MARKET PERSPECTIVE

클라이언트 측 WAF: 차세대 보안 최전선

크리스토퍼 로드리게스(Christopher Rodriguez)

EXECUTIVE SNAPSHOT

그림 1

Executive Snapshot: 클라이언트 측 위협과 새로운 솔루션

2018년 보안 연구원들은 온라인 카드 스키밍 또는 웹 스키밍이라고 불리는 새로운 형태의 사이버 범죄를 발견했습니다. Magecart 공격은 애플리케이션 기능이 서버에서 클라이언트로 이동하고 있는 트렌드를 악용했습니다. 공격자들은 WAF가 없는 사용자의 브라우저에서 신뢰할 수 있는 애플리케이션 소스에 악성 코드를 주입할 수 있었습니다. 이 공격은 장기간 계속 되었고 기업 웹 애플리케이션 보안 체계의 취약한 부분을 보여주는 데이터 유출 사고였습니다.

핵심 내용

- 클라이언트 측 스크립트는 애플리케이션 아키텍처의 중요한 툴이며 사용자 경험, 애플리케이션 성능, 분석, 보안을 강화합니다.
- 스크립트는 모든 곳에 사용됩니다. 오늘날 웹사이트에는 수십 개의 다양한 스크립트가 있으며, 써드파티 스크립트는 전체 스크립트의 2/3를 차지합니다.
- 클라이언트 측 스크립트는 여러 이해관계자가 얽힌 복잡하고 역동적인 기능 생태계입니다.
- 클라이언트 측 보안에 대한 기본적인 모범 사례가 있습니다. 그러나 클라이언트 측 보안은 복잡하고 여러 도전과제가 있기 때문에 이런 보안 위협 기법을 방어할 수 있는 기업 보안 솔루션에 대한 수요는 높아질 것입니다.

권장 사항

- 시장에서 구매 가능한 솔루션의 기능은 매우 큰 차이를 보입니다. 구매자의 핵심 목표는 문제가 발생하지 않도록 보안과 비즈니스 요구사항 사이의 균형을 맞추는 것입니다.
- 많은 벤더사가 클라이언트 측 가시성과 제어에 대해 잘 알지 못합니다. 새롭게 시장에 진입하는 벤더사는 자체 솔루션을 구축할지 또는 기존 벤더사를 인수하거나 파트너십을 맺을지 신중하게 고민할 것입니다.
- 수많은 IT 기업이 클라이언트 측 스크립트나 환경에 대한 인사이트가 부족합니다. 관련 보안 문제를 이해하는 기업은 더 적습니다. 데모, 연구, 개념 증명(PoC), 체험판 등 시장의 인식을 제고할 수 있는 방법이 필요합니다.

출처: IDC, 2021

April 2021, IDC #US47623221

신규 시장 개발과 역학

이 IDC 시장 보고서는 위협 기법, 새로운 솔루션, 클라이언트측 웹 애플리케이션 방화벽(WAF) 시장의 미래를 분석합니다.

Akamai, Cymatic, PerimeterX, Tala Security 는 클라이언트 측 위협에 대처하기 위해 WAF 보안을 확장함으로써 새로운 길을 열고 있습니다. 클라이언트 측 스크립트는 새롭게 부상하는 위협 기법이며, 보안 시장은 이에 대처하기 위해 발전하고 있습니다.

이러한 보안 솔루션은 일반적으로 "클라이언트 측 WAF", *안티 스크립팅* 또는 *스크립트 보안*으로 지칭되는데, 용어가 혼란스러울 수 있습니다. 다음과 같은 옵션을 고려해 보시기 바랍니다.

- WAF 는 웹 애플리케이션에 적용되는 일련의 통제 수단을 연상시킵니다. 그러나 클라이언트 측 스크립트는 애플리케이션 보안 패러다임에서 본질적으로 제어 지점이 다릅니다.
- 클라이언트 측 WAF 는 WAF 에서 잘 정립된 보안 제어와의 연관성을 의미하는 유용한 용어지만 '스크립트 보안'은 애매모호할 수 있습니다.
- 안티 스크립팅이라는 용어는 스크립트를 원하지 않고 문제가 있는, 노골적으로 악의적인 기술로 일반화합니다. 그러나 실제로 스크립트는 애플리케이션 아키텍처에서 유용하고 강력한 툴입니다.

IDC 는 전반적으로 이런 솔루션을 클라이언트 측 WAF 로 지칭하는데, 가장 큰 이유는 WAF 라는 용어가 주는 친숙함 때문입니다. 또한 클라이언트 측 WAF 라는 용어는 클라이언트 측 위협을 스크립트에만 국한하지 않습니다.

서론

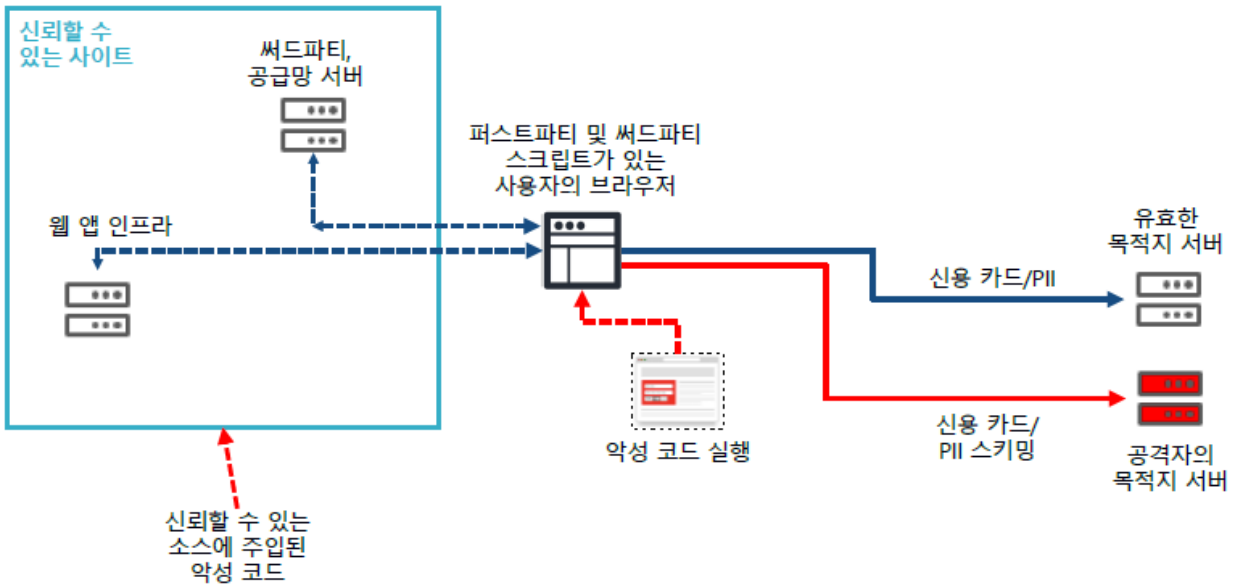
결제 카드 데이터를 스키밍(skimming)하는 새로운 기법이 2018 년에 등장했는데 Magecart 해커 그룹이 만든 것입니다. Magecart 공격은 클라이언트 브라우저에서 실행되는 스크립트를 새로운 위협 기법으로 악용했습니다. 공격 캠페인이 탐지된 후 이뤄진 조사에 따르면 Magecart 그룹은 Ticketmaster, NewEgg, British Airways 를 포함한 대형 온라인 기업의 웹사이트를 수개월 동안 감염시킨 것으로 나타났습니다.

Magecart 캠페인은 클라이언트 측 공격을 사용해 웹 스키밍(온라인 카드 스키밍 또는 폼 재킹)을 진행했습니다. 이 공격 기법에서 가장 눈에 띄는 요소는 웹 스키밍이지만 워터링 홀 공격 및 크립토재킹과 같은 다른 공격도 가능합니다. 이러한 공격의 목표는 다양할 수 있지만, 전반적으로 클라이언트 측 공격은 대규모의 장기적인 데이터 유출로 이어지는 데이터 유출 캠페인일 가능성이 있습니다.

그림 2 는 클라이언트 측 공격의 라이프사이클을 전체적으로 보여줍니다. 악성 코드는 WAF 가 제공하는 보안 범위에서 멀리 떨어진 브라우저에서 실행됩니다. 또한 타사의 소스와 당사자기업 소스에 모두 악성 코드를 주입할 수 있습니다.

그림 2

웹 스키밍 공격의 구조(브라우저)



출처: Akamai, 2021

업계 현황

클라이언트 측 WAF 는 성장 잠재력이 큰 초기 시장입니다. 이 기술은 애플리케이션 개발 방법이 변화하면서 발생하는 새로운 위협 기법에 대처합니다. 애플리케이션 기능은 최근 몇 년 동안 서버에서 클라이언트로 옮겨왔는데, 앞으로 이런 추세가 약화될 가능성은 낮습니다. 서버에서 클라이언트로 기능이 옮겨가면서 서버의 성능 요구사항이 분산되고, 따라서 사용자는 더 높은 성능과 인터랙티브한 경험을 얻을 수 있습니다. 그 결과 인터랙티브 온라인 경험을 구현하기 위한 툴로써 스크립트의 인기가 갈수록 높아지고 있습니다. 스크립트는 추적, 분석, 사용자 경험, 보안 등 합법적인 용도로 광범위하고 다양하게 사용됩니다. 게다가 스크립트는 오늘날 웹사이트에서 보편적으로 사용됩니다. 웹사이트에는 15 개 이상의 스크립트가 포함되어 있는 것으로 추정되기도 합니다.

게다가 자바스크립트의 간편함 덕분에 IT 전문가가 아닌 사람들도 스크립팅을 채택할 수 있게 되었습니다. IT 부서가 아닌 사업부서도 스크립트를 사용해 다양한 목적으로 코드를 만들어 웹 자산에 삽입할 수 있습니다. 또한 스크립트를 사용하면 타사 서비스를 더욱 쉽게 통합하고 삽입할 수 있습니다. 그러나 WAF 와 같은 핵심 툴에 집중하는 기업들은 스크립트의 보안 측면을 대부분 간과하고 있습니다.

전반적으로 이 위협에 대한 이해가 부족한 편입니다. 이 분야에서 가장 광범위하게 논의되는 위협은 주로 타사 스크립트에 관한 것입니다. Magecart 캠페인이 이와 밀접하게 관련되어 있습니다. Magecart 해커들은 공격 대상인 고객의 공급업체 파트너 코드에 접근해 신뢰받는 스크립트에 악성 코드를 주입했습니다. 이 위협 기법에 대처하기가 정말 어렵다고 느낀 기업들도 있습니다. 대규모 온라인 기업이 직면한 여러 다양한 위협에 대응해 웹사이트를 보호하는 작업만 해도 간단한 일이 아닌데, 파트너 시스템의 취약점까지 감안해야 한다면 실제로 불공평하게 보일 수 있습니다. 타사 스크립트는 IT 기업이 파트너의 코드, 업데이트, 변경 사항에 대한 가시성도 갖고 있지 않고 제어할 수도 없기 때문에 가장 큰 문제가 됩니다.

게다가 타사 스크립트는 대부분의 웹 페이지에 있는 스크립트 중 하나일 뿐이므로 웹 스키밍은 문제의 일부분에 불과합니다. 참고로 Akamai 연구원들은 스크립트의 약 67%가 타사 스크립트일 것이라 추정했습니다. 결국 대부분의 웹 페이지는 내부 이해관계자와 타사의 스크립트로 구성된 생태계입니다. 서버가 탈취되는 경우 이러한 내부 시스템은 악성 코드를 제공하는 역할도 할 수 있습니다.

리스크를 줄이는 데 도움이 될 수 있는 몇 가지 모범 사례가 있습니다. 타사 스크립트에 대한 보다 강력한 통제가 좋은 출발점입니다. 정기적인 코드 검토와 애플리케이션 테스트 역시 좋은 방법입니다. 또한 IT 기업은 하위리소스 무결성(SRI)과 같은 기술을 활용해 해시하고 스크립트의 변경을 탐지할 수 있습니다. 이러한 옵션은 보안에 반드시 필요한 기반이지만 실제 사례에서 볼 수 있듯이 치밀한 위협 행위자들은 탐지를 피하기 위해 교묘한 고급 전술을 사용합니다. 즉, SRI 및 기타 방법을 사용하는 것이 좋은 출발점은 되겠지만 지능적인 공격에 대한 효과는 제한적입니다.

또한 공격자들은 공격을 할 수 없는 상황이 될 때까지 좀처럼 공격을 멈추지 않습니다. Magecart 공격이 헤드라인을 장식한 이후 해커들은 이 공격을 여러 가지 방법으로 수정했습니다. 예를 들어, 배너 광고를 통해 악성 코드를 주입하기 위한 수단으로 광고주의 네트워크를 공격 표적으로 삼을 수 있습니다. GitHub 와 같은 코드 저장소(repository)를 공격할 수도 있습니다. 이러한 저장소는 오픈 소스 라이브러리와 코드 스니펫을 포함하는데 이 저장소가 많은 기업들의 신뢰를 받고 있고 자사 웹 애플리케이션에 재사용되기도 합니다. 결과적으로 이런 소스가 신뢰를 받고 있기 때문에 안전한 웹사이트에 악성 스크립트를 주입하기 위한 수단이 될 수 있습니다.

이 문제에 접근하는 방식은 벤더사마다 조금씩 다릅니다. 현재 시장에 나와 있는 솔루션들은 주로 자바스크립트 태그를 통해 배포되기 때문에 스크립트 실행에 앞서 보안 기능을 삽입할 수 있습니다. 여기에서 각 솔루션의 차이가 명확하게 드러납니다. 핵심 기능은 대체로 스크립트 및 통신에 대한 가시성과 매핑(소스와 타깃 등)입니다. 추가적인 기능에는 취약점 관리, 정책 실행, 악의적인 활동, 의심스러운 이벤트 탐지 등이 있습니다. 키 및 임베딩된 데이터의 암호화, 코드 난독화, 샌드박스, 기타 방어 수단 등 고급 기능도 있습니다. 현재 이 접근 방식은 핵심 보안 기능의 가시성과 자동화를 충분히 제공하는 것으로 보입니다. 시간이 지나면서 더 정교한 탐지 방법이 도입될 수도 있지만 최종 사용자 환경을 저해하거나 웹사이트 기능 '중단'을 초래하지 않으면서 충분한 보안을 제공하는 것이 앞으로의 핵심이 될 것입니다.

벤더 사례

현재 클라이언트 측 WAF 를 위한 상용 제품이 몇 가지 있으며, 그 범위와 기능은 다양합니다. Digital.ai(구 Arxan), Source Defense, Cymatic, Tala Security, ChameleonX(2019 년 Akamai 에 인수됨)를 포함해 몇몇 전문 기업들이 있습니다. 광범위한 웹 애플리케이션 보안 포트폴리오를 갖춘 기업들도 있습니다. 예를 들어 Akamai 는 포괄적인 웹 애플리케이션 및 API 보안 포트폴리오를 통해 멀티벡터 공격을 방어하기 위한 접근 방식의 일부로 2020 년 Page Integrity Manager 를 출시했습니다. 마찬가지로 PerimeterX 는 2019 년 자사의 기업 봇 관리 솔루션을 보완하는 제품을 발표했습니다. Cloudflare 는 가장 최근에 시장에 진입했는데 2021 년 3 월에 새로운 솔루션을 출시했습니다. IDC 는 이 벤더사들이 봇 관리 부문에서 경험이 있는 만큼 이것이 클라이언트 측 보안 분야에서 어느 정도 친숙도를 제공하는 데 도움이 되었을 것으로 평가합니다. 봇 관리를 제대로 하는 것은 매우 까다로운데, 우수한 봇 관리 솔루션은 봇 행동을 탐지하고 분류하기 위해 여러 가지 기법(자바스크립트 등)을 사용합니다.

클라이언트 측 공격은 탐지하기가 어려울 수 있습니다. 그러나 일단 탐지되면 영향을 받는 기업과 그 기업의 고객들이 얼마만큼의 재정적 손실을 치러야 하는지 분명히 드러납니다. 예를 들어 이런 데이터 유출이 발생하면 유출된 고객 레코드 수로 측정될 수 있습니다. 기존의 경쟁사들은 스크립트 기반 위협 탐지 및 방어 분야에서 높은 효율성을 증명했습니다. 이로 인해 공격자들은 다른 곳에 노력을 집중하게 됐고, 이것이 업계에서 일종의 두더지 잡기 게임으로 이어졌습니다. 공격자들의 목표는 보안 조치가 전혀 없거나 취약한 웹사이트를 찾는 것입니다. Magecart 공격이 분명히 발생했음에도 불구하고 위협 기법에 대한 시장의 인식은 여전히 낮기 때문에 공격자들은 새로운 공격 대상을 찾아낼 수 있었습니다. 이런 모든 요소들 때문에 이 위협 기법에 대한 전반적인 인식이 높아질 수 있고 수요가 발생하면서 앞으로 몇 년 동안 시장에 진출하는 기업은 증가할 것입니다.

시장 전략

사이버 범죄자들이 이 공격이 수익성이 있다고 생각하는 한, 클라이언트 측 위협은 대규모 온라인 기업이 대처해야 할 어려운 과제가 될 것입니다. 이는 랜섬웨어와 같이 대량 살포되는 공격보다 훨씬 더 표적화된 공격입니다. 공격의 표적이 된 기업이 스크립트 기반 공격을 탐지하고 방어하는 데는 시간이 걸립니다. 또한 이런 문제에 대한 주류 시장의 인식이 높아지려면 시간이 걸리고 노력이 필요합니다. 벤더사는 지속적인 교육, 데모, 개념 증명(PoC) 테스트를 통해 인식을 제고해야 합니다.

자체 제품과 기능을 도입하는 기업들이 증가할 가능성이 큽니다. Akamai 는 개인 식별 정보(PII)를 제출하고 접속이 이뤄지는 브라우저에 로딩된 스크립트로 인해 생성되는 공격면의 확장에 대처하기 위해 1 년 전에 Page Integrity Manager 를 출시했습니다. 또한 코로나 19 로 인해 인터넷 거래가 급증하면서 클라이언트 측 위협이 2020 년에 크게 확산되기도 했습니다.

Cloudflare 는 가장 최근에 시장에 진입한 기업으로 Cloudflare Page Shield 라는 새로운 솔루션을 발표했습니다. 이전까지 Cloudflare 는 Tala Security 와의 기술 제휴를 통해 이 위협 기법에 대처했습니다.

Cloudflare 는 자체 클라이언트 측 보안 기능을 개발하기로 결정했지만, IDC 는 다른 기업들이 이런 접근 방식을 도입하는 것은 쉽지 않다고 지적합니다. 대부분의 벤더사들은 클라이언트 측 WAF 기능을 개발하기에 앞서 자바스크립트 클라이언트를 활용하는 봇 탐지 기법을 사용했습니다. 레거시 WAF 솔루션에는 이러한 기능 또는 클라이언트 측 코드에 대한 다른 경험이 없습니다.

웹 애플리케이션 및 API 보안 제품 라인을 강화하고 있는 벤더사의 경우 전문 솔루션을 인수하는 것이 동등한 경쟁력을 확보하는 최선의 방법일 수 있습니다. Akamai 의 ChameleonX 인수는 맞춤형 기술과 클라우드 확장성을 결합해 얻을 수 있는 잠재적인 이점을 보여주는 사례입니다. Page Integrity Manager 는 매일 64 억 건의 스크립트 실행을 분석하고 매달 37 억 개 이상의 페이지 뷰를 보호합니다. 매주 약 4 천만 건의 의심스럽고 악의적인 최종 사용자 상호작용이 관측되는데 Akamai 는 이를 기반으로 실시간 알림, 근본 원인 분석, 즉각적인 방어, 자동화 정책 생성을 제공할 수 있습니다.

IDC 의 관점

사이버 범죄자들이 이 공격 기법에 수익화 기회가 있다고 보는 한 클라이언트 측 공격의 보안 간극은 더 커질 것이며 앞으로 수년간 이어질 수 있습니다. 이에 대한 중요한 이유는 클라이언트 측 위협 기법에 대한 이해도가 부족하다는 것이 큰 원인입니다. 일반적으로 WAF 솔루션은 웹 서버를 대상으로 하는 웹 애플리케이션 트래픽을 분석하여 작동합니다. 지난 몇 년 동안 자바스크립트의 인기가 높아지면서 많은 기능이 클라이언트 브라우저로 이동했습니다. 그러나 많은 기업들은 이러한 사실을 간과하거나, 웹 기능을 클라이언트 브라우저로 이동할 때 발생하는 리스크와 보안 측면의 영향에 대해 적절하게 평가하지 않았습니다.

이것이 랜섬웨어와 같이 대규모로 이루어지는 공격보다 훨씬 더 표적화된 공격이라는 사실은 시장 혼란을 가중시키는 원인이 되고 있습니다. 예를 들어 대부분의 기업은 WAF 및 DDoS 방어 솔루션으로 어떤 공격에 대처할 수 있는지 잘 알고 있습니다. 원치 않는 봇이나 악성 봇으로 인해 발생하는 보안 리스크는 주류 인지도를 얻고 있는 또 다른 사례입니다. 그러나 API 보안 및 클라이언트 측 보안과 같은 비교적 새로운 영역은 마치 물속에 잠긴 빙산의 나머지 부분과 같이 눈에 보이지 않는 심각하고 새로운 리스크 영역입니다(그림 3 참조).

그림 3

웹 애플리케이션 및 API 보안

출처: IDC, 2021

기업이 잠재적인 공격 기법을 이해한 뒤에도 여러 도메인, 웹 페이지, 웹 애플리케이션으로 구성된 복잡한 IT 환경에서 실행되는 스크립트를 분류하고 이해하는 프로세스는 매우 어려운 작업이 될 수 있습니다. Magecart 공격이 발생했을 때, 주입된 악성 스크립트를 탐지하기 위해 변경사항을 확인해야 했는데 코드를 한 줄씩 수동으로 검토하는 프로세스가 사용됐습니다. 연구원들이 근본적인 문제와 모범 사례를 알게 되면서 지금은 이 프로세스가 보다 간소화되었습니다. 그러나 공격 표적이 된 대부분의 기업에서 스크립트 기반 공격을 탐지하고 방어하는 데 시간이 걸린다는 사실에는 변함이 없습니다. 위협 기법을 이해하는 데 시간이 걸리고, 기존 보안 간극이나 악용을 탐지하는 데 추가적인 시간이 소요되기 때문입니다. 또한 스크립트의 75%는 분기마다 변경되기 때문에 위협 기법은 움직이는 표적과 같습니다. 새로운 변경 사항이 있을 때마다 새로운 취약점과 악성 코드가 발생될 가능성이 있기 때문입니다.

그러나 시간이 절대적으로 중요합니다. 클라이언트 측 공격으로 인한 보안 침해는 장기간 계속되었고 공격자들에게 몇 개월 앞서 나갈 수 있는 기회를 제공했습니다. 그 사이 수많은 신용 카드와 기타 PII 가 유출됐습니다. 공격이 탐지되면 공격자는 해당 공격을 중단하고 다음 희생자를 찾아 새로운 공격을 시작하게 됩니다. 기본적으로 클라이언트 측 공격은 탐지하는 데 상당한 시간이 걸리는데 이런 불균형은 사이버 범죄자에게 큰 이점이 되므로 반드시 시간을 줄여야 합니다.

따라서 보안 업계가 이 문제에 대해 교육하고 구매자 인식을 개선하는 데 있어 가장 큰 장애물은 시간입니다. 벤더사는 지속적인 교육, 데모, 개념 증명(PoC) 테스트를 통해 인식을 제고해야 합니다. 예를 들어 Akamai 는 Page Integrity Manager 제품을 무료로 체험할 수 있는 기회를 제공합니다. 이 솔루션은 웹 페이지의 스크립트 생태계에 대해 전반적인 정보와 함께 다양한 스크립트, 취약점, 리스크 요인에 대한 분석을 제공합니다. 다른 벤더사들도 평가판과 데모, 교육 리소스를 제공합니다.

IDC 는 이러한 접근 방식을 높이 평가합니다. 상황의 시급성이나 보안 솔루션의 가치 및 효과를 가장 잘 전달하는 것은 개념 증명(PoC)입니다. 프리미엄 구독으로 전환하면 벤더사에게 확실한 이점을 가져다 줄 수 있습니다. 구매자 역시 전통적으로 대부분의 기업에서 완전히 사각지대에 존재했던 위협 기법에 대한 가시성을 확보한다는 큰 이점을 얻을 수 있습니다.

IDC 는 앞으로 클라이언트 측 WAF 시장을 모니터링하면서 이것이 WAF, DDoS 방어, 봇 관리, 온라인 사기 방지와 같은 기존 시장에 미치는 영향을 파악할 예정입니다. 클라이언트 측 보안 사각지대가 해소된 후에는 보안 통제 지점으로서 클라이언트 측의 잠재적 가시성 및 실행 기능이 미치는 영향에 대한 보다 심층적인 논의가 필요할 것입니다.

자세히 보기

관련 연구

- IDC FutureScape: Worldwide Future of Trust 2021 Predictions (IDC #US46912920, 2020 년 10 월)
- Pervasive Application Edge Defense: An Application-Based Framework for Trust (IDC #US46810219, 2020 년 9 월)
- IDC Market Glance: Software-Defined Secure Access, 2Q20 (IDC #US46291520, 2020 년 5 월)
- Worldwide Internet Defense Forecast, 2020-2023: Infrastructure and Application Security Drive Business Value (IDC #US46022619, 2020 년 2 월)
- Security Convergence at the Edge: Emerging Pervasive Data Defense and Response Platforms (IDC #US46075520, 2020 년 2 월)

시놉시스

본 IDC 시장 보고서는 위협 기법, 새로운 솔루션, 클라이언트 측 WAF 시장의 미래에 대한 분석을 제공합니다. 웹 환경에서 실행되는 클라이언트 측 스크립트를 표적으로 삼는 위협을 완벽하게 이해하는 IT 기업은 거의 없습니다. 사이버 범죄자들은 잡히지 않고 막대한 금전적 이득을 얻기 위해 은밀하게 악성 코드를 실행하는 수단으로 클라이언트 측 스크립트를 공격해 왔습니다. 이 위협 기법이 향후 몇 년 동안 더욱 두드러지게 나타나면서 엔터프라이즈 클라이언트 측 WAF 솔루션에 대한 수요도 꾸준히 증가할 전망입니다.

IDC 네트워크 보안 제품 및 전략 연구 매니저인 크리스토퍼 로드리게스(Christopher Rodriguez)는 "클라이언트 측 스크립트는 보안의 다음 전선입니다. 사이버 범죄자들은 수익성 높은 공격을 끊임없이 추구하고 있으며 기업 디지털 보안 스택에서 새로운 틈을 발견했습니다."라고 말합니다.

IDC 소개

IDC(International Data Corporation)는 정보 기술, 통신, 소비자 기술 시장에 대한 마켓 인텔리전스, 자문 서비스, 이벤트를 제공하는 유수의 글로벌 기업입니다. IDC 는 IT 전문가, 기업 임원, 투자 커뮤니티가 기술을 구매하고 비즈니스 전략을 수립할 때 사실에 기반한 결정을 내릴 수 있도록 지원합니다. 1100 여 명의 IDC 애널리스트들이 전 세계 110 여 개국에서 기술 및 산업 기회와 트렌드에 대한 글로벌, 지역별, 현지 전문 지식을 제공합니다. IDC 는 지난 50 년 동안 고객이 주요 비즈니스 목표를 달성할 수 있도록 전략적 인사이트를 제공해 왔습니다. IDC 는 세계 최고의 기술 미디어, 연구, 이벤트 기업인 IDG 의 자회사입니다.

글로벌 본사

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com