디도스 방어 서비스 제공업체 평가 방법:

4가지 주요 기준

Akamai
FASTER FORWARD

목차

소개 3
기준 #1: 위협 인텔리전스 3
기준 #2: 실무 경험 4
기준 #3: 방어 능력 4
기준 #4: 방어 용량 6
결론 8

소개

디도스(DDoS, 분산 서비스 거부 공격) 공격 규모가 커지고 새로운 공격 기법이 등장하면서 디도스 공격에 관한 기사가 전 세계 뉴스 헤드라인을 장식하고 있습니다. 디도스 공격의 위협 양상이 끊임없이 역동적으로 변화함에 따라, 디도스 방어 서비스에 대한 수요 역시 증가하고 있으며 많은 서비스 제공업체들이 시장에 진입하고 있습니다. 하지만, 디도스 방어 서비스는 대부분 클라우드 기반이기 때문에 기업 입장에서는 디도스 방어 서비스 제공업체를 평가, 분석하고 구분하는 데 어려움을 겪고 있습니다.

디도스 방어 서비스 제공업체가 대규모의 정교한 인터넷 공격을 확실하게 방어할 역량을 갖추었는지 어떻게 판단할 수 있을까요? 이 백서에서는 디도스 방어 서비스 업체와 계약하기 전에 해당 업체를 평가하는 4가지 기준에 대해 알아보도록 하겠습니다. 아카마이는 고객사가 서비스 제공업체의 위협 인텔리전스, 경험, 방어 능력을 평가할 수 있도록 각 기준과 관련된 주요 문항을 마련했습니다. 당사의 지침은 여러 디도스 공격 시나리오에 따른 검증된 방어 방식과 실제 경험은 물론, 사이버 범죄자와 디도스 공격자의 심리 및 전략에 대한 날카로운 통찰력을 바탕으로 작성되었습니다.

기준 #1: 위협 인텔리전스

디도스 공격에 대해 더 많이 알고 서비스 제공업체가 어떻게 디도스 공격을 방어하는지 더 잘 이해할수록 디도스 방어 전략을 선제적으로 관리할 수 있습니다. 따라서 최근의 공격 추세, 새로운 툴킷 개발, 최신 사이버 위협에 대해 철저한 이해가 중요합니다. 방어 서비스 제공업체는 디도스 보안 전문가로 구성된 전문 연구팀을 만들고 종합적인 위협 인텔리전스를 정기적으로 제공해야 합니다.

확인해야 할 사항:

디도스 위협 인텔리전스를 담당하는 사내 연구팀을 운영하고 있습니까?

역량 있는 디도스 방어 서비스 제공업체는 디도스 전문 엔지니어로 구성된 사내 연구팀을 두고 있으며 이 연구팀은 공격 벡터와 툴킷의 변화 양상을 추적합니다. 또한, 이 연구팀은 새로운 방어 전략과 공격 대응 수단을 정기적으로 사전 개발하는 과정에서 핵심적인 역할을 담당하고 있습니다. 위협 인텔리전스 팀은 고객사 및 일반 대중에게 이런 인텔리전스를 정기적으로 공개해야 하고 이는 해당 서비스 제공업체의 역량을 가늠하는 좋은 기준이 됩니다. 역량이 미흡한 업체들은 타사가 제공하는 정보와 기존 방어 장치에 의존해야 하기 때문에 변화하는 공격 기법에 대응하기 위해선 소프트웨어를 업데이트해야만 합니다. 디도스 전문가와 기술자들이 위협에 대응하기 위해 개발한 툴을 사용해 공격을 방어하면서 축적된 현장에서의 실무 경험 및 정보와 비교해보면 역량이 미흡한 업체들의 위협 인텔리전스는 그 수준이 크게 떨어질 수밖에 없습니다.

고객에게 어떤 위협 인텔리전스를 게시 및 제공합니까?

서비스 제공업체가 고객에게 제공하는 위협 정보를 확인하십시오. 보고서에는 최신 디도스 툴킷, 새로운 공격 벡터, 혁신적인 공격 방어 기법에 관한 내용이 정기적으로 수록되어야 합니다. 업체가 제공하는 보고서를 살펴보면 해당 업체가 최신 공격 벡터와 툴킷을 방어하기 위해 인프라와 연구에 얼마나 투자하고 있는지를 확인할 수 있습니다. 위협 인텔리전스의 품질을 바탕으로 해당 업체의 서비스 품질을 판단할 수 있고 또한 해당 업체가 고객사의 네트워크 자산을 보호할 역량을 갖추고 있는지 확인할 수 있습니다. 타사 정보에만 의지하는 업체는 새로운 공격 벡터에 대응할 수 있는 역량이 미흡할 수밖에 없습니다.

기준 #2: 실무 경험

강력한 사이버 핵티비스트 단체를 이기기 위해 현장 실무 경험만큼 중요한 건 없습니다. 공격자들은 서비스 제공업체의 방어 능력에 도전장을 던질 뿐만 아니라, 서비스 업체가 가장 악의적인 형태의 사이버 공격을 막아낼 수 있는지 확인합니다. 노련한 디도스 방어 서비스 제공업체는 성공적으로 공격을 방어한 경험을 바탕으로 자사 네트워크를 개선시킴으로써 제로데이 유형의 디도스 이벤트나 예상치 못한 공격에 대한 대응 여력을 크게 향상시킬 수 있습니다. 디도스 방어 서비스 제공업체는 고객을 보호하기 위해 존재하고 고객은 제공업체가 디도스 공격을 막아줄 것이라 기대하고 있기 때문에, 서비스 제공업체는 모든 종류의 사이버 공격을 방어할 수 있는 역량을 갖추고 있어야 합니다.

확인해야 할 사항:

일반 고객에게 디도스 방어 서비스를 얼마나 오랫동안 제공해 왔습니까?

사내 네트워크를 디도스 공격으로부터 보호한 경험을 서비스 경력에 포함시키려는 업체가 많습니다. 하지만, 타사 네트워크 보호는 자사 네트워크 보호와 완전히 다른 일입니다. 경험이 많을수록 실력이 쌓인다는 말처럼 서비스 제공업체가 대응해본 공격이 많을수록 더욱 효율적이고 복원력이 뛰어난 네트워크와 공격 대응 수단을 갖출 수 있습니다. 수년간 실제 공격자를 직접 대응하면서 축적된 실무 경험이 있어야만 디도스 공격을 제어할 수 있는 전문성을 키울 수 있습니다.

네트워크를 증설하고 방어역량을 키우는데 소요되는 비용을 충당할 만큼 충분한 고객 기반이 있습니까?

서비스 제공업체의 고객 기반을 들여다보면 해당 업체의 역량을 파악하는 데 필요한 정보를 얻을 수 있습니다. 포춘(Fortune)지가 선정한 500대 기업 같은 탄탄한 고객 기반을 갖춘 업체의 경우 충분한 매출과 수익이 발생하기 때문에 대용량 트래픽을 처리할 수 있습니다. 또한, 새로운 공격 유형에 대응할 수 있는 기법과 역량에 지속적으로 투자할 수 있는 자본력을 보유하고 있습니다. 서비스 업체가 수익을 내고 있습니까? 고객 기반이 취약하거나 수익을 충분히 내지 못하는 중소 서비스 업체는 모든 유형, 모든 규모의 공격으로부터 고객을 보호하는 데 필요한 대역폭 용량과 역량에 재투자할 여력이 부족할 수 있습니다.

기준 #3: 방어 능력

모든 기업은 그 규모에 상관없이 기존의 공격 벡터, 새로운 공격 벡터뿐만 아니라 최대 규모의 사이버 공격으로부터 기업을 보호할 수 있는 탄탄한 역량을 갖춘 디도스 방어 서비스 제공업체가 필요합니다. 기업 규모가 작기 때문에 대기업 수준의 방어 시스템이 필요하지 않다고 생각하면 오산입니다. 디도스 공격자는 세계 최대 은행을 공격하는 데 사용하는 상당히 정교한 툴킷을 소도시의 소규모 신용 조합을 공격할 때도 동일하게 사용합니다.

또한, 기업마다 필요한 디도스 방어 수단은 모두 상이합니다. 네트워크 환경의 아키텍처에 따라, 취약한 자산을 보호하기 위해서는 여러 가지 기술과 도구가 필요합니다. 따라서, 다양한 포트폴리오를 갖춘 우수한 디도스 방어서비스 제공업체를 선택해야만 고객의 네트워크를 보호하는 데 가장 적합한 기술과 방법을 통해 향후 변화하는 보안 수요에 적절하게 대응할 수 있습니다.

확인해야 할 사항:

지원 가능한 트래픽 리디렉션 방식은 무엇입니까?

클라우드 기반의 우수한 디도스 방어 서비스는 공격 발생 시 트래픽을 리디렉션하는데 필요한 두 가지 주요 기능을 모두 제공합니다. 첫 번째는 BGP(Border Gateway Protocol) 경로 전파 변경에 기반한 기능인데, 인터넷상의 모든 라우터가 경로 정보를 교환하는 방식입니다. 이러한 IP 경로 기반의 리디렉션은 모든 포트와 프로토콜을 아우르나, 인터넷에서 가능한 최소한의 경로 전파인 최소 /24대역이 필요합니다. 이를 대체하는 방법으로는 DNS 기반의 리디렉션이 있는데, 보통 BGP에 필요한 최소 대역인 /24를 갖추지 못한 고객이 선택합니다. DNS 리디렉션은 개별 IP 주소를 보호할 수 있고 일반적으로 7레이어(애플리케이션 레이어) 공격을 한층 견고하게 방어할 수 있습니다. 고객의 네트워크 환경에 따라 데이터 센터와 타사의 클라우드 자산 모두를 디도스 공격으로부터 보호해야 하는 하이브리드 아키텍처가 필요한 경우도 있습니다. 디도스 방어 서비스 업체는 반드시 이 두 가지를 모두 보호할 수 있는 검증된 역량을 보유하고 있어야 합니다.

온디맨드(주문형)와 상시 가동 디도스 서비스 옵션을 모두 제공합니까?

서비스 제공업체를 선택할 때, 기업의 다양한 요구사항에 따라 온디맨드와 상시가동 디도스 방어 서비스를 모두 제공하는지 확인해야 합니다. 기존의 디도스 방어 서비스는 온디맨드 형태로 판매되어 왔습니다. 즉, 평소에는 대기 상태였다가 고객의 네트워크가 공격을 당하는 경우에만 방어서비스 제공업체의 클라우드 혹은 네트워크로 트래픽을 라우팅하는 방식입니다. 하지만 디도스 위협의 양상이 복잡해지고 다양해지면서 고객들은 이제 서비스 제공업체가 모든 네트워크 트래픽을 상시 감시하는 서비스를 원하고 있습니다. 상시 가동 방식을 이용하면, 공격을 신속하게 방어할 수 있고 일부 환경에서 성능을 개선시키는 등 몇 가지 장점이 있습니다. 네트워크 자산, 비즈니스의 특성, 다운타임에 대한 허용치 등의 요소를 고려해 온디맨드 서비스와 상시 가동 서비스를 적절하게 결합하는 경우도 있습니다. 다만 상시가동 서비스를 고려할 경우에는 트래픽 성능, 오탐(정상적인 트래픽을 공격으로 오인함) 리스크 등에 대한 확인이 반드시 필요합니다.

타사의 호스팅 환경에 있는 DNS 서버도 보호할 수 있습니까?

대부분의 디도스 방어 서비스는 고객의 데이터 센터에서 호스팅되는 DNS 서버를 보호할 수 있습니다. 하지만 대부분의 서비스 제공업체는 타사 환경에서 호스팅되는 DNS 서버에 대한 대규모 정교한 디도스 공격에 대처할 준비가 되어 있지 않습니다. 타사 호스팅 환경을 이용하면, 다수의 고객이 동일한 DNS 서버 환경에 있기 때문에 리스크 역시 공유될 수 있다는 점에 유의해야 합니다. 다시 말해, 한 고객사가 공격을 받으면 호스팅 업체의 가동이 중단되고 이로 인해 공격대상이 아니었던 회사까지 악영향을 받을 수 있습니다. 여러 고객을 동시에 수용하는 환경에서는 디도스 공격의 위험이 크게 높아지기 때문에 DNS 호스팅 제공업체의 디도스 방어 능력을 반드시 정확하게 이해해야 합니다. 현재 자사가 디도스 공격 대상이 될 가능성이 낮다 하더라도 동일한 호스팅 환경을 공유하는 다른 기업이 상당히 위험한 상황에 노출되어 있을 수도 있습니다.

공격 방어 시간에 대한 SLA(Service Level Agreement, 서비스 수준 협약)가 가능합니까?

그렇습니다. 당연히 가능해야 합니다. 공격 방어 시간에 관한 SLA는 서비스 제공업체가 디도스 공격을 얼마나 신속하게, 효과적으로 방어할 것인지 정의합니다. 다른 SLA는 고객이 공격 발생에 대해 신고한 후 얼마나 신속하게 대응하고 전화를 할 것인지, 서비스 라우팅에 소요되는 시간 등의 부차적인 내용만 다루고, 얼마나 신속하게 공격을 방어할 수 있는지와 같은 원론적인 내용은 다루지 않습니다. 디도스 공격을 방어할 때 속도는 매우 중요합니다. 대응 속도가 느려지면 다운타임이 길어지고 매출 손실이 발생하며 브랜드 이미지가 손상될 수 있기 때문입니다.

디도스 외에 클라우드 보안 서비스를 제공합니까?

클라우드 보안 서비스 제공업체가 디도스 외에 다른 보안 서비스를 제공합니까? 아니면 디도스 방어 서비스만 제공합니까? 이 질문을 꼭 해야 하는 이유는, 클라우드로 이동하고 있는 기업의 자산이 점점 증가하면서 디도스 이외에 다른 보안 기능에 대한 필요성 역시 커졌기 때문입니다. 덧붙여, 피싱, 데이터 유출, 웹 애플리케이션 공격 등 사이버 위협이 증가하면서 종합적인 클라우드 보안 서비스에 대한 수요 역시 커지고 있습니다. 그 이유는 무엇일까요? 여러 가지 보안 문제가 동시다발적으로 발생했을 때 인터넷상에서 다수의 클라우드 보안업체로 트래픽을 리디렉션하는 것은 상당히 복잡한 일이 될 수 있습니다. 따라서, 종합적인 클라우드 보안 서비스 포트폴리오를 갖춘 단일 업체를 선정하면 웹 보안 프로세스를 간소화하고 비용 효율성을 높일 수 있습니다.

어떤 종류의 공격을 성공적으로 방어했습니까?

서비스 제공업체에서 방어할 수 있다고 제시한 공격 유형 목록에 만족하지 마십시오. 해당 업체가 성공적으로 방어한 공격 규모, 유형, 벡터 등의 내용이 기재된 문서(정기간행물)를 요구해야 합니다. 서비스 제공업체는 고객을 대신해 실제로 대응했던 디도스 공격에 관한 분기별 통계자료를 투명하게 게시하고 공유해야 합니다. 만약 해당 업체가 이런 데이터를 공유하고 있지 않다면 그 업체의 디도스 방어 능력과 실무 경험을 판단하기가 매우 어렵습니다.

완벽한 관리형 디도스 서비스를 제공합니까? 어떤 방식으로 방어 전략을 추진합니까?

최근에는 기본적인 방어 기능과 더불어 플랫폼에 대한 셀프 디렉팅 액세스를 제공하는 하이브리드 디도스 방어서비스 제공업체들도 등장했습니다. 그러나 이런 접근방식은 상당히 위험합니다. 디도스는 고도의 전문 영역이기 때문에 트래픽 분석 능력이 있고 디도스 공격 발생 시 고객사 전담 인력을 제공하는 업체를 선정해야 합니다. 또한 서비스 제공업체는 방어 전략을 수립하고, 이벤트 과정에서 고객과 긴밀한 의사소통을 진행하고, 과도한 방어 조치가 취해지진 않았는지 확인해야 하며, 신속하게 방어 시그니처를 개선하고 정교하게 튜닝할 수 있어야 합니다. 우수한 디도스 방어 서비스 제공업체는 업무에 적극적이고 고객사의 사고 대응 계획과 원활하게 통합될 수 있도록 커뮤니케이션 과정을 매끄럽게 진행합니다. 또한 새로운 제로데이 디도스 공격에 대응하고 방어할 역량을 충분히 갖추고 있습니다.

각각의 네트워크와 방어 플랫폼에 어떤 종류의 이중화가 제공되나요?

가장 포괄적인 디도스 방어 서비스를 제공하는 업체는 다수의 네트워크 서비스 플랫폼(BGP, 프록시, DNS)을 사용해 디도스 위협과 관련되어 있는 모든 리스크에 대응합니다 각 플랫폼의 이중화 및 복원력에 대해 질문하십시오. 각각의 플랫폼은 상이하고, 모두 안정적이어야 하기 때문입니다. BGP의 경우 데이터 센터 이중화에 대해 먼저 질문하고 만약 데이터 센터가 유지 관리 목적이나 공격으로 인해 오프라인 상태가 됐을 때 네트워크 트래픽에 어떤 영향을 미치는지 질문하십시오. 프록시 서비스와 관련해서는 업체가 보유하고 있는 물리적 서버 대수와 서버 분산 방식에 대해 알아야 합니다. 서버 한 대가 고장 난 경우, 어떻게 트래픽을 다른 서버로 리디렉션합니까? DNS 서버가 공격을 받으면 어떤 백업이 이뤄집니까? 만약 서비스 제공업체에서 DNS 가동 시간에 대한 SLA를 제공할 경우 DNS 이중화에 대해 반드시 질문해야 합니다.

기준 #4: 방어 용량

방어 능력은 디도스 방어 서비스 제공업체를 구분짓는 핵심 요소입니다. 디도스 공격의 목표는 트래픽을 처리하는 모든 기기의 대역폭, 메모리, CPU 등을 고갈시켜 네트워크 및 시스템 다운을 유발하고 기업의 온라인 활동이나 애플리케이션을 중단시키는 것입니다. 역량 있는 디도스 방어 서비스 제공업체는 대규모 디도스 공격을 방어하는데 필요한 대역폭을 구매하기 위해 가장 큰 비용을 지출합니다. 네트워크 규모, 방어 능력 그리고 방어 서비스 비용 사이에는 직접적인 관련이 있습니다. 쉽게 말해, 리소스에 대한 액세스를 많이 제공할수록 서비스 비용은 높아집니다. 하지만, 수백 기가비트의 대역폭과 수백만 달러의 방어 장치를 구매하는데 드는 비용, 디도스 공격으로 인한 매출 하락과 이미지 손상 등을 고려하면, 양질의 방어 서비스를 구매하는 데 소요되는 비용은 합리적이라 할 수 있습니다.

확인해야 할 사항:

각 보호 플랫폼에 어떤 네트워크를 사용하고 있고, 방어 능력은 어느 정도입니까?

서비스 제공업체의 네트워크와 방어 능력을 초과하는 대규모 공격이 발생하면 해당 업체의 모든 디도스 방어 능력은 무용지물이 되고 맙니다. 역량 있는 디도스 방어 서비스 제공업체는 공격 벡터별로 다양한 방어 플랫폼을 보유하고 있습니다. 따라서, 각 플랫폼의 용량 혹은 대역폭을 확인해야 하고 또한 네트워크를 보호하는 방어 플랫폼의 용량이 지금까지 발생한 최대 규모의 인터넷 공격보다 더 큰지 확인해야 합니다. 또한, 새로운 디도스 공격이 생겨나고 공격 규모와 파괴력도 커지고 있기 때문에 이런 디도스 공격보다 한발 앞서 나갈 수 있도록 방어 능력에 지속적으로 투자하고 있는지 확인하십시오.

공격 규모 혹은 공격 횟수에 따라 정해진 수수료가 있습니까?

시장에는 수많은 가격책정 모델이 있는데 정해진 규모나 횟수를 초과하는 디도스 공격에 대해 추가 수수료를 부과하는 서비스 업체들도 있습니다. 하지만, 고객은 자사 네트워크에 가해질 공격의 규모와 횟수를 통제할 수 없습니다. 또한 공격자들은 글로벌 대기업과 중소기업을 공격할 때 모두 동일한 공격 방식과 툴킷을 사용하고 있습니다. 공격자들은 손상된 기기로부터 리소스를 훔치기 때문에 1 GB, 20 GB, 100 GB 등 공격 규모에 상관없이 공격자들 입장에서는 어떤 비용도 지불할 필요가 없습니다. 공격자들이 마음대로 결정한 공격 규모나 횟수에 따라 서비스 수수료를 지불할 의향이 있습니까? 서비스 제공업체를 비교할 때 고정 수수료나 공격 한도가 있는지 면밀하게 살펴보십시오.

네트워크와 방어 능력이 전 세계적으로 어떻게 분산되어 있나요? 해당 서비스가 애니캐스트(Anycast) 혹은 이와 유사한 기술을 이용해 공격 트래픽을 여러 지역으로 분산시킵니까?

디도스 공격을 분할시켜 여러 지역에서 처리하는 방법은 이미 검증된 성공적인 방어 방법입니다. 애니캐스트 혹은 이와 유사한 기술을 사용하는 서비스 제공업체는 여러 곳의 데이터 센터를 동시다발적으로 활용하고 공격 트래픽이 시작된 지점과 가까운 곳에서 공격에 대응할 수 있습니다. 다시 말해, 방어 역량을 전 세계적으로 분할시키는 것입니다. 이 방법을 사용하면 공격 규모가 과다하게 커져 통신사가 악의적인 공격 트래픽과 정상적인 트래픽 모두를 포기하는 사태를 방지할 수 있습니다. 따라서 공격을 세분화하면 거대한 규모의 공격에도 대응할 수 있습니다. 또한, 전 세계적으로 분산된 방어 네트워크는 이중화 효과도 있습니다.

디도스 공격으로 인해 네트워크가 다운된 적이 있습니까?

서비스 제공업체가 이를 밝히지 않은 경우 간단한 인터넷 검색을 통해 이 질문에 대한 답을 찾을 수 있습니다. 언론에 보도되었던 사건이나 네트워크 다운 내역이 있는지 확인하십시오. 서비스 제공업체가 자사 네트워크조차 온라인으로 유지할 용량과 처리능력을 갖추지 못했다면 방어 플랫폼의 대역폭 혹은 설계 관련 문제가 분명히 문제가 존재한다는 뜻입니다. 최악의 상황은 부실한 디도스 방어서비스 제공업체를 선택하는 바람에 서비스 요금은 요금대로 지불하면서 디도스 공격 발생으로 다운타임을 계속 겪는 것입니다.

각각의 방어 플랫폼에서 성공적으로 방어한 최대 규모의 공격은 무엇입니까?

이 질문을 통해 디도스 방어서비스 제공업체의 실질적인 역량을 판단할 수 있습니다. 마케팅 숫자는 얼마든지 조작이 가능하기 때문에, 각 방어 플랫폼(BGP, 프록시, DNS)에서 성공적으로 방어한 최대 규모의 디도스 공격 그래프를 요청하십시오. 최대 규모의 공격 그래프가 없다는 것은 해당 업체가 그 공격에 제대로 대응하지 못했다는 뜻입니다. 이 경우, 해당 업체는 통신사의 ACL을 사용한 업스트림 공격 차단에 의존했을 가능성이 큽니다. 이러한 접근법은 어느 정도 효과가 있지만, 완화 업체가 고대역폭 공격을 차단할 능력을 갖추고 있지 않다는 의미이므로 적색 경보나 마찬가지입니다. 완화 업체에서는 규모와 유형에 관계없이 어떠한 공격도 저지할 능력을 갖추고 있어야 합니다.

동시다발적으로 일어난 공격을 방어하느라 서비스 거부가 발생한 적이 있습니까?

이 질문에 대한 답은 언제나 "아니요"여야 합니다. 시장에 진입하는 디도스 방어서비스 제공업체가 늘어나면서 이 질문은 매우 중요해졌습니다. 업체의 성장 전략은 무엇이며 용량 계획에 어떤 접근 방식을 취하고 있습니까? 고객 기반의 성장에 맞춰 새 대역폭을 충분히 프로비저닝하고 추가하고 있습니까? 또한, 대규모 공격을 동시에 몇 개까지 처리할 수 있습니까? 여러 공격이 동시다발적으로 발생했을 때, 방어의 우선순위는 어떤 기준으로 정하며 이를 어떻게 관리합니까? 이 질문은 통해, 고객은 서비스 제공업체가 현재 방어하고 있는 디도스 공격의 수에 상관없이 자사 네트워크가 완벽히 보호되고 있다는 확신을 얻을 수 있습니다.

결론

디도스 방어에 대한 전문성을 갖춘 보안 서비스 제공업체를 선택하는 일은 가장 중요한 비즈니스 의사 결정 중 하나입니다. 의사 결정이 제대로 이루어지지 않을 경우 상당한 경제적 손실이 발생하며 기업 평판 역시 상당한 타격을 받게 됩니다. 온라인 기업이 디도스 공격을 제대로 방어하지 못하면 수백만 달러의 매출 손실은 물론 고객의 신뢰와 믿음까지 잃어버릴 수 있습니다. 또한 사이버 공격 혹은 데이터 유출에 관한 뉴스가 헤드라인을 장식할 경우 투자자의 신뢰까지 잃게 됩니다.

디도스 공격자는 마치 놀이터의 불량배처럼 매우 공격적이고 교묘하며, 상대의 약점을 파고들어 우위를 점합니다. 안타깝지만 사이버 공격은 빈번히 발생하는 현실이 되었고 온라인 기업은 이에 대응해야만 하는 상황입니다. 최신 사이버 보안 기술과 우수한 IT 인력을 보유한 기업을 대상으로 공격자들은 압도적인 수의 봇넷과 크라우드 소싱을 이용해 무한정 계속되는 공격 캠페인을 시작하고 매일 시그니처를 변경할 수 있습니다. 다행히 이런 위협에 홀로 맞서 싸우지 않아도 됩니다. 풍부한 정보를 바탕으로 제대로 된 디도스 방어서비스 제공업체를 선택한다면 최전선에서 귀사를 방어하는 든든한 아군을 얻을 수 있습니다.