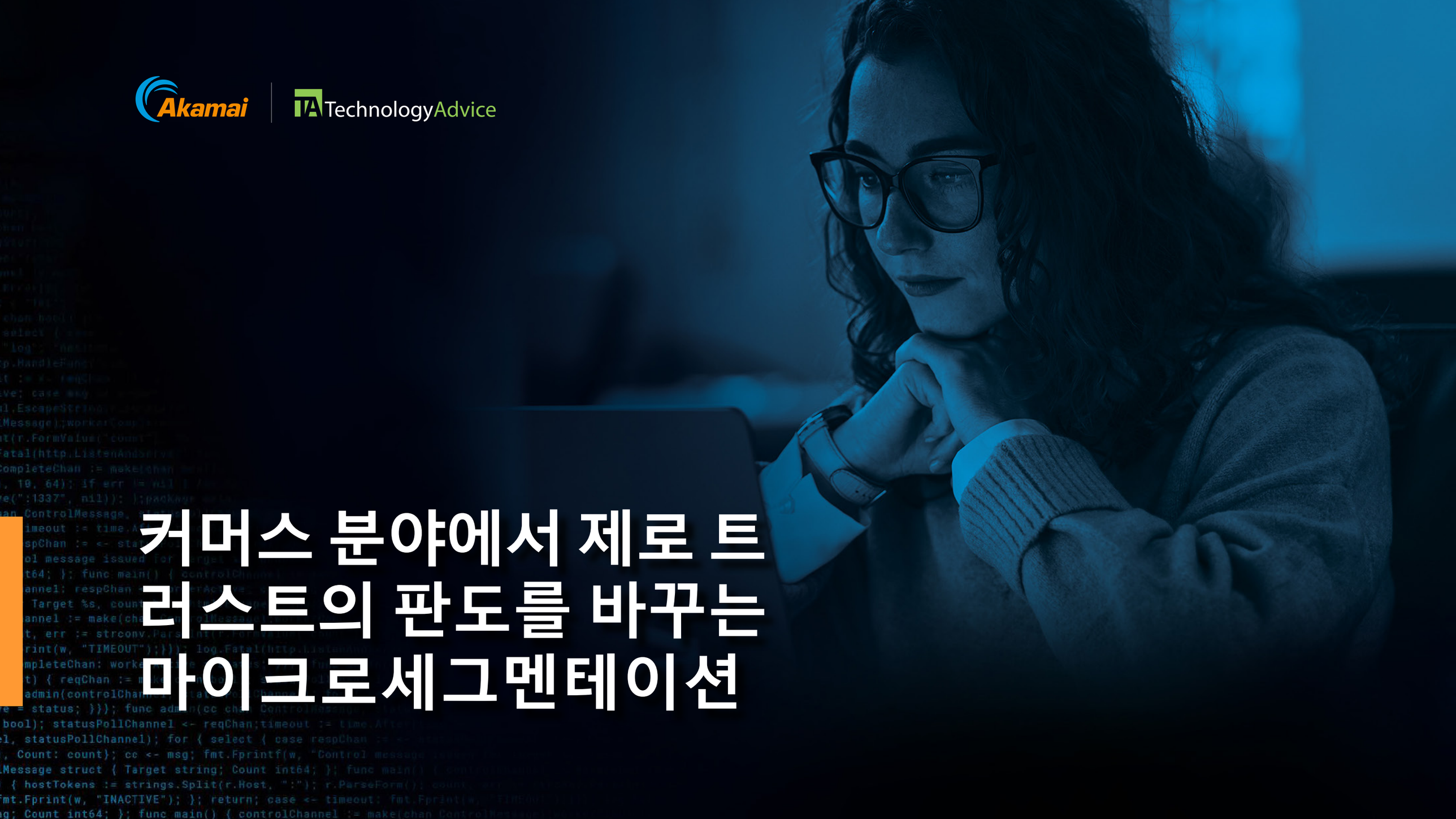
Akamai | TechnologyAdvice



커머스 분야에서 제로 트러스트의 판도를 바꾸는 마이크로세그멘테이션

리테일, 여행, 호텔 분야의 커머스 기업은 민감한 기업 또는 금융 데이터로 수익을 창출하려는 사이버 범죄자, 랜섬웨어 기업, 사기꾼의 매력적인 공격 대상입니다. RH-ISAC 산업 인사이트 보고서에 따르면 가장 일반적으로 도난의 대상이 되는 정보 종류는 신용카드 및 결제 정보, 보상 또는 로열티 프로그램의 PII(Personally Identifiable Information), 지적 재산입니다.

공격자가 랜섬웨어 및 기타 종류의 멀웨어를 배포할 목적으로 네트워크에 침입할 수 있기 때문에, 이들의 가시권 내에 들어온 기업과 보안팀은 수많은 침입 지점과 씨름해야 합니다. 모든 기업이 피싱 이메일, 도난당한 VPN 인증정보, 제로데이 악용으로 인한 피해에 직면한 가운데, 커머스 기업은 키오스크, IoT 디바이스, 매장 내 태블릿, POS 단말기, 게스트 Wi-Fi 등으로 인해 발생하는 추가적인 리스크도 관리해야 합니다. 비즈니스 운영을 위해 대중에게 개방되는 리테일 매장은 복잡성을 가중시키며 기업은 물리적 공격표면과 모든 범위의 추가 위협에 노출됩니다.

보안 인시던트의 82%를 차지하는 주요 원인인 인적 실수를 보완하기 위해 방대한 데이터와 수많은 공격 기법에 대응해야 하는 기업 보안팀 직원의 부담은 점점 증가하고 있습니다. PCI(Payment Card Industry) 또는 정부 규제(GDPR, SEC 등)의 규제 감시가 강화되고 압박이 가중되면서 이미 부족한 IT 보안 예산과 리소스는 더 많이 소모되고 있습니다.

모든 리스크를 제거하는 것은 불가능하지만, 오늘날의 커머스 기업은 불가피한 감염 확산이나 경계 방어 우회를 신속하게 탐지하고 차단하기 위해 '유출을 가정하는' 사고방식을 도입해야 합니다. Akamai의 제로 트러스트 세그멘테이션 솔루션은 커머스 기업이 애플리케이션, 서버, 네트워크 환경을 더 쉽고 빠르게 보호하고 암호화 손상과 민감한 데이터 유출을 모두 방지할 수 있도록 지원합니다.

마이크로세그멘테이션은 소프트웨어 정의 접근 방식을 통해 더욱 강화되는 기능으로, 커머스 기업에 3가지 핵심 기능을 제공하는 제로 트러스트 보안 프레임워크의 기반을

제공합니다. 첫째, 마이크로세그멘테이션은 측면 이동을 차단해 랜섬웨어 감염의 잠재적 영향을 자연스럽게 제한합니다. 둘째, PCI 컴플라이언스 준수 유지에 드는 비용을 절감할 수 있습니다. 마지막으로 마이크로세그멘테이션은 레거시 인프라뿐만 아니라 하이브리드, 멀티클라우드, 마이크로서비스 환경 전반에서 오늘날의 복잡한 생태계를 보호하는 데 필요한 정밀한 가시성과 커버리지를 제공합니다.

랜섬웨어의 잠재적 영향 제한

공격자는 랜섬웨어 공격을 준비하면서 기업의 핵심 자산을 찾기 위해 이메일 피싱 링크 클릭, 보안 설정 오류, 오픈 RDP 포트 또는 감염된 인증정보를 통해 주기적으로 네트워크를 탐색합니다. 성공적인 대량 암호화 이벤트와 데이터 유출을 통한 이중 갈취 공격을 받은 기업은 여러 단계의 재정적 손실과 비즈니스 피해를 입게 됩니다.

온라인 주문과 매장 운영이 느려지거나 중단되어 고객이 상품을 구매하거나 호텔 또는 항공권을 예약할 수 없게 되면 **직접적인 비즈니스 손실**이 즉각적으로 발생할 수 있습니다. 공격의 확산을 막는 과정에서 중요한 시스템과 서버에 접속할 수 없게 되거나 오프라인 상태가 되면 이커머스 운영이 기존 주문을 처리, 실행, 배송하지 못할 수 있습니다.

민감한 회사 또는 고객 데이터가 유출되면 공개적인 망신과 브랜드 평판 손상으로 **간접적인 비즈니스 손실**이 발생합니다. 랜섬웨어 조직은 '폭로' 사이트에 공격 사실을 공개하고 데이터를 유출해 피해자를 더 많이 갈취하고 성공적인 대가 지불에 대한 압박을 가중시키는 기법을 즐겨 사용합니다. 기업은 SEC의 최근 요구사항에 따라 비즈니스에 중대한 영향을 미치는 경우 4일 이내에 SEC에 통보해야 하는데 이는 언론 보도와 평판 손상으로 이어집니다.

컨설턴트와 IT 팀이 데이터를 복구하고 백업을 복원하며 시스템을 다시 온라인 상태로 만들기 위해 노력하는 과정에서 랜섬웨어 복구와 직접적으로 관련된 법률 비용, 인시던트 대응, 데이터 포렌식, 유출 해결을 위한 **복구 비용**이 많이 듭니다. 여기에 소송 비용이나 민감한 정보 유출로 인한 규제 처벌 및 벌금이 추가될 수 있습니다. 사이버 보험료가 급격히 인상되거나 랜섬웨어 보상금 지급이 거부되거나 보험 적용이 아예 중단될 수도 있습니다.

이렇게 리스크가 높기 때문에 랜섬웨어 공격은 2024년 리테일 및 호텔 CISO의 가장 큰 리스크 우려 사항으로 꼽혔고, 보안 리더들은 공격자가 발판을 마련한 후 리스크를 줄여줄 제어 조치에 언제든 투자할 준비가 되어 있습니다. 그러나 랜섬웨어가 확산하려면 공격자가 초기 접속 권한을 확보한 후 측면으로 이동해 영향력을 극대화해야 합니다. Microsoft 디지털 방어 보고서 2022에 따르면 랜섬웨어 인시던트의 93%는 공격자가 중요한 애플리케이션과 인프라를 잠그도록 허용하는 부적절한 측면 이동 제어로 인해 발생했으며, 공격자가 기업 네트워크 내 엔드포인트에서 측면 이동을 시작하는 데 걸리는 평균 시간은 1시간 42분에 불과했습니다.

Akamai의 최근 세그멘테이션 현황 데이터에 따르면, 이커머스 기업은 지난 12개월 동안 다른 업계에 비해 랜섬웨어 공격을 가장 많이 받은 것으로 나타났습니다. 그렇기 때문에 CISO와 보안 전문가들은 랜섬웨어 감염 리스크를 줄이고 공격표면을 최소화하며 랜섬웨어 킬 체인을 차단하기 위해 마이크로세그멘테이션과 같은 제로 트러스트 기반의 보안 툴로 전환하고 있습니다.

측면 이동을 통한 탐색을 탐지하고 차단하면 공격자가 권한을 상승시키고, 민감한 정보를 찾고, 대규모 랜섬웨어 공격을 전파하기 위해 IT 자산에 접속하는 데 어려움을 겪게 됩니다. 애널리스트들이 인정한 Akamai의 마이크로세그멘테이션 솔루션은 전체 커머스 인프라의 중요 워크로드에 최소 권한 접속 원칙을 적용함으로써 애플리케이션과 워크로드의 횡방향 데이터 흐름에 대한 심층적인 가시성과 소프트웨어 정의 정책을 통한 정밀한 보호를 통해 측면 이동을 제한하고 공격자의 추적을 차단하도록 지원합니다.

대표적인 사이버 보험사들도 마이크로세그멘테이션의 가치를 잘 알고 있습니다. 랜섬웨어로 인해 보험 구매와 청구가 급증하면서 여러 보험사들은 보안 제어 요구사항과 면밀한 조사를 강화하고, 보험료를 전년 대비 최대 96%까지 인상하고, 막대한 손실에 대비해 랜섬 보상금 지급 한도를 축소해야만 했습니다. 사이버 보험 시장에서 보험료가 너무 높아 구매할 수 없는 기업들도 있고 보험 가입이 아예 거부되는 경우도 있습니다. 사이버 보험만으로 침입으로 인한 피해와 그로 인한 재정적 손실을 막을 수 없지만, 마이크로세그멘테이션과 같은 보안 제어 수단을 활용하면 계약 심사에 필요한 최신 요구사항을 보다 간편하게 충족할 수 있습니다.

"머신에 단일 에이전트를 배포해 측면 이동으로 인한 엔드포인트 공격 문제를 해결했습니다."

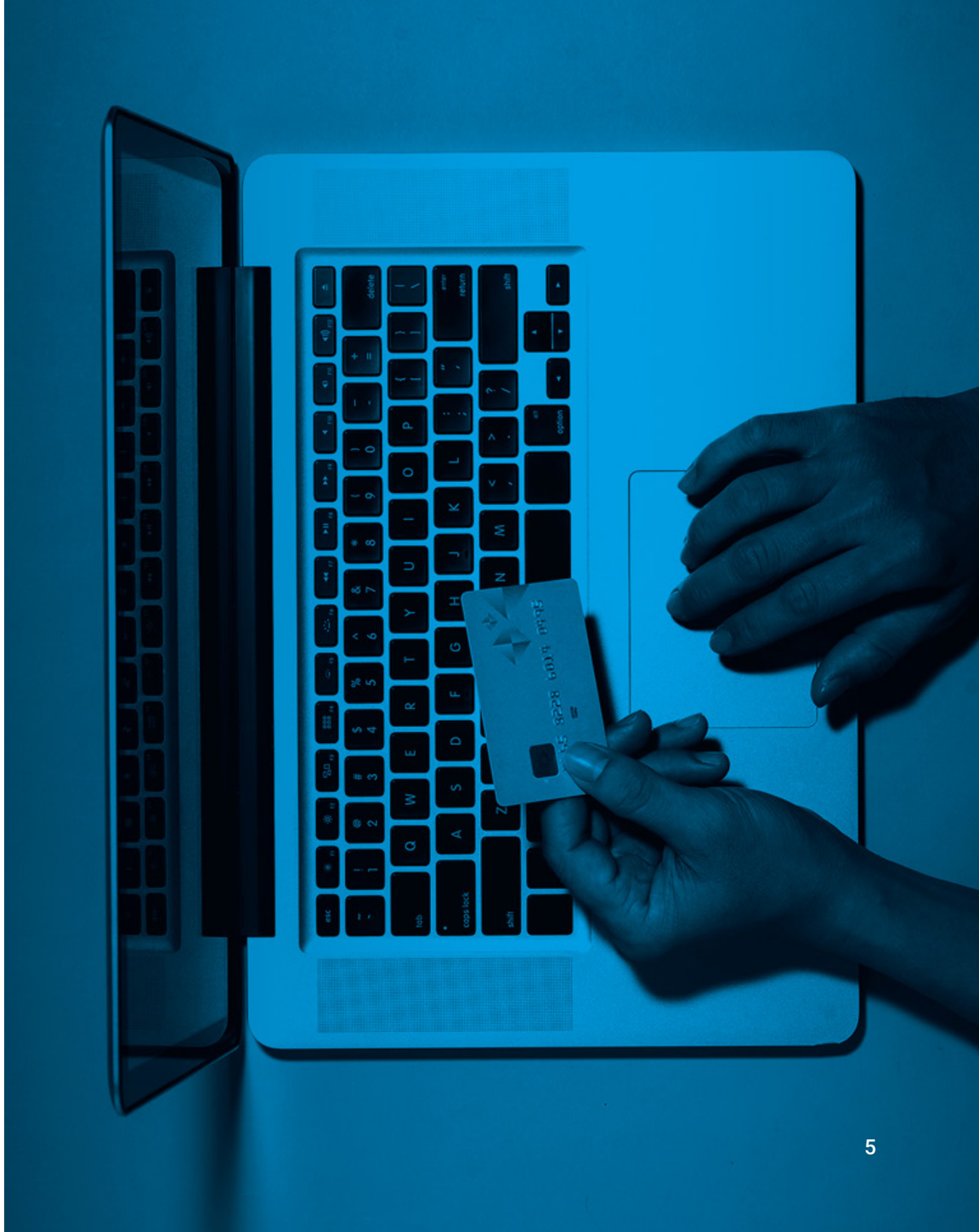
글로벌 리테일 및 소비재 제조업체
인프라 아키텍트

PCI 컴플라이언스 감사 범위 축소

이커머스 기업들도 잘 알다시피 PCI 컴플라이언스 준수 및 유지는 연간 거버넌스, 리스크 및 컴플라이언스 예산의 상당 부분을 차지하며 보안 FTE와 리소스에 상당한 부담을 줄 수 있습니다. PCI 데이터 보안 표준(PCI DSS)에 따라 CDE(Cardholder Data Environment)를 보호하려면 보안 정책 및 제어를 지속적으로 감사해야 합니다. CHD(Cardholder Data)와 상호 작용하거나 보안에 영향을 미칠 수 있는 사람, 프로세스, 기술을 식별하는 PCI 범위 지정도 PCI 감사 수행과 관련된 비용을 크게 증가시킬 수 있습니다.

네트워크 세그멘테이션은 PCI DSS의 공식 요구사항은 아니지만, 커머스 기업은 수년 동안 컴플라이언스 범위, 비용, 리스크, 유지 관리의 어려움을 경감시키기 위해 vLAN, ACL, 내부 방화벽과 같은 전통적인 네트워크 세그멘테이션 방법을 활용해 왔습니다. 그러나 최신 리테일 기업의 IT 환경이 하이브리드, 멀티클라우드, 마이크로서비스 아키텍처 전반에서 더욱 역동적으로 변화하면서 레거시 세그멘테이션 기술과 기법은 그 속도를 따라가지 못해 운영 오버헤드, 복잡성, 애플리케이션 다운타임은 물론 보안 공백이 발생하고 있습니다.

레거시 세그멘테이션 방식은 관리 및 유지 관리가 번거롭고 CDE 경계 내의 시스템, 네트워크, 애플리케이션을 적절히 보호하고 제어하기 위해 리소스를 소모하기 때문입니다. 기업은 데이터 센터와 클라우드에서 컨테이너 기반 자산에 이르기까지 다양한 기반으로 운영되기 때문에 애플리케이션 및 시스템 통신 흐름에 대한 포괄적인 가시성이 부족하고 PCI에서 요구하는 방화벽 설정 표준을 유지하는 데 어려움을 겪는 경우가 많습니다.



이는 보안 공백이 발생하고 PCI 감사가 실패하는 잘못된 세그멘테이션 관행으로 이어집니다. 그래서 커머스 기업들은 인프라 전반에서 CDE와 범위 외 시스템을 보다 쉽게 분리하고, PCI 감사 범위를 줄이고, 레거시 툴의 지원 범위를 훨씬 뛰어넘는 프로세스 레이어 7까지 세그멘테이션 및 적용을 가능하게 함으로써 컴플라이언스를 가속하기 위해 **소프트웨어 정의 세그멘테이션으로 전환**하고 있습니다. Akamai의 경량 에이전트는 방화벽, 네트워크 변경, 서버 재부팅이 필요하지 않고 기본 인프라와 독립적으로 운영되기 때문에 애플리케이션 다운타임이 없으며 변경 제어 또는 유지 관리 기간을 피할 수 있습니다.

소프트웨어 정의 세그멘테이션은 기본 인프라 및 운영 체제에서 보안을 분리하기 때문에 네트워크나 애플리케이션을 건드리지 않고도 독립적으로 세그멘테이션을 수행할 수 있습니다. 커머스 기업이 이 접근 방식을 도입하면 분산된 스테이트풀(stateful) 검사 방화벽 역할을 하는 솔루션을 통해 환경 전반에서 정밀한 네트워크 및 자산 가시성을 확보해 완벽한 커버리지를 달성할 수 있습니다. 또한 배포 및 관리에 필요한 노력과 리소스가 줄어들고 **SecOps 생산성이 최대 95% 향상되기 때문에** PCI 컴플라이언스에 따른 많은 어려움 없이 더욱 강력한 보안 체계를 갖출 수 있습니다. 커머스 기업은 감사 시 네트워크에 대한 실시간 및 기록 보기를 활용해 컴플라이언스 여부를 검증할 수도 있습니다.

"소프트웨어 정의 세그멘테이션을 통해 프로세스 수준에서 세그멘테이션 정책을 생성하고 실행할 수 있기 때문에 보안 체계와 PCI-DSS 기술 요구사항을 준수하는 역량이 크게 개선되었습니다."

The Honey Baked Ham Company 수석 인프라 엔지니어

IoT에서 레거시 인프라에 이르는 가시성 및 범위 확보

랜섬웨어 확산 차단부터 PCI 컴플라이언스 보안 제어 관리까지, 커머스 기업은 오프라인 매장, 생산 시설, 유통 창고와 같은 물리적 위치를 보호해야 하는 복잡한 문제에 직면했습니다. 항공사의 경우 IoT 센서와 디바이스를 통해 항공기 시스템을 실시간으로 모니터링하고 예측 유지보수를 통해 성능과 안전을 강화할 수 있습니다. 호텔 업계에서는 IoT 기반 디바이스를 배포해 고객 경험과 운영 효율성을 높이기 위해 설계된 스마트 호텔 객실을 구현합니다.

하드웨어 및 소프트웨어 취약점이 증가할 수밖에 없는 이유는 이렇게 수많은 위치와 환경에 호스트 기반의 보안 에이전트를 실행할 수 없는 수많은 IoT(Internet of Things) 또는 OT(Operational Technology) 자산이 포함되어 있기 때문입니다. Forrester의 "2023년 IoT 보안 현황" 리서치에 따르면 글로벌 수석 보안 리더의 33%가 **외부 사이버 공격의 가장 큰 표적으로 IoT 디바이스**를 꼽았습니다. 따라서 기업은 IoT 및 OT 환경을 보호하는 에이전트리스 기능을 갖춘 세그멘테이션 솔루션을 배포하고 공격자가 더 광범위한 IT 인프라에 접속하기 위해 디바이스 취약점을 악용하는 리스크를 최소화해야 합니다.

이런 종류의 솔루션은 새로 연결된 디바이스를 지속적으로 모니터링하고 승인되지 않은 디바이스가 네트워크와 통신하는 것을 자동으로 차단할 수 있어야 합니다. Akamai 솔루션은 통합 디바이스 핑거프린팅을 통해 연결된 디바이스를 자동으로 검색하고 논리적 그룹으로 분류해 확장 가능한 추상적인 보안 정책의 기반을 형성합니다. 통합 인터페이스를 통해 IoT 및 OT 디바이스에 대한 세그멘테이션 정책을 생성할 수 있으며, 다른 정책과 마찬가지로 디바이스가 새로운 네트워크 위치로 로밍할 때에도 디바이스 위치나 환경 내 디바이스 수에 관계없이 핑거프린팅된 디바이스를 따릅니다.

제로 트러스트 기반 정책은 에이전트 없이 네트워크 스위치 ACL을 통해 적용되기 때문에 IoT 및 OT 배포 전반에서 리스크를 초래하는 정책 공백을 없앨 수 있습니다. 이와 같이 보안 경계를 확립하는 동시에 IT 관리 시스템, 전용 업데이트 서버, 로깅 서버에 필요한 연결을 허용해 보안 제약 조건을 줄일 수 있습니다. Akamai 솔루션을 사용하면 모든 IoT 및 OT 시스템을 IT 인프라와 함께 검색, 시각화, 매핑해 기업 자산을 한 눈에 파악할 수 있습니다.

IoT/OT 자산과 기타 안전한 엔드포인트 보안 외에도, 수많은 리테일 기업이 패치가 불가능한 레거시 또는 지원 종료 운영 체제 및 인프라에서 실행되는 시스템, 서버, 애플리케이션에 의존하면서 상당한 리스크를 초래하고 있습니다. 이러한 레거시 서버 중 상당수는 기업의 매출을 창출하거나 핵심 역할을 하고 있기 때문에 제거할 수 없으며, 특히 클라우드에서 탄생한 이커머스 기업이 아닌 경우 더욱 그렇습니다. Akamai의 에이전트는 업계를 대표하는 가장 광범위한 커버리지와 호환성을 바탕으로 최신 및 레거시 운영 체제에서 모두 실행되어 네트워크 흐름에 대한 완벽한 가시성을 제공하며, Windows 및 Linux 운영 체제의 개별 프로세스 및 서비스 수준과 함께 MacOS 엔드포인트에 대한 커버리지까지 제공합니다.

다른 솔루션은 레거시 운영 체제에 대한 부분적인 가시성만 제공하며, Windows Server 2008 R2 이전의 Microsoft Windows 시스템에 대한 가시성은 제공하지 않습니다. 이는 기존 마이크로세그멘테이션 솔루션의 에이전트가 2002년 이후 시스템에서만 사용 가능한 Windows 방화벽에 의존해 정책을 시행하기 때문입니다. Linux 시스템용 에이전트는 Linux 환경에 대한 레이어 7 프로세스 수준의 룰 없이 레이어 4 가시성만 지원하며, iptables에 의존해 정책을 적용합니다. Akamai Guardicore Segmentation 기능은 기본 인프라에 의존하지 않고 작동하기 때문에 신규 및 레거시 등 거의 모든 Windows 및 Linux 운영 체제에서 지원됩니다.

간편하고 빠르고 직관적이며 더욱 안전한 솔루션

본사에서 리테일 매장, 데이터 센터에서 클라우드까지, 그리고 그 이상의 범위까지 제로 트러스트를 도입해 중요한 IT 자산을 보호하고 보안을 유지하려면 마이크로세그멘테이션이 필수적입니다.

Akamai Guardicore Segmentation은 기존의 느린 네트워크 세그멘테이션 방식에 비해 배포 및 적용, 모니터링, 인시던트 대응에 소요되는 시간과 노력을 획기적으로 줄여주는 간소화된 솔루션입니다. 정책 변경 사항을 신속히 구축할 수 있으며 복잡한 네트워크 변경이 필요하지 않아 판매 성수기, 프로모션, 제품 출시 또는 기타 주목할 만한 이벤트 기간에 더욱 편리합니다.

중요한 사실: 기업이 고객, 게스트, 승객에게 품질과 안전 중 하나를 선택하라고 요구하지 않는 것처럼, 좋은 마이크로세그멘테이션 솔루션은 보안과 민첩성 중 하나를 선택하라고 요구하지 않습니다. 이제 더 이상 어려운 방식으로 세그멘테이션하지 않아도 됩니다.

더 자세한 정보가 필요하신가요?

Akamai 제로 트러스트 포트폴리오 솔루션인 Akamai Guardicore Segmentation을 통해 공격표면을 줄이고, 중요 애플리케이션을 보호하고, 컴플라이언스를 간소화하는 방법을 확인하세요.

자세히 보기

TechnologyAdvice | Akamai

Akamai는 구축 및 전송되는 장소에 상관 없이 만들어지는 모든 것에 보안 기능을 내장하도록 지원함으로써 고객 경험, 직원, 시스템, 데이터를 보호합니다. Akamai 플랫폼은 글로벌 위협에 대한 가시성을 바탕으로 제로 트러스트 지원, 랜섬웨어 차단, 앱 및 API 보안 또는 DDoS 공격 차단을 목표로 보안 체계를 조정하고 발전시켜 지속적으로 안심하고 혁신하며 확장하고 가능성을 현실로 구현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com 및 akamai.com/blog를 확인하거나 X (기존의 Twitter) LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다.