Akamai

보고서

헬스케어 공급업체를 위한 사이버 보안

서론

급변하는 시장에서 경쟁하기 위해 헬스케어 공급업체는 고품질 환자 치료와 우수한 경험을 제공하고자 새로운 디바이스와 애플리케이션을 도입합니다. 새로운 디바이스와 애플리케이션이 추가될 때마다 환자에게는 혜택이, 기업에는 보안 리스크가 따릅니다.

이러한 복잡한 IT 환경은 PHI(Protected Health Information)의 높은 가치와 만나 사이버 범죄자에게 거부할 수 없는 기회를 제공하며, 사이버 범죄자는 계속해서 시스템을 공격하고 있습니다. 미국 보건복지부 보고서와 IBM의 리서치에 따르면, 팬데믹이 시작된 이후 헬스케어 업계에서 사이버 공격이 50% 증가했으며, 이러한 공격은 인시던트당 평균 713만 달러로 가장 많은 비용을 발생시켰습니다. IBM 보고서에 따르면, 악성 공격자가 빠른 복구가 필요한 병원 및 헬스케어 시스템을 노린 랜섬웨어 공격이 가장 흔한 위협이었고, 그 다음은 데이터 유출과 서버 접속이었습니다. 특히 헬스케어 공급업체는 다크웹에서 EHR(Electronic Health Record)이 개당 1000달러에 거래되는 반면, 신용카드 정보는 약 110달러, 사회보장번호는 단 1달러에 거래되기 때문에 랜섬웨어의 매력적인 표적이 되고 있습니다.

시스템을 향한 위협이 지속적으로 증가하고 있으나, 대부분의 기업은 이를 방어할 준비가 제대로 되어 있지 않습니다. 더 심각한 문제는 이미 침입을 당했음에도 인지조차 하지 못하는 기업도 있다는 사실입니다. 공격자는 이미 데이터를 유출하고 있거나 공격할 적절한 시기를 기다리고 있을 수 있습니다.

지금이야말로 디바이스의 인벤토리와 인프라에 연결되는 방식을 확인하고 기업의 공격표면을 명확히 파악해야 할 때입니다. 취약점이 어디에 존재하는지 효과적으로 파악해 적절한 방어 계획을 수립하면 사이버 공격의 잠재적 영향을 예방하거나 최소화할 수 있습니다.

가장 치명적인 사이버 보안 리스크에 대처하는 방법

위협 #1: 피싱 공격

피싱은 모든 업계에서 가장 흔한 사이버 공격 기법 중 하나입니다. 헬스케어 부문 사이버 보안 조정 센터에 따르면, 2021년에는 헬스케어 부문에 대한 피싱 공격이 크게 증가했습니다. 실제로 Akamai는 2020년 한 해 동안 범죄자들이 코로나19와 재정적 지원 약속 또는 경제적 어려움으로 인한 스트레스를 악용해 전 세계 사람을 대상으로 피싱 공격을 일으키는 것을 관측했습니다

피싱은 사기성 이메일이나 웹 페이지를 통해 민감한 데이터를 획득하려고 시도합니다. 피싱이 성공하면 사용자가 실수로 로그인 인증정보를 입력하도록 유도해 공격자가 네트워크에 침입할 수 있는 통로가 생깁니다.

뉴욕에서 실업 수당을 신청하는 사람들에게 이런 일이 발생했습니다. CSO Online의 전 편집자이자 현재 Akamai 보안 연구원인 스티브 래건(Steve Ragan)의 피싱 보고서에 따르면, 2021년 초에 PUA(Pandemic Unemployment Assistance) 프로그램을 노린 피싱 키트가 다수 발견되었습니다. 이 프로그램은 코로나19 봉쇄 기간 동안 도움이 필요한 사람들을 지원하기 위해 만들어졌고, 수백만 명의 미국인에게 필수적인 서비스를 제공했습니다.

레이건은 전국에 방영된 CBS News에서 뉴욕 주민을 겨냥한 실업 수당 피싱 키트와 범죄자들이 이 사기로 유출된 개인 정보를 수집하고 판매하는 방법에 대해 이야기했습니다. 뉴스 방영 후 레이건은 위스콘신, 인디애나, 펜실베이니아, 매사추세츠에서 주민들을 대상으로 하는 PUA 사기를 발견했습니다.

피싱 공격을 차단하고 방어하는 방법

기존의 보안 조치 및 권한 설정에 따라 다르지만, 범죄자가 단일 사용자 계정에 대한 접속 권한을 확보하면 네트워크의 중요한 부분을 자유롭게 지배할 수 있게 됩니다. 기업의 네트워크 내부로 침투한 후에는 그 범위를 넓힐 수 있습니다.

마이크로세그멘테이션은 공격자의 접속을 최초 접속 권한을 얻은 네트워크 부분으로만 제한해 측면 이동을 방지하고 그 외의 영역에 더이상 영향을 끼치지 못하도록 합니다. 범죄자가 어떤 진입점을 사용하더라도 기업의 더 넓은 네트워크에 접속하지 못하도록 차단함으로써 유출의 영향을 제한합니다.

마이크로세그멘테이션과 더불어 MFA(Multi-Factor Authentication)는 피싱 공격을 막는 최고의 방어선 중 하나입니다. 계정에 대한 접속을 허용하기 전에 신원 확인을 한 번 더 요구함으로써 추가적인 보안 레이어를 제공해 감염된 인증정보가 악용되는 것을 방지합니다.

특히 FIDO2 인증 솔루션인 MFA는 최신 공격을 방어할 수 있고, 사용자의 모바일 디바이스에서 문자 또는 인증 앱을 통해 생성된 고유 코드를 입력하도록 요구합니다. 이 추가 로그인 단계는 범죄자가 정확한 로그인 인증정보를 가지고 있는 경우에도 피싱 공격을 차단하는 데 도움이 됩니다.

피싱과 같은 소셜 엔지니어링 공격 기법을 주제로 직원을 교육해야 합니다. 현실적으로 피싱은 끊임없이 변하기 때문에 확실한 해결책이 없는 문제 중 하나입니다. 범죄자들이 다음에 무슨 짓을 할지 예측하기 어렵습니다. 피싱에서는 사람이 여전히 중요한 요소이므로, 가장 취약한 연결 고리로 남게 됩니다.

따라서 보안을 쉽게 만들어야 합니다. Akamai는 아무리 지능적인 사이버 범죄자의 공격도 방어할 수 있는 간편한 피싱 방지 MFA 솔루션을 제공합니다.

위협 #2: 지원되지 않는 레거시 소프트웨어

오래된 소프트웨어는 또 다른 심각한 취약점입니다. 새로운 보안 업데이트(패치)가 즉시 설치되지 않으면 네트워크에 침투할 수 있는 백도어가 생깁니다. 특히 지원 기간이 만료되어 더 이상 업데이트를 받지 못하는 구형 디바이스의 경우 더욱 그렇습니다.

지원되지 않는 소프트웨어는 제로데이 취약점이 있어 기업이 자체적으로 패치하기를 주저할 수 있습니다. 사용자 지정 패치를 만들면 디바이스의 보증이 무효화되어 문제가 발생했을 때 수리 비용이 많이 들 수 있습니다.

의료 디바이스는 수명이 길기 때문에 최신 버전의 운영 체제로 부지런히 업데이트하지 않거나 지원되지 않는 운영 체제를 실행하는 경우 해커가 취약점을 악용해 데이터를 훔치거나 병원 네트워크에 침투해 진료를 방해할 수 있습니다. 실제로 Fortune에 따르면, 유방조영술 머신부터 MRI 머신까지 인터넷에 연결된 의료 영상 디바이스의 83%가 취약한 것으로 나타났습니다.

오래된 디바이스, 특히 유지 관리 주기가 지난 디바이스일수록 범죄자가 써드파티 디바이스를 통해 기업의 네트워크에 접속할 수 있는 취약점을 알고 있을 가능성이 높습니다.

예를 들어, Windows 95는 유지 관리가 중단된 지 수년이 지났지만, 직접 쓰기가 가능했던 마지막 운영 체제였기 때문에 여전히 많은 MRI 머신이 이 운영 체제에 의존하고 있습니다. 사내 개발자가 취약점을 패치할 수는 있지만, 패치로 인해 머신에 대한 보증이 무효화될 수 있습니다. MRI 머신을 완전히 교체하는 것이 안전한 유일한 방법이지만 많은 시설에서 큰 비용을 지출해야 합니다.

네트워크 관리자는 지원되지 않는 시스템을 네트워크에서 분리하려고 노력하지만, 특히 환자 치료를 위해 디바이스가 필요하고 의사에게 데이터를 신속하게 제공해야 하는 경우에는 이런 방법이 불가능합니다. 또한 네트워크에 연결된 모든 디바이스의 맵이 불완전해 백도어가 발생하면 분리할 수 없습니다. 볼 수 없으면 방어할 수 없습니다.

취약하고 지원되지 않는 디바이스를 보호하는 방법

이러한 디바이스가 기업의 네트워크에 접속하지 못하도록 보호하려면 ZTNA(Zero Trust Network Access) 아키텍처로 전환해야 합니다. ZTNA는 들어오는 모든 요청을 안전성이 입증될 때까지 잠재적 위협으로 취급하는 프레임워크로, 소프트웨어가 오래되었더라도 공격자가 디바이스에 접속하기 전에 효과적으로 차단합니다.

ZTNA로의 전환은 과거의 성과 해자 접근 방식에서 검증 후 신뢰하는 제로 트러스트 모델로의 근본적인 전환을 의미합니다. 제로 트러스트 접근 방식은 사이버 공격을 완전히 차단하지는 못하지만, 잠재적 피해를 치명적인 수준에서 관리 가능한 수준으로 제한할 수 있습니다. HealthITSecurity의 말이 이를 잘 설명합니다. "공격자가 인증정보를 획득하고 하나의 디바이스를 조작하는 데 성공하더라도 제로 트러스트 아키텍처를 적용하면 더 이상 나아가지 못할 가능성이 높습니다."

Akamai는 공급업체가 현재 워크플로우를 중단하거나 유연성을 해치지 않고 제로 트러스트 아키텍처로 전환할 수 있도록 지원하는 강력한 계획을 제공합니다. 이 청사진 가이드로 ZTNA를 시작하세요.

위협 #3: 재택근무 및 BYOD를 도입한 공급업체

21세기의 치료 연속성은 분산되어 이루어집니다. 환자는 집에서 편안하게 치료받고, 공급업체는 직접 대면하지 않고 모바일 디바이스를 통해 진료합니다. 이렇게 접근성이 높아지면서 직원들이 현장과 집을 오가며 네트워크에 접속하고 관리되지 않는 디바이스로 로그인함에 따라 사이버 보안 리스크가 급격히 증가하고 있습니다.

팬데믹 이전에도 팀원이 가정용 네트워크에서 시스템에 로그인하기도 했겠지만, 펜데믹 동안 기업의 네트워크에 접속하는 개인용 디바이스의 수는 불가피하게 급증했습니다. 이러한 노트북, 태블릿, 스마트폰이 멀웨어에 감염된 경우 랜섬웨어 공격의 진입 경로가 될 수 있습니다.

예를 들어, 팀원이 실수로 가짜 웹 페이지에 로그인 인증정보를 입력해 피싱 공격의 피해자가 된다면 악성 공격자는 사용자가 가진 접속 권한을 똑같이 갖게 되어 파일을 암호화하고, 팀을 배제하고, 기업을 마비시켜 파일 복호화를 위한 거액의 랜섬을 요구할 수 있습니다.

네트워크 엣지를 보호하는 방법

기업의 네트워크에 접속하는 사용자(위치, IP 주소, 사용 디바이스 등)를 면밀히 모니터링하면 이와 같은 상황이 발생할 가능성을 최소화하고 공격이 발생하기 전에 차단할 수 있습니다.

개인용 디바이스를 사용하거나 재택근무를 하는 팀이라면 다음과 같이 자문해보세요.

- 들어오는 요청을 최대한 면밀하게 조사하고 공격이 발생하기 전에 차단하기 위해 ZTNA(Zero Trust Network Access) 접근 방식을 도입하고 있나요?
- 범죄자가 기업 네트워크에 침입하는 경우 접속을 제한하고 측면 이동을 방지하기 위해 마이크로세그멘테이션을 구축했나요?
- 지연 시간을 최소화하며 빠르고 쾌적한 사용자 경험을 유지하면서 네트워크를 보호하기 위해 SASE(Secure Access Service Edge) 프레임워크를 사용하고 있나요?
- 디바이스와 계정 로그인 시 접속 코드, 강력하고 고유한 비밀번호, MFA(Multi-Factor Authentication)를 사용하고 있나요?

Akamai는 원격 근무자 보안 솔루션으로 네트워크 접속 관리를 손쉽게 할 수 있도록 지원합니다.

위협 #4: 잘못된 데이터 흐름 매핑

한 발은 온프레미스에, 다른 한 발은 클라우드에 걸쳐 있으면 데이터가 어디에 있고 어떻게 흐르는지 파악하기가 불가능에 가깝습니다. 여기에는 몇 가지 원인이 있습니다.

첫째, 데이터의 양입니다. 벤더사, 계약업체, 컨설턴트 모두가 서로 다른 디바이스, 툴, 솔루션을 사용하기 때문에 매시간은 아니더라도 매일 네트워크에서 추가되고 제거되는 디바이스와 애플리케이션의 수를 따라잡기가 벅찰 수 있습니다.

둘째, 하드웨어와 소프트웨어를 추적하는 시스템이 팀원의 이직, 프로세스 변경, 우선순위 문제 등으로 인해 없어져 더 이상 정확하지 않거나 신뢰할 수 없게 된 경우입니다.

이유가 무엇이든, 보이지 않는 것은 보호할 수도 없기 때문에 네트워크와 연결된 디바이스를 시각화해야 합니다.

연결된 디바이스의 흐름을 매핑하는 방법

연결된 디바이스의 로드맵을 만들 수 있는 가시성 툴을 갖추어야 합니다. 특히 2019년 HIPAA Journal의 기사에 따르면, 헬스케어 기업의 82%가 지난 12개월 동안 연결된 디바이스를 겨냥한 사이버 공격을 받았다고 합니다.

연결된 디바이스 매핑의 첫 번째 단계는 네트워크에 연결되지 않은 디바이스를 포함해 네트워크 전반에서 데이터의 흐름을 추적해 데이터가 어디에서 오고 어디로 가는지 알려주는 솔루션을 선택하는 것입니다. 이를 통해 정보가 어디로 흘러가는지 실시간으로 네트워크 다이어그램을 파악할 수 있으며, 네트워크에 있을 수 있는 악성 의도를 가진 디바이스를 발견하는 데 도움이 됩니다. 핵심 시스템, 자산, 데이터(예: PHI)에 소프트웨어 정의 마이크로세그멘테이션 링을 설정하면 기업이 네트워크 내에서 공격자의 측면 이동을 제한할 수 있습니다. Akamai의 마이크로세그멘테이션 툴로 필요한 가시성을 확보하세요.

위협 #5: 네트워크, 앱, 시스템의 복잡성 관리

어떤 애플리케이션과 소프트웨어가 데이터를 읽을 수 있는지 알고 계시나요? 소셜 미디어 플랫폼과 같은 일부 소프트웨어 애플리케이션은 개인정보 보호정책이나 서비스 약관에 개인정보 침해 가능성을 명확히 명시하고 있습니다. 이메일 공급업체처럼 좀 더 은밀하지만, 여전히 상당한 리스크를 초래하는 애플리케이션도 있습니다(예: 사진에 PHI가 포함되었을 때 디바이스의 사진을 볼 수 있는 경우).

앱이 환자 식별자나 비밀번호를 포함해 클립보드에 복사된 항목을 볼 수 있도록 허용할 수도 있습니다. 디바이스에 환자 정보가 있는 경우 써드파티(또는 공격자)가 이를 보고 기록할 가능성이 있습니다.

팀 교육, 전체 네트워크 파악, 엣지 보호

헬스케어 기업의 모든 직원에게 개인 디바이스 사용의 리스크와 환자의 개인 정보를 보호하는 데 필요한 사항을 교육해야 합니다.

또한, 기업이 공격표면과 잠재적 기법에 대해 어떤 관점을 갖고 있는지 고려하는 것도 중요합니다. 보안팀이 여러 클라우드 서비스 사업자와 온프레미스 데이터 센터에 걸쳐 전체 네트워크를 모니터링하고 있나요? 아니면 여러 그룹이 기업 인프라의 여러 측면을 담당하는 구조로 분리되어 있나요? 특히 공격이 발생하는 동안에는 기업의 전체 네트워크와 그 활동을 종합적인 관점으로 파악해야 합니다.

네번째로 소개한 위협과 마찬가지로, 네트워크 엣지를 보호하기 위한 최선의 방어 옵션은 제로 트러스트 아키텍처와 계정 로그인을 위한 마이크로세그멘테이션 및 MFA를 결합하는 것입니다. 소유자와 클라우드 또는 온프레미스 상주 여부에 관계없이 모든 시스템을 보호하는 하나의 공급업체를 두면 사용자 경험을 방해하지 않으면서 네트워크를 보호할 수 있습니다.

비활동의 영향

여러가지 형태로 비용이 발생할 수 있습니다. 가장 명백한 것은 재정적 비용인데, IBM의 데이터 유출 비용 보고서 2021에 따르면 미국 헬스케어 기업은 단일 데이터 유출과 관련된 총비용으로 평균 923만 달러를 지출했습니다. 다른 비용으로는 환자 안전 및 신뢰와 같은 보다 질적인 비용이 있으며, 이는 헬스케어 기업에 더 크지는 않더라도 동등한 영향을 미칠 수 있습니다.

환자 안전 약화

사이버 보안과 관련된 가장 중요한 목표는 환자 안전입니다. 공격으로 인해 IT 시스템이 강제로 종료되면 환자 진료에 차질이 생깁니다. 치료와 예약이 늦어져 환자의 건강에 부정적인 결과를 초래할 수 있습니다. 실제로 최근 한 소송에서는 랜섬웨어 공격으로 인해 환자가 사망했다는 주장이 최초로 제기되기도 했습니다.

한편, 원격 환자 모니터링(예: 심박수 또는 혈당 수치)에 사용되는 연결된 의료 디바이스는 치료에 더 직접적인 위협이 될 수 있습니다. 예를 들어, 환자의 혈압 수치를 제대로 파악하지 못하면 위험한 상태를 알아채고 치료하지 못해 심각한 상황이 벌어질 수 있습니다.

환자 신뢰 상실

신뢰할 수 있는 치료를 제공하지 못하고 환자 정보를 보호하지 못하면 환자의 신뢰를 잃게 됩니다. 환자의 90% 이상이 데이터 유출로 인해 개인 정보가 유출될 경우 공급업체를 바꾸겠다고 답변했습니다. 실제 수치는 더 낮을 수도 있지만, 계산해보면 환자의 절반 또는 1/10만 이탈하더라도 환자 수가 얼마나 달라질까요? 그리고 새로운 환자를 점진적으로 확보하는 동안 얼마나 오래 손실이 지속될까요?

매출 손실

데이터 유출로 인한 가장 큰 비용 요인은 비즈니스 손실이 38%로 제일 높았습니다. EHR, 이메일 서버 등 핵심 공급업체 시스템이 다운되면 비즈니스가 중단됩니다. 환자 진료에 미치는 영향은 말할 것도 없고 예약, 방문, 대면은 물론 매출까지 없어진다는 의미입니다.

샌디에이고에 본사를 둔 Scripps Health는 2020년 5월에 대규모 사이버 공격을 받아 응급실 진료 및 대기 수술이 줄어들어 9160만 달러의 매출 손실을 입었습니다.

의료 시스템 네트워크의 일부가 계속 운영되고 있더라도 공격 기법을 찾아 취약점을 패치하고 포렌식 분석을 완료할 때까지는 그 무엇도 안전하다고 확신할 수 없습니다.

오버헤드 증가

사이버 보안 엔지니어를 구인하고, 고용하고, 유지하는 데는 상당한 비용이 들지만, 공격이 발생하면 실제로 훨씬 더 많은 비용이 듭니다. 기업에서 자체적으로 사이버 보안팀을 고용하면 커버리지에 큰 간극이 생길 수 있습니다.

일반적으로 기업이 네트워크에서 공격자를 식별하고 퇴출하는 데 시간이 오래 걸릴수록 비용은 더욱 증가합니다. Ponemon Institute의 보고서에 따르면, 사이버 공격을 처음 200일 이내에 탐지한 경우 기업이 126만 달러 이상을 절약할 수 있다고 합니다. 안타깝게도 같은 보고서에서 공격을 식별하고 차단하는 데 평균 287일이 걸린다고 밝혔습니다. 무려 287일입니다! 즉, 공격자들이 9개월 이상 네트워크 인프라 내부에 머물면서 공격을 계획하고 실행해 병원의 평판과 수익에 최대한의 피해를 입히는 경우가 많다는 뜻입니다.

보안팀이 공격을 식별하고 조치를 취하는 데 필요한 시간을 정량화하는 것이 필수적입니다. 보안 벤더사를 매니지드 서비스와 엔지니어링 지원을 제공하는 업체로 통합하면 상당한 비용을 절감할 수 있습니다

규제 벌금

귀중한 개인 정보를 많이 보유하고 있는 경우 데이터 유출로 인해 규제 기관으로부터 막대한 벌금이 부과될 수 있습니다. 2021년 11월 30일 기준으로 보건복지부 산하 민권청은 106개의 HIPAA 적용 대상 기업에 총 1억 3100만 달러 이상의 벌금을 정산하거나 부과했습니다. 이는 여기에 언급된 추가 비용 외에도 처벌당 평균 120만 달러가 넘는 금액입니다.

헬스케어 기업이 사이버 공격에 가장 효과적으로 대비하는 방법

오늘날의 사이버 위협은 헬스케어 기업에 업계 최고의 보안을 요구합니다. 환자와 비즈니스가 보안에 달려 있기 때문에 보안에 소홀히 하면 매우 큰 대가를 치뤄야 합니다.

재정적 제약, 우선순위 문제, 리스크의 불확실성 때문에 너무 많은 리스크를 감수하게 될 수 있습니다. 하지만 보안 활동은 철저하고, 전략적이고, 경계심을 갖고, 민첩하게 이루어져야 합니다.

오늘 안전하게 보호되는 생태계가 내일도 반드시 안전하리라는 보장은 없습니다. 위협은 빠르게 진화합니다. 공격자가 새로운 취약점을 악용하는 데 걸리는 시간은 하루도 채 안 될 수 있습니다.

이 위협 영역을 줄이고 연방 권고에 명시된 백업 접근 방식에 대한 조언(최소 두 가지 형식으로 3개의 사본을 저장하고 1개는 오프라인에 저장)을 받아들이려는 공급업체들이 하이브리드 접근 방식을 모색하는 경우가 늘고 있습니다. 온프레미스 데이터 스토리지를 사용하면 보안을 보다 효과적으로 제어할 수 있지만 비용이 많이 들 수 있고, 특히 팬데믹으로 촉발된 현재의 의료 데이터 급증과 헬스케어 디지털 전환에 맞춰 필요한 속도로 확장하기가 어려울 수 있습니다. 퍼블릭 클라우드 데이터 스토리지는 보다 비용 효율적이지만 장애 리스크가 있으며, 데이터가 어떻게 보호되는지 파악하기 어려울 수 있습니다.

하이브리드 접근 방식을 사용하면 민감한 데이터는 온프레미스에 보관하고 덜 민감한 데이터는 클라우드에 저장할 수 있습니다. 하지만 두 가지 스토리지 유형 간에 전송되는 데이터를 보호하고 데이터 전송 및 조회 권한이 있는 사람에게만 접속을 허용하는 보안 조치를 마련해야 하기 때문에 이 방법도 완벽하지는 않습니다. ZTNA 아키텍처를 구축하기 위한 7가지 주요 요구사항을 준수하면 사용자에게 업무에 필요한 애플리케이션에만 접속 권한을 부여하고 MFA가 제공하는 추가 보안을 활용해 데이터를 보호할 수 있습니다.

Akamai는 가상의 공격이 아니라 실제 공격이 발생했을 때 대비할 수 있도록 지원합니다. Akamai와 함께 네트워크에 대한 통합적인 관점을 구축해 공격을 신속하게 발견하고 피해를 효율적으로 방어하세요. Akamai는 분산 서비스 거부 및 랜섬웨어 공격으로부터 네트워크를 보호해 원활하고 안전한 웹 경험(앱 및 API 포함)을 제공합니다.

네트워크의 엣지를 강화해 유출 가능성을 제한하고 유출이 발생했을 때 피해 반경을 줄입니다. 또한, 사용자 접속의 유연성을 유지하면서 보안을 제공하기 때문에 기업은 끊임없이 변화하는 운영 및 치료 요구사항 속에서 최적의 헬스케어 결과를 제공하는 데 집중할 수 있습니다.

점점 더 정교해지는 사이버 범죄와 확장되는 클라우드 기반 공격표면으로부터 환자 정보를 보호하는 것이 그 어느 때보다 중요해졌습니다. 환자 중심의 기업과 정부 기관은 Akamai의 엣지 플랫폼을 믿고 선택해 환자와 더 가까이에서 디지털 경험을 제공하고 위협은 멀리서 차단할 수 있습니다.

Akamai를 믿고, 사이버 보안을 끝없는 부담에서 경쟁력으로 바꿔보세요.

자세한 내용을 알아보면 Akamai에 문의하거나 +1-877-425-2624번으로 연락해주세요.

Akamai는 온라인 라이프를 강력하게 지원하고 보호합니다. 전 세계의 혁신적인 기업들은 매일 수십억 명 고객의 생활, 업무, 여가를 돕고 디지털 경험을 안전하게 전송하기 위해 Akamai를 선택합니다. Akamai는 세계에서 가장 크고 가장 신뢰 받는 엣지 플랫폼을 통해 사용자와 가까운 곳에서 앱, 코드, 경험을 제공하고 위협을 먼 곳에서 차단합니다. Akamai의 보안, 콘텐츠 전송, 엣지 컴퓨팅 제품과 서비스에 관해 자세히 알아보시려면 홈페이지(www.akamai.com), 블로그(blogs.akamai.com)를 방문하거나 X, LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2022년 02월 발행.