은 속도로 찾아내지 못하는 다단계 익스플로잇 경로를 식별할 수 있습니다.

모든 구성 요소는 2026년 상반기 동안 조직 환경에서 관찰되었습니다. 이 체인은 프론티어 AI 준비도 점수의 보정 기준으로 사용되는 적대 모델을 나타냅니다.



©2026 Zscaler, Inc. 모든 권리 보유.

사례 증거:_
진행 중인 세 개의 조직

다음은 조직들이 문제 해결 여정의 다양한 단계에 있음을 보여주는 익명화된 사례 연구입니다. 이는 초기 상태 조건과 평가 과정에서 확인된 격차를 해소하기 위해 사용된 운영 방법론을 보여줍니다.

사례 1

글로벌 금융 서비스 조직

초기 상태: 인터넷에 노출된 자산 10,000개 이상. 검증된 CVE 4,000개 이상(고유 CVE 900개 이상, 심각도 165개). 해당 대상 조직에서 가장 흔한 CVE 3개(CVE-2024-38475, CVE-2021-40438, CVE-2023-44487)가 노출된 인프라에서 확인되었습니다.

평가 분석 결과: 해당 조직의 광범위한 인터넷 연결 자산에는 여러 세대에 걸친 인프라 업그레이드 과정에서 누적된 심각한 취약점이 패치되지 않은 채 남아 있었습니다. SSL 검사는 대부분의 트래픽을 포괄하도록 확장되지 않았습니다. 디셉션 기능은 승인되었지만 아직 배포되지 않았습니다. AI 관련 기능은 관리 범위 밖에 있었습니다.

조치 착수: 165개의 심각한 CVE에 대한 우선 패치 적용. SSL 검사 기능을 선택 사항에서 선택 해제 방식으로 전환. 핵심 금융 부문에 대한 디셉션 조치 활성화. AI 표면 게이팅 시작.



©2026 Zscaler, Inc. 모든 권리 보유.



사례 2

글로벌 식품 생산업체

초기 상태: 노출된 VPN 어플라이언스 13개. 거버넌스 경계 외부에 있는 공개 AI 표면 40개(그룹 내 규모 대비 AI 노출 밀도가 가장 높음). 노출된 인프라에서 검증된 CVE 2개.

평가 분석 결과: 조직의 급속한 디지털 전환 속도가 보안 프로그램의 새로운 보안 취약점 통합 속도를 앞질렀습니다. AI 엔드포인트는 사업 부서에서 운영 계획의 일환으로 구축되었지만 아직 보안 아키텍처를 거치지 않았습니다. 프라이빗 액세스 환경에 대한 세분화 정책이 수립되지 않았습니다. VPN 인프라는 마이그레이션이 완료될 때까지 인터넷에 직접 노출된 상태였습니다.

조치 착수: 개인 액세스 뒤에 VPN 보호(즉시). 40개 엔드포인트에 대한 AI 표면 게이팅. 세분화 정책 신규 생성. 운영 세그먼트에 디셉션 배포.

사례 3

글로벌 명품 대기업

초기 상태: 범위 내 공개 이름 487개. 월간 검사되지 않은 암호화 트래픽 922TB. 정의된 애플리케이션 10,000개.

평가 분석 결과: 해당 조직의 검사 아키텍처는 보수적인 선택적 동의 모델로 구축되어 대부분의 암호화된 트래픽이 검사되지 않은 상태였습니다. 10,000개의 애플리케이션과 거의 전무한 세분화로 인해 환경은 그에 상응하는 접근 제어 없이 확장되었습니다.

조치 착수: SSL 검사 전환을 최우선 순위로 설정. 10,000개 애플리케이션에 걸쳐 와일드카드 교체. 디셉션 활성화. AI 거버넌스 기준선 구축.

©2026 Zscaler, Inc. 모든 권리 보유.

구현 현실성:_
90일 스프린트에 실제로 필요한 조치

대부분의 경우 제어 권한이 이미 확보되어 있고 의존 관계도 잘 파악되어 있기 때문에, 기술적으로 90일 이내에 복원력을 확보하는 것이 가능합니다. 하지만 이는 쉬운 일이 아니므로 최고 경영진의 지시가 필요합니다.프론티어 AI 준비도 격차를 해소하는 것은 이사회 차원의 관심, CISO와 CEO 간의 협력, 그리고 전담 실행 역량을 필요로 하는 기업 차원의 이니셔티브입니다.이는 진화하는 위협 환경 속에서 공동의 협력을 도모할 수 있는 기회입니다.
보안 책임자가 취해야 할 조치:

1. SEC, DORA 및 NIS2 규제 맥락에서 현재 준비도를 이사회에 간략히 설명합니다.

2. 90일 스프린에 대한 경영진의 원을 확보하고, 담당자를 지정하며, 최고 경영진에게 정기적으로 보고합니다.

3. 구현을 위해 소규모의 전담 팀을 배정하되, 검사 범위 확장, 와일드카드 교체 중 접근 권한 조정 등으로 인해 발생하는 마찰은 활성화 과정에서 예상되는 부분임을 인지해야 합니다.

SSL 검사는 부서 간 협업이 필수적입니다.
조직은 IT 및 보안팀과 협력하여 현재 검사 범위를 완벽하게 파악하고, 검사가 필요한 트래픽 스트림을 식별하며, 검사가 운영상 불가능한 경우(예: 인증서 고정 애플리케이션 또는 레거시 통합)를 결정해야 합니다. 검사를 적용할 수 없는 경우, 브라우저 격리, 엔드포인트 DLP, CASB 기반 API 검사, DNS 계층 필터링과 같은 완화 제어를 통해 인라인 복호화 없이도 가시성을 확보하고 위협을 방지할 수 있습니다.

와일드카드 교체에는 애플리케이션 소유자와의 협의가 필요합니다. 200개 이상의 와일드카드를 명명된 FQDN으로 교체하는 작업은 보안 팀 단독으로 수행할 수 있는 것이 아닙니다. 각 와일드카드는 비즈니스 부서, 개발 팀 및 공급업체가 소유한 애플리케이션으로 연결되므로 접근 권한의 연속성을 검증해야 합니다. 보안 팀은 목표 아키텍처를 정의하지만, 실행에는 여러 부서 간의 협업이 필수적입니다.

이 일정은 전담 실행 역량을 전제로 합니다.
스프린트팀(엔지니어 2~4명)을 지정한 조직은 일정대로 진행되었습니다. 기존 워크로드 내에서 개선 작업을 진행한 조직은 추진력을 유지하기 위해 추가적인 지원을 받았습니다. 이들의 성공은 최고 경영진의 후원, 즉 최고위급 임원과의 정기적인 소통, 전담 팀 구성 및 확보된 역량, 그리고 목표 점수 대비 주간 마일스톤 보고에 달려 있었습니다.

중요한 보안 업데이트로 인해 일시적인 운영 변경이 발생할 수 있지만, 이러한 조치는 보다 탄력적인 장기적인 방어 체계를 구축하는 데 필수적입니다. 평가에 따르면 초기 점수 37점과 같은 격차를 선제적으로 해결하는 것이 현대 디지털 위협 관리에서 매우 중요한 단계임을 강조합니다. 이러한 단기적인 조정과 강력한 보호의 필요성 사이의 균형을 맞추는 것은 조직의 전반적인 보안 태세를 강화하는 데 핵심적인 부분입니다.



©2026 Zscaler, Inc. 모든 권리 보유.

권장 사항

1 보안 통제의 시행 모드를 활성화합니다

평가 대상 조직 모두 구성 변경을 통해 완벽하게 적용할 수 있는 영향력이 큰 보안 통제(IPS, 인증, 악성 IP 차단, 도메인 프론팅 보호)를 갖추고 있었습니다. 보안 운영팀은 보유하고 있는 모든 기능의 활성화 상태를 감사하고, 필요에 따라 공급업체의 구성 감사 및 활성화 지원을 활용하여 14일 스프린트 내에 해당 기능을 시행 모드로 활성화해야 합니다.

모든 SOC 팀이 우려하는 점을 잘 알고 있습니다. IPS를 모니터링에서 차단으로 전환하면 오탐이 발생하여 트래픽이 중단될 수 있습니다. 올바른 접근 방식은 단계적 배포입니다. 중요하지 않은 부분에서 시작하여 조정 및 검증을 거친 다음, 명확한 롤백 기준을 설정하여 프로덕션 환경으로 확장하는 것입니다.

2 모든 AI 접점에 신원 인식 접근 제어 기능을 즉시 도입합니다

공용 인터넷에서 접근 가능한 모든 AI 엔드포인트는 기업 차원의 신원 확인 절차를 거쳐야 합니다. 이는 평가 대상 모든 조직에 100% 권장됩니다. 신원 확인 기반 접근 방식이 도입될 때까지 AI 인프라는 인터넷에 연결된 모든 공격자에 의해 악용될 수 있습니다.

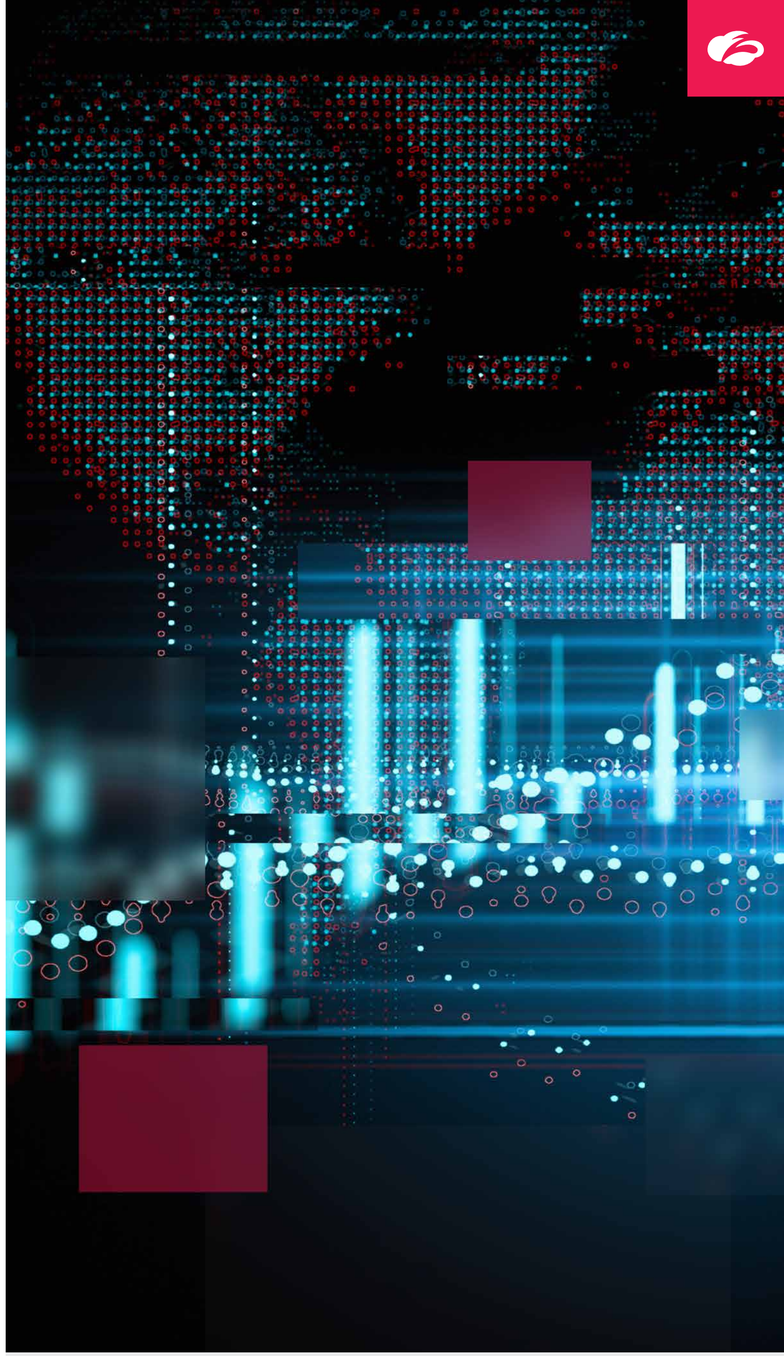
3 90일 이내에 SSL/TLS 검사 적격 보장률을 최소 70%까지 높입니다

모델을 선택적 동의 방식에서 선택적 거부 방식으로 전환합니다. 기본적으로 모든 트래픽을 검사한 다음, 세부적인 제외 대상을 생성합니다. “다른 정책 무시” 규칙을 삭제합니다. 검사 제외(Do-Not-Inspect) 예외 사항을 필요한 최소한의 항목으로 줄입니다. 2~4주간 애플리케이션 중단이 발생할 것을 감안해 계획을 수립합니다. 헬프데스크 업무량 급증에 대비해 인력을 배정합니다. 이러한 보안 범위가 없으면 DLP, IPS, 샌드박싱 및 AI 기반 트래픽 제어 기능이 대부분의 트래픽에서 제대로 작동할 수 없습니다.

SSL 검사는 보편적인 방식이 아니라 위험도에 기반해야 합니다. 가장 중요한 애플리케이션과 위험도가 높은 트래픽부터 시작하여 선택적으로 확장합니다. 일부 애플리케이션 및 서비스는 인증서 고정이나 규제 제약과 같은 예외 사항을 요구하기 때문에 조직은 예외 처리 경로와 신속 대응 절차를 사전에 정의해야 합니다. 현장 점검이 불가능한 경우, 보완 조치를 통해 가시성 공백을 줄입니다.

4 중요 부분에서 와일드카드 도메인을 명명된 FQDN으로 대체합니다

와일드카드 항목에 대한 모든 프라이빗 액세스 구성을 감사합니다. 핵심 자산인 금융 시스템, 지적 재산 저장소, 신원 확인 인프라를 우선적으로 교체합니다. 인증 시간 초과, 모든 액세스 규칙에 대한 장치 상태 유효성 검사, 그리고 각 ID를 필수 애플리케이션에만 제한하는 애플리케이션 수준 세분화를 구현합니다. 애플리케이션 담당자와의 부서 간 협업을 위한 계획을 수립합니다.



©2026 Zscaler, Inc. 모든 권리 보유.

5 핵심 네트워크 구간에 디셉션을 배포합니다

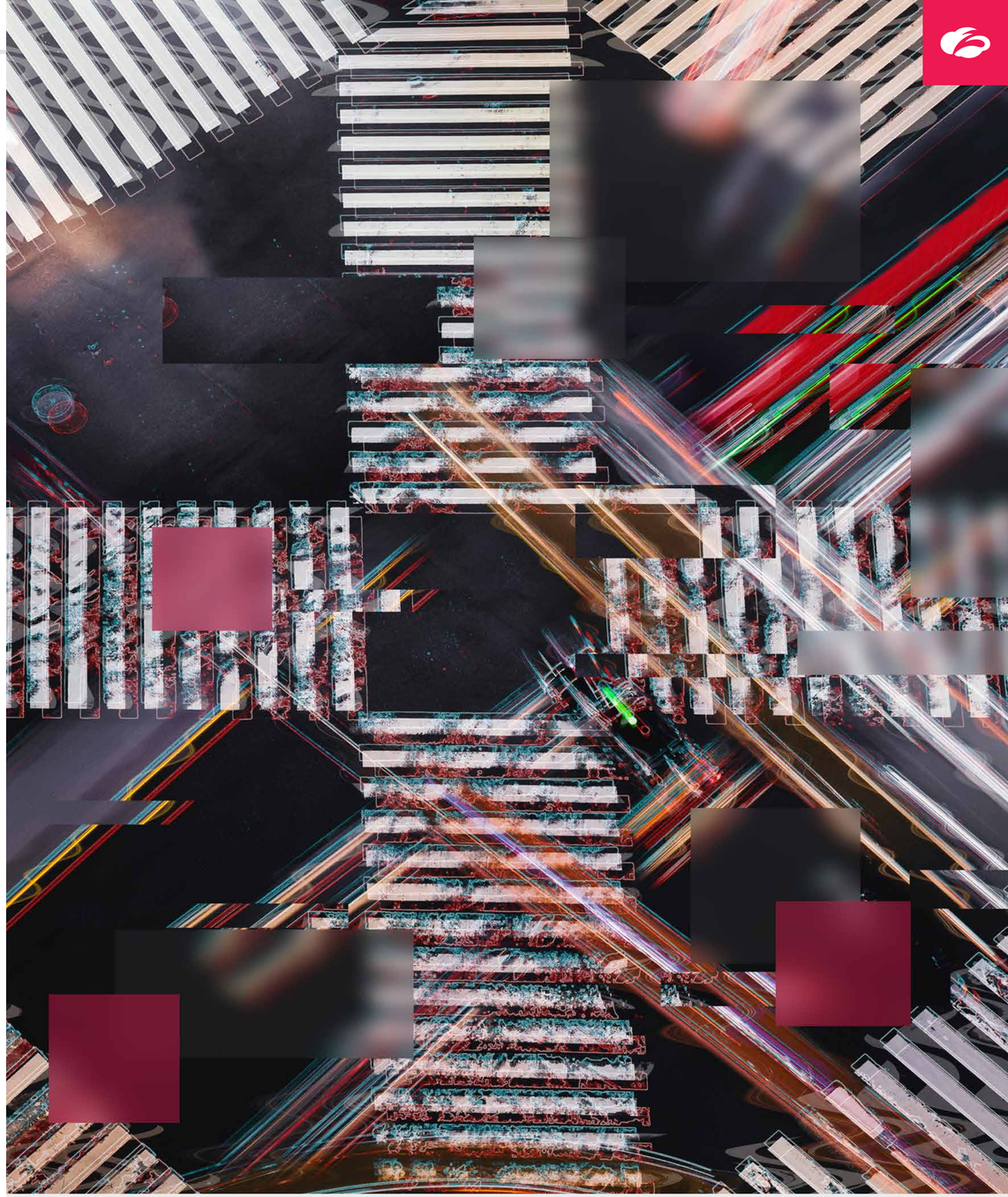
조직은 핵심 애플리케이션 주변에 디코이를 배치하여 방어 체계를 강화할 수 있으며, 이를 통해 SOC팀이 더 신속하게 대응할 수 있도록 정확도가 높은 경고를 제공하는 독립적인 탐지 계층을 구축할 수 있습니다. 디코이가 작동되면 Deception은 분석가의 승인 없이도 로그인된 모든 장치에서 ZPA를 통해 침해당한 사용자의 개인 애플리케이션 접근 권한을 자동으로 취소합니다. 이는 공격자가 방향을 바꾸기 전에 차단하여, SOC 대기열 속도가 아닌 공격 속도에 맞춰 측면 이동을 막습니다.

6 인터넷에 노출된 VPN 어플라이언스를 제로 트러스트 브로커 액세스 뒤로 이전합니다

검색 가능한 모든 VPN 장치는 사전 인증 공격 표면입니다. 30일 이내에 브로커링 액세스를 통해 모든 VPN 인프라를 전면적으로 보호합니다. 노출된 기기는 90일 이내에 폐기합니다. 이로써 프론티어 AI 모델이 먼저 탐색할 진입점이 사라집니다.

7 평가 후 72시간 이내에 인터넷에 노출된 자산의 CISA-KEV 취약점을 패치합니다

CVE-2024-38475, CVE-2021-40438 및 CVE-2023-44487은 EPSS 점수가 1.0에 가깝고 현재 활발히 악용되고 있는 것으로 확인되었습니다. 즉시 패치하거나 가상 패치를 적용합니다. 유지 관리 시간이 필요한 경우, 그 시간 동안 공격 시도를 차단하기 위해 자율 가상 패치를 배포합니다.



©2026 Zscaler, Inc. 모든 권리 보유.

규제 노출 관련 참고 사항

40점 미만의 점수를 받은 조직은 사이버 사고 발생 가능성과 잠재적 영향력을 높이는 통제상의 취약점을 가지고 있을 수 있습니다. 우리는 조직들이 위험 노출을 줄이고 회복력을 강화하는 데 도움이 되도록 이 보고서의 권장 사항을 검토하고 실행에 옮기기를 권장합니다. 경우에 따라 이러한 약점과 관련된 사건은 SEC 항목 1.05(양식 8-K)에 따른 공시 고려 사항을 야기할 수도 있습니다.

DORA 또는 NIS2의 적용을 받는 조직의 경우, 기본적인 통제 장치가 미비하다는 점은 ICT 위험 관리 및 전반적인 운영 복원력을 강화할 수 있는 기회를 나타낼 수도 있습니다.

다음 단계

프론티어 AI 준비도 평가는 각 조직에 정량화된 초기 점수, 우선순위가 지정된 개선 순서, 그리고 기존 기능을 확장하거나 미세 조정함으로써 달성 가능한 90일 목표를 제공합니다. 본 보고서의 데이터는 업계의 기준이 됩니다. 모든 보안 책임자에게 중요한 질문은 자사의 조직이 전체 조직 대비 어느 위치에 있는가 하는 것입니다.

분석 결과를 확인하셨습니다. 이제 노출도를 확인해 보세요.

Zscaler 전문가와 상담하여 환경 내 AI 관련 위험이 존재할 수 있는 영역을 파악하고, 우선적으로 해결해야 할 사항을 알아보세요.

위험을 파악하고, 신속하게 행동하며, 안전을 유지하세요.
더 자세한 정보는 zscaler.com/campaign/zscaler-ai-security-demo에서 확인하세요.

ThreatLabz 소개

ThreatLabz는 Zscaler의 보안 연구 부서입니다. 세계 최고 수준의 이 팀은 새로운 위협을 탐지하고 전 세계 수천 개의 Zscaler 플랫폼 사용 조직을 항상 안전하게 보호하는 역할을 담당합니다. 멀웨어 연구 및 행위 분석 외에도, 팀원들은 Zscaler 플랫폼의 지능형 위협 방어 기능을 위한 새로운 프로토타입 모듈 연구 개발에 참여하고 있으며, Zscaler 제품 및 인프라가 보안 규정 준수 기준을 충족하는지 확인하기 위해 정기적으로 내부 보안 감사를 실시합니다. ThreatLabz는 자사 포털인 research.zscaler.com 에 새롭게 등장하는 위협에 대한 심층 분석 자료를 정기적으로 게시합니다.

팔로우하세요: X @ThreatLabz | ThreatLabz 보안 연구 블로그

©2026 Zscaler, Inc. 모든 권리 보유.

zscaler™ | Act Fast. Stay Secure.

Zscaler 소개

Zscaler(NASDAQ: ZS)는 고객이 더욱 민첩하고 효율적이며 탄력적이고 안전하게 디지털 전환을 가속화할 수 있도록 지원합니다. Zscaler Zero Trust Exchange™ 플랫폼은 위치에 관계없이 사용자, 장치 및 애플리케이션을 안전하게 연결하여 수천 개의 고객사를 사이버 공격 및 데이터 손실로부터 보호합니다. 전 세계 150개 이상의 데이터 센터에 분산된 SSE 기반 Zero Trust Exchange™는 세계 최대 규모의 인라인 클라우드 보안 플랫폼입니다. 자세한 내용은 **zscaler.com**에서 확인하거나 X에서 **@zscaler**를 팔로우하세요.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ 및 **zscaler.com/legal/trademarks**에 명시된 기타 상표는 (i) 미국 및/또는 기타 국가에서 Zscaler, Inc.의 등록 상표 또는 서비스표이거나 (ii) Zscaler, Inc.의 상표 또는 서비스표입니다. 기타 모든 상표는 해당 소유자의 자산입니다.

+1 408.533.0288 **Zscaler, Inc. (본사) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**