모든 환경 전반에서 웹 애플리케이션 및 API 보호

포괄적이고 사용하기 쉬운 SaaS 보안 솔루션으로 멀티 클라우드와 온프레미스 인프라 전반에 구축된 귀사의 웹 애플리케이션과 API를 보호하십시오.

주요 이점

포괄적이고 사용하기 쉬운 SaaS 보안 구현
단일 SaaS 보안 솔루션으로 모든 클라우드와 온프레미스 환경의 웹 애플리케이션과 API를 보호할 수 있습니다.

분산 애플리케이션 및 멀티 클라우드 환경을 위해 특별히 설계된 솔루션으로 어디서나 구축 가능
F5 분산 클라우드 플랫폼(F5 Distributed Cloud Platform)은 처음부터 고도로 모듈화된 분산형 모던 애플리케이션들에 쉽게 접근할 수 있는 첨단 보안 기능들을 제공하기 위해 개발되었습니다.

end-to-end 관리 및 정책 적용으로 SecOps들이 더 많은 작업을, 더 빨리 수행할 수 있도록 지원
클라우드 및 온프레미스 환경 전반에서 이식 가능한 가시성과 통합 보안 정책을 제공함으로써 SecOps 팀의 업무 효율성을 향상시킵니다.

통합 서비스, SaaS 폼 팩터 및 유연한 구축을 통한 TCO 절감
별도의 정책과 인프라를 유지 관리할 필요가 없는 단일 클라우드 보안 스택으로 서로 다른 클라우드 보안 솔루션들을 통합해 전반적인 TCO를 절감할 수 있습니다.

개발자 경험 향상 및 서비스 시간 단축
일반 프로세스의 일부로서 보안 워크로드 배포와 검증을 자동화할 수 있도록 기존 CI/CD 워크플로우 및 DevOps 툴에 쉽게 통합함으로써 개발자 경험을 최적화합니다.

멀티 클라우드와 엣지 환경 전반으로 애플리케이션 및 API 보호 확대

오늘날 애플리케이션 세계에서 애플리케이션 보안은 비즈니스 연속성을 결정합니다.

기업 애플리케이션 보호는 이제 기업 비즈니스, 고객 및 수익원의 보호를 의미합니다. 온라인 상거래를 운영하거나 진행하려는 어느 누구도 보안을 소홀히 할 수 없는 것도 바로 이 때문입니다. 기업의 애플리케이션에 대한 위협이 만연한 상황이지만, 예전부터 애플리케이션 보안 기술과 전문 기술을 도입, 구현 및 유지 관리하는 것은 어려운 일이었습니다. 개발 모델과 애플리케이션 아키텍처가 발전하며 멀티 클라우드 배포, API 확산, auto-scaling, 서버리스 구현 등을 포함하게 되면서 이는 더욱 어려워졌습니다.

모던 마이크로서비스는 증가하는 애플리케이션 사용량을 수용하고 향상된 성능을 제공하기 위해 점차 분산 애플리케이션 아키텍처를 사용하여 구축되고 있습니다. 사용자의 가용성과 성능 기대치가 변화하고 있기 때문에, 기업들은 origin 클라우드로 장거리를 이동하는 것과는 대조적으로 가까운 지사 및 위성 사이트에서 경량의 애플리케이션을 실행하여 온프레미스 또는 엣지에서 데이터 액세스와 주요 텔레메트리 처리 속도를 높이는 방식을 선택하고 있습니다. 하지만, 이 경우, 기업들이 분산 애플리케이션 인스턴스에 일관되고 효과적인 보안을 제공하기 어려울 수 있습니다.

NetOps와 SecOps는 빠른 변화 속도를 따라잡을 수 없었으며, DevOps 팀은 NetOps와 그 보안 툴킷들을 기업이 요구하는 혁신의 방해 요인으로 생각하고 있습니다. 뿐만 아니라, 모던 마이크로서비스 기반 애플리케이션과 API의 성장으로 애플리케이션 공격 경로가 확대되면서 전통적인 솔루션들은 일관된 보안 커버리지를 제공할 수 없습니다. 이때문에 SecOps 팀은 서로 다른 여러 레거시 보안 솔루션들을 사용하고 유지 관리해야 했는데, 그 결과, 많은 노력에도 불구하고 매우 저조한 성과를 거두고 있습니다.

이러한 과제들은 결국, 높은 TCO와 진화하는 공격에 맞서는 보안 효과의 저하를 초래했습니다. 한계에 달한 리소스와 효과적이지 못한 툴들은 공격이 발생했을 때 SecOps가 수동으로 대응해야 한다는 것을 의미하며, 이미 과부하 상태인 리소스에 더욱 부담을 가중시키고 있습니다.

보안을 소홀히 하는 기업들은 비즈니스 자체에 위험을 감수해야 합니다. 하지만, 복잡성을 간소화하고 사이버 범죄자들을 어렵게 만드는 방법이 있습니다. 능동적이고 확장 가능하며 머신러닝과 글로벌 위협 인텔리전스를 활용하는 보안 중심 인프라에 대한 투자는 비즈니스 운영의 토대가 되는 웹 애플리케이션과 API를 보호하는 데 성패를 가르게 될 것입니다.

주요 특징

애플리케이션들이 구축된 위치에 관계없이 모든 기능을 갖춘 보안 솔루션
상태 모니터링을 통한 자가 치유(self-healing)와 점진적인 롤아웃(progressive rollout) 등을 비롯한 중앙집중식 제어 영역을 통해 애플리케이션과 워크플로우가 네트워크 엣지, 퍼블릭 클라우드 또는 온프레미스 등 어디에 구축되어 있건 관계없이 보안 프로비저닝을 자동화합니다.

요구사항에 맞게 확장되는 강력한 보호 기능
기업의 필요에 따라, 또는 개별 애플리케이션의 필요에 따라 첨단 웹 방화벽(WAF) DDoS 완화, 봇 감지 및 API 보안 등과 같은 강력한 적응형 보안 서비스를 추가할 수 있습니다.

중앙집중식 관리: 네트워크 + 애플리케이션 + 보안
애플리케이션 배포, 인프라 상태, 보안, 가시성 및 성능에 대한 자세한 현황 정보를 비롯해 이기종 엣지 및 클라우드 구축 환경 전반의 애플리케이션에서 인프라까지 망라하는 통합된 가시성을 확보할 수 있습니다.

특수한 용도로 개발된 글로벌 네트워크
F5는 13개 대도시를 잇는 20개 이상의 글로벌 PoP를 통해 앱과 앱(app-to-app) 간 연결과 글로벌 앱 딜리버리를 위해 최적화된 고성능 글로벌 백본을 제공합니다.

계정정보 및 비밀번호 관리
자동 인증서 갱신을 통해 각 애플리케이션 인스턴스를 위한 계정정보 라이프사이클을 관리하여 여러 멀티 클라우드 및/또는 엣지 환경 전반의 애플리케이션들에 통일된 계정정보 서비스를 제공합니다.

중앙에서 보안을 유지하면서 전세계적으로 손쉽게 운영하는 방법

F5는 탁월한 성능과 전 세계적인 규모로 고객의 모던 애플리케이션들을 보호하고 보안을 유지합니다. F5의 클라우드 네이티브 보안 서비스들은 지난 수십 년 동안 전 세계적으로 모든 규모 기업들을 위해 모든 규모 및 유형의 애플리케이션을 보호하면서 축적한 경험을 통해 뒷받침됩니다.

이들 서비스들은 머신러닝과 전 세계에서 입수한 위협 인텔리전스를 활용하여 끊임없이 진화하는 잠재적인 위협으로부터 애플리케이션들을 보호합니다. 보안에 대한 계층화된 모듈형 접근 방식을 통해 기업들은 필요한 제어 툴만 구입하고 구현할 수 있기 때문에 비용을 절감하고 전반적인 효율성을 높일 수 있습니다.

또한, F5 분산 클라우드 플랫폼을 사용하면 데이터센터에서 클라우드와 엣지에 이르기까지, 컨테이너화된 모던 애플리케이션들을 배포하고 실행할 수 있으며, 클라우드 네이티브 관리, 일관된 보안, end-to-end 가시성이 제공됩니다. 단 몇 분 내에 효율적으로 배포되는 공통 정책 및 서비스 집합을 통해 전 세계 사용자들은 주요 애플리케이션들을 점차 더 많이 사용할 수 있게 됩니다.

솔루션 구성 요소

F5 WAAP(F5 Distributed Cloud Web Application and API Protection) 솔루션은 글로벌 데이터센터 네트워크 전반에서 운영되며 광범위한 클라우드 네이티브 애플리케이션 인프라와 강력하고 효과적인 애플리케이션 및 API 보호 서비스를 제공합니다.

- **웹방화벽(Web Application Firewall):** 중간 프록시의 역할을 수행하고 애플리케이션 요청 및 응답을 검사하여 해킹, 제로데이 익스플로잇(zero-day exploit), L7 DoS(Denial of Service) 등 다양한 위험을 차단하고 완화함으로써 수많은 위협으로부터 웹 기반 애플리케이션을 보호합니다.
- **API 보호:** 침해 또는 다른 서비스 중단을 야기하기 위해 API를 악용하려고 시도하는 위협 행위자로부터 API를 보호합니다. API 보호는 WAF와 비슷한 기능을 수행하지만, 전통적인 WAF는 그 고유한 특성으로 인해 일반적으로 API 프로토콜이나 데이터 흐름에 대한 충분한 커버리지를 제공하지 않습니다. 따라서, WAF만을 구축한 경우, 많은 애플리케이션들에 심각한 커버리지 공백이 발생하게 됩니다.
- **봇 방어:** 악의적인 자동화를 관리 및 방어하고 정상적인 M2M(machine-to-machine) 통신을 중개하여 웹사기, 지적재산도용, 크리덴셜 스터핑(credential stuffing) 및 계정탈취, 산업 스파이, DoS(Denial of Service) 등과 같은 비즈니스 로직 위험을 막습니다.
- **DDoS 차단:** 고객의 신뢰를 잃고 서비스에 접속할 수 없도록 하기 위해 기업 서비스에 과부하를 발생시켜 네트워크 연결을 중단시키거나 방해하려고 시도하는 스푸핑된(spoofed) 비정상적인(malformed) 트래픽, 요청 폭주, 기타 형태의 오용 등을 필터링하는 방식으로 네트워크 레벨에서 볼륨 Dos 공격을 차단합니다.

기업 애플리케이션을 보호한다는 것은 바로 비즈니스, 고객 및 수익원을 보호한다는 것을 의미합니다.

애플리케이션이 어디에 구축되어 있건 관계없이 모든 애플리케이션에 원하는 모든 보호 기능을 원활하게 추가한 다음, 필요에 따라 보호 기능을 구현하고 발전시켜 인젝션(injection), XSS(Cross-Site Scripting), 소프트웨어 취약점 등과 같은 일반적인 위협을 방어할 수 있습니다.

또한, F5 분산 클라우드 WAAP는 중앙 지점에서 세계 전역에 분산된 애플리케이션들에 대한 운영 통찰력과 성능 데이터를 제공합니다. 이를 통해 전반적인 효율성을 높이고, 지원을 간소화하며, 기업이 성장하고 고객을 유지하는 데 도움이 되는 비즈니스 인텔리전스 지표를 향상시킬 수 있습니다.

중앙에서 관리되는 F5의 클라우드 플랫폼은 보다 쉽게 감사를 수행하고, 애플리케이션에 대한 정책 준수를 지원하며, 애플리케이션들이 직면한 위험과 위협에 대해 적절한 정책이 적용되도록 보장하는 등 다른 관련 이점들도 제공합니다.

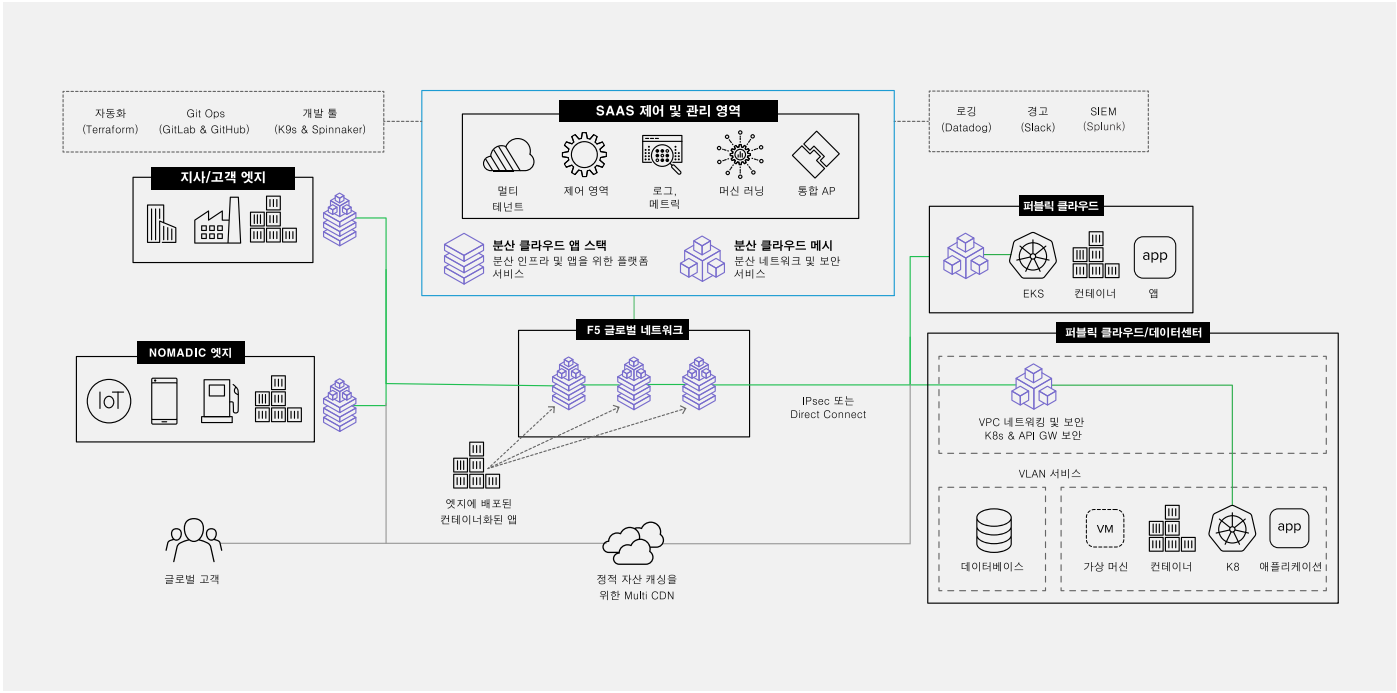

그림 1: F5 분산 클라우드 플랫폼

F5 분산 클라우드 WAAP 솔루션은 글로벌 데이터센터 네트워크 전반에서 운영되며 광범위한 클라우드 네이티브 애플리케이션 인프라와 강력하고 효과적인 애플리케이션 및 API 보호 서비스를 제공합니다.

매우 강력하고 효과적이며 확장 가능한 보안을 통해 우수한 디지털 경험 제공

애플리케이션은 비즈니스의 원동력이며 사이버 범죄자들도 이를 잘 알고 있습니다. 최신 위협에 대응하기 위해서는 확장 가능한 적응형 보안 솔루션이 필요합니다. 애플리케이션들이 점차 모듈화되고 분산되면서, 중앙집중식 SaaS 인프라를 통해 관리되는 동시에 어느 위치에나 배포가능한 보안 서비스가 필요합니다.

F5 분산 클라우드 플랫폼은 오늘날 애플리케이션 아키텍처가 요구하는 보안 성능과 사용 편의성을 제공합니다. 이는 규모에 맞춰 탁월한 성능과 가용성을 갖춘 모던 애플리케이션 서비스를 제공하는 보다 나은 방법입니다. 데이터센터나 코로케이션 사이트에서 클라우드 파트너, 그리고 엣지에 이르기까지 고객들이 원하는 어디에서나 컨테이너와 마이크로서비스 애플리케이션들을 구축해 실행함으로써 클라우드 네이티브 운영, 일관된 보안 및 end-to-end 관리를 제공할 수 있습니다.

일관되고 반복 가능한 결과와 글로벌 커버리지 및 적용을 위해 "단 한 번 작성하고 어디서나 실행하는(Write-Once, Run Anywhere)" 보안 정책의 이점을 거둘 수 있습니다. F5의 애플리케이션 보호에 대한 API 기반 접근 방식은 네트워크, 보안 운영 및 개발자들 간의 협업을 향상시키며, 클라우드 독립적인 애플리케이션 배포 및 관리 인프라는 애플리케이션들이 어디에 구축되어 있건 관계없이 클라우드 간 운영, 성능, 분석 및 위협 가시성을 제공합니다.

이 혁신적이고 쉽게 접근할 수 있는 플랫폼은 기업들이 애플리케이션 보호 커버리지 공백을 줄이고 애플리케이션 포트폴리오 전반에 일관된 커버리지를 적용하도록 지원할 수 있습니다. F5 분산 클라우드 WAAP를 통해 보다 간편하게 효과적인 보안을 구현하고 귀사의 비즈니스와 고객들이 요구하는 혁신에 박차를 가하십시오.

다음 단계:

자세한 내용은 f5.com/waap에서 확인할 수 있습니다.

DC0420 | OV-CLOUD-789852666