하이브리드 데이터 센터에 필수적인 NGFW 기능소개

종합 요약

현대적 데이터 센터가 발전하면서 애플리케이션과 데이터가 하이브리드 인프라에 점점 분산되고 있습니다. 업무에 중요한 워크플로는 민첩성이 높아지겠지만, 그와 동시에 기업의 공격면이 늘어나 가시성과 제어 능력이 떨어집니다. 네트워크 엔지니어링 및 운영 관리자는 하이브리드 IT 데이터 센터 환경을 보호하도록 설계된 지능적 기능을 탑재한 통합 보안이 필요합니다.

특히, 이들에게는 차세대 방화벽(NGFW)이 필요합니다. 여기에는 중요한 위험 관리 기능, 기업 곳곳으로 데이터 센터 보호를 넓히는 확장성, 비즈니스 연속성을 보장하는 회복 탄력성, 직원의 부담을 낮추고 대응 시간을 단축하는 자동화와 오케스트레이션이 포함됩니다.

회사에서 가동 중단이 발생했을 시 2년간 발생하는 평균 총비용은 신뢰도와 평판 훼손을 포함해 약 700억 원에 달합니다.[1]

분산된 데이터 센터로 인한 공격면의 증가

요즘 비즈니스 사용자는 하이브리드 IT 인프라 전체로 분산되는 데이터 센터에서 중요한 애플리케이션에 액세스합니다. 이들의 워크플로와 데이터는 온프레미스, 코로케이션, 프라이빗/퍼블릭 클라우드에 존재하고, 이렇게 취약한 콘텐츠가 여기저기 흩어져 있기 때문에 기업의 공격면은 끊임없이 확장됩니다.

많은 네트워크 엔지니어링 및 운영 관리자가 이렇게 위험 노출이 상승하는 것에 대응해서 개별적 포인트 보안 솔루션을 더하는 방법으로 새로운 보안 공백을 가리고, 변화하는 규제 요구 사항에 준수하려고 합니다. 안타깝게도 이런 산발적인 전략으로는 현재와 미래에 나타나는 모든 취약성을 해결할 수 없습니다. 악성 사이버 활동 또는 자연재해로 인해 업무에 지장이 발생할 가능성이 커졌고, 기업 보안의 총소유비용(TCO)과 운영 복잡성도 같이 높아졌습니다.

하이브리드 IT 환경 보안

네트워크 엔지니어링 및 운영 관리자가 팽창하는 데이터 센터 공격면 문제를 해결하려면 먼저 하이브리드 IT 환경 전체적으로 보안을 통합해야 합니다. 또한, 지능적 기능과 더불어 전체적 가시성, 정책 관리, 침입 방지(IPS)를 제공하는 NGFW 보안을 통해 다음과 같은 요소를 확보해야 합니다.

- **성능.** 위험을 관리하려면 고성능 네트워크에 발맞출 수 있는 보안과 공격면을 효과적으로 줄이는 강력한 기능이 필요합니다.

하이브리드 데이터 워크로드와 관련된 가장 큰 우려 사항은
데이터 보안/규정 준수(71%), 성능(62%), 간편한 관리(53%)입니다.[2]

- **회복성과 확장성.** 하이브리드 IT 환경이 확장되고 다각화되었기 때문에 데이터 센터 보안으로 확장성, 회복성, 가용성을 제공하여 안정적인 비즈니스 연속성을 보장해야 합니다. 전체적인 네트워크 및 보안 아키텍처도 네트워크 중단과 자연재해로 발생하는 중단 사태를 감당할 수 있어야 합니다.
- **자동화 및 오케스트레이션.** 통합 보안 아키텍처는 하이브리드 IT 인프라에 지능적 자동화 기능을 제공합니다. 자동 보안 대응과 가속화된 관리 기능은 위험 노출의 여지를 줄이면서도 직원의 업무 부담, 인간의 오류, 운영 경비(OpEx)를 낮춥니다.

위험 관리 성능

데이터 센터 방화벽은 대개 네트워크의 가장 빠른 곳에 배포됩니다. 그러므로 이런 사용 사례에서 배포된 효과적인 NGFW 솔루션은 네트워크 성능에 미치는 영향을 최소화하고 지능적 L7 보안을 적용할 수 있어야 합니다. 이를 위해서는 NGFW가 네트워크 병목을 일으키지 않고 보안 기능을 안정적으로 실행할 수 있는 전용 보안 프로세서가 솔루션에 탑재되어 있어야 합니다. 분산된 현대의 데이터 센터를 보호하려면 각 환경(예: 온프레미스, 코로케이션, 클라우드)에 배포된 모든 보안 요소는 물론이고, 사용자, 애플리케이션 기기에 대한 정보까지 볼 수 있어야 합니다.

보안 침해의 1/3 이상이 신뢰할 수 있는 내부 소스에서 발생하기 때문에,[3] 내부 네트워크의 액세스 제어도 필수입니다. 네트워크 엔지니어링 및 운영 관리자에게는 다양한 사용 사례(예: 사용자, 기기, 애플리케이션에 대한 동적인 신뢰)에 대응할 만큼 확장성과 유연성이 뛰어난 네트워크 망분리가 필요합니다.

현재 기업의 77%가 기업 내에서 통합되지 않은 포인트 보안 솔루션을 사용하고 있습니다.[4]

그러나 독립적 망분리 자체만으로는 현재의 지능적 위협에 대항하는 데 중요한 보안 기능(예: 콘텐츠 검사)을 제대로 제공할 수 없습니다. 그래서 데이터 센터에 대한 NGFW 배포는 여러 망분리 기술에 맞게 변경하고, 타사 보안 솔루션과 연결하여 위협 인텔리전스를 공유하고, 콘텐츠 검사 및 자동 위협 보호를 제공할 수 있어야 합니다.

오늘날 위협이 발생하는 정도와 속도를 따라가려면 통합된 보안 아키텍처에서 실시간으로 인텔리전스를 공유하는 보안이 필요합니다. 그와 동시에 인공 지능(AI)을 활용한 보안으로 알려지지 않은 위협을 찾아내야 합니다. 특히, AI 기반 위협 탐지 및 예방은 위치와 관계없이 모든 디지털 자산에 적용할 수 있어야 합니다.

회복성 및 확장성

끊임없이 확장되는 디지털 혁신은 보안에 직접적 영향을 미칩니다. 데이터 센터 워크로드는 하이브리드 IT 인프라에 점점 분산되고 있어서, 새로운 애플리케이션을 사용하고 워크로드가 늘어나면 기존의 어플라이언스를 넘어 온프레미스, 클라우드, 가상 머신(VM) 배포 이터레이션까지 대규모로 확장되는 탄력적 보안이 필요합니다. 데이터 센터 보안도 암호화되지 않은 데이터 플로와 암호화된 데이터 플로를 포함하여 끊임없이 늘어나는 트래픽의 요구 사항에 맞게 변경되어야 합니다.

현재 총 네트워크 트래픽의 72% 이상이 암호화된 데이터로 구성됩니다. 이 수치는 전년 대비 20% 가까이 늘어났습니다.[5] 암호화된 트래픽이 증가하면 HTTP 및 HTTPS 트래픽 검사 도구를 통한 지능적 가시성이 필요합니다. 분산된 데이터 센터는 암호화된 데이터 플로를 따라 은밀하게 움직이는 위협에 취약합니다.
이런 위협을 완화하려면 사용자와 시스템, 그리고 시스템 사이를 오가는 대량의 트래픽에 고급 보안 소켓 계층(SSL)/전송 계층 보안(TLS) 암호화 검사(및 샌드박싱과 디코이/함정 통합)를 제공하면서도 애플리케이션에 성능을 미치지 않는 보안이 필요합니다. 최신 TLS 1.3 검사 기능도 포함해야 합니다.[6]

회복성과 가용성 측면에서 보았을 때, 구성 요[6]소 장애가 발생할 시 실시간 장애 조치를 취할 수 있도록 하는 솔루션이어야 합니다. 기본으로 제공되는 N+1 클러스터링은 완전히 중복된 아키텍처를 제공하여 단일 고장 지점을 제거합니다. 독립적 산업 전문가를 통한 타사 검증 테스트를 받으면 실제 상황에서 솔루션이 얼마나 안정적인지 확인하는 데 도움이 됩니다.

자동화 및 오케스트레이션

사이버 보안 기술 인력 부족 현상이 지속되면서 많은 소수 인력 보안 기업이 심각한 업무 부담에 시달리게 되었습니다. 운영 복잡성을 줄여야 OpEx 비용을 줄이고 기술 보안 인력이 수동 작업 대신 사업 성과에 집중하기 때문에 최적화를 달성할 여력이 생깁니다.

따라서 효과적인 데이터 센터 방화벽이라면 간소화된 배포 및 관리에 최적화된 워크플로와 같은 기능을 포함해야 합니다. 통합 보안 아키텍처는 하이브리드 인프라에서 보안을 조정하는 자동 대응과 인텔리전스 공유를 위한 기반을 제공합니다. API를 지원하는 NGFW 솔루션은 중요한 장점을 제공합니다. 예를 들어, 워크플로 자동화, 오케스트레이션, 패치되지 않은 애플리케이션과 지속해서 변경되는 DevOps 환경에 대한 보안 대응이 있습니다.

또한, 솔루션에는 사용자, 기기, 애플리케이션에 대한 지속적 신뢰를 설정하는 비즈니스 로직을 적용하고 보안 프로세스(예: 프로비저닝, 액세스 제어)를 자동화하는 기능도 필요합니다. 직원의 업무 부담과 OpEx 비용이 감소하면서도 운영 효율과 보안 효과는 높일 수 있습니다. 규정 준수 보고와 감사 프로세스를 자동화하는 NGFW 기능은 네트워크 엔지니어링 및 운영 관리자가 워크플로 부담을 줄이면서도 변화하는 정부 및 산업 규제, 보안 표준(예: NIST(National Institute of Standards and Technologies), CIS(Center for Internet Security))을 따라갈 수 있도록 도와줍니다.

IT 의사결정자의 절반 이상(54%)이 하이브리드 모델 도입 시 인력 유지도 문제가 된다고 답했습니다.[7]

통합된 업계 최고의 NGFW 성능을 선택할 필요성

데이터 센터가 분산되고 하이브리드 IT 전략으로 옮겨갈수록 기업의 공격면은 확장됩니다. 데이터 센터 성능 수준을 높여야 한다는 요구가 계속되는 가운데, 네트워크 엔지니어링 및 운영 관리자는 보안을 지키면서도 사용자 요구를 수용해야 합니다. 위험이 증가하고, 네트워크가 중단될 가능성이 커지면서 비용이 상승하는 것을 피할 수 없기 때문에 기업에서는 현대적 데이터 센터를 위한 보안이 무엇인지 다시 생각해야 합니다. 네트워크 엔지니어링 및 운영 관리자는 보안과 성능이라는 두 마리 토끼를 잡기 위해서 안정적 NGFW 솔루션(성능, 회복성, 확장성, 자동화 기능을 갖춘 솔루션)에 기반한 통합 보안 아키텍처를 받아들여야 합니다.

[1] Filip Truta, "Downtime Can Cost a Company up to $67 Million Over Two Years, Threatening Brand Reputation," Security Boulevard, 2019년 2월 21일.

[2] Alison DeNisco Rayome, "91% of tech leaders say hybrid cloud is 'ideal' IT model," TechRepublic, 2018년 11월 15일.

[3] "2019 Data Breach Investigations Report," Verizon, 2019년 4월.

[4] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, 2019년 5월 23일.

[5] John Maddison, "Encrypted Traffic Reaches A New Threshold," Network Computing, 2018년 11월 28일.

[6] Alex Samonte, "TLS 1.3: What This Means For You," Fortinet, 2019년 3월 15일.

[7] Alison DeNisco Rayome, "91% of tech leaders say hybrid cloud is 'ideal' IT model," TechRepublic, 2018년 11월 15일.

www.fortinet.com/kr

725546-0-0-EN