정적 애플리케이션 보안 테스트에 대한 Magic Quadrant

Gartner RAS Core Research Note G00208743, Joseph Feiman, Neil MacDonald, 2010년 12월 13일

본 조사에서 우리는 정적 애플리케이션 보안 테스트 시장의 발전에 대해 분석하고 비즈니스 및 기술 비전 그리고 그 비전을 자사 제품 및 서비스에 이행하는 능력을 기준으로 벤더들을 평가한다.

알아두어야 할 사항

금전적인 동기에 의한 공격이 점점 늘어나고 기업들이 자사 네트워크, 데스크톱 및 서버 인프라스트럭처에 대한 보안을 개선하면서, 애플리케이션 수준의 공격에 대한 변화가 나타났다. SAST(Static application security testing)는 애플리케이션 보안을 겨냥한 기술 시장 중 하나다.

애플리케이션을 개발하거나 구입하는 모든 IT 조직에게 SAST는 이제 의무적인 요구사항으로 간주되고 있다. 비록 SAST 시장이 아직 성숙 단계에 이르지는 않았지만, 그 필요성이 전략적으로 중요하기 때문에 기업들은 SAST 기술과 프로세스를 채택해야만 할 것이다.

SAST 기술은 점진적으로 발전하고 있다: SAST 시장만이 최근 Gartner의 "2010년 데이터 및 애플리케이션 보안에 관한 관심주기(Hype Cycle)"에서의 환멸기(Trough of Disillusionment)를 벗어났다. 주로 애플리케이션 보안 채택에는 기술적인 진보뿐만 아니라 애플리케이션 개발 및 유지보수 프로세스의 변화도 요구하기 때문에, 시장이 완벽하게 성숙하고 기술이 보편적으로 채택되는 데까지는 5년 이상이 소요될 것으로 예상된다. 단순히 SAST 솔루션이나 다른 애플리케이션 보안 기술을 구입한다고 해서 애플리케이션 보안 문제를 해결할 수 있는 것은 아니다. 사고방식과 프로세스에 대한 변화도 더불어 이루어져야 하며, 이를 이행하는 것은 쉬운 일이 아니다.

지속적으로 시장 통합이 진행되고 있으며, 현재 시장에서는 대규모 애플리케이션 개발 플랫폼 벤더들이 SAST 기술을, 그리고 소규모의 혁신적인 신생기업들이 포인트 솔루션(point solution)을 제공하고 있다.

전략 계획의 전제

2012년에 이르면, 일류 SAST 벤더들은 그들의 전략적 목표인 엔터프라이즈 보안 인텔리전스를 사용하게 될 것이다.

2015년에 이르면, 60% 이상의 기업들이 그들의 애플리케이션 개발 프로세스에 SAST 솔루션을 사용하게 될 것이다.

2015년에 이르면, 70% 이상의 기업들이 그들의 아웃소싱, SaaS, 클라우드 및 상용 소프트웨어 공급자들의 SAST 테스트 입증을 요구하게 될 것이다.

Gartner

2 MAGIC QUADRANT

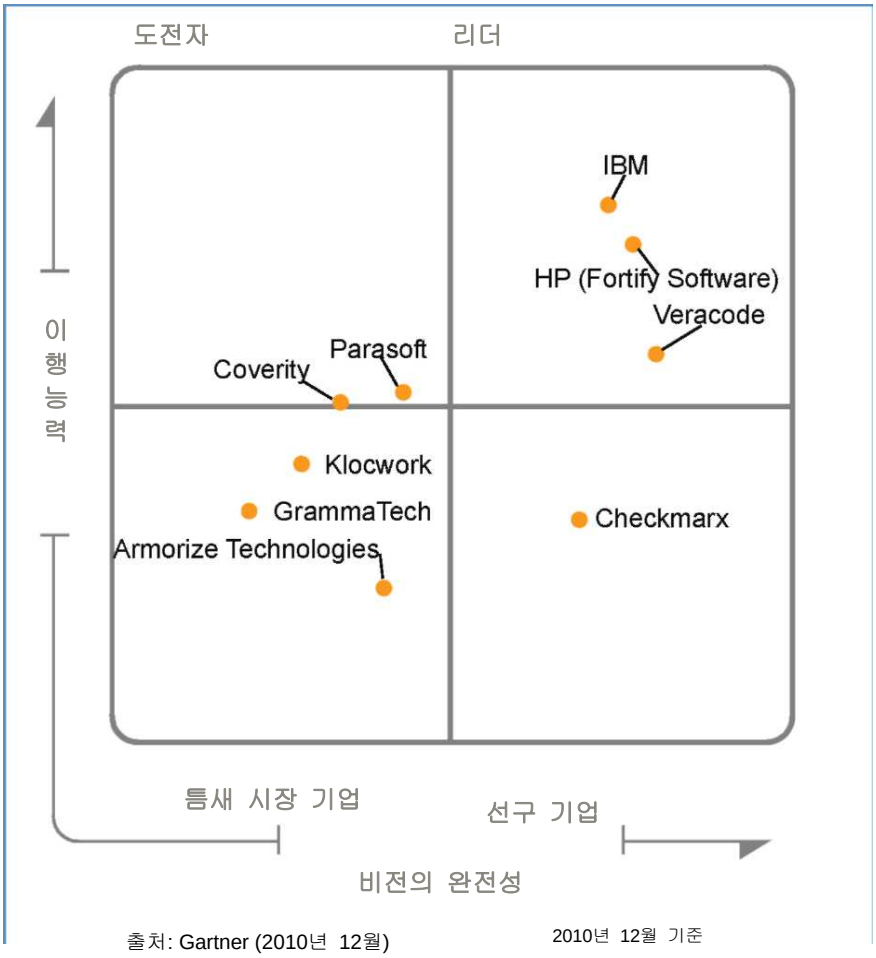
시장 개요

지난 18개월 동안, 새로운 핵심적인 추이가 나타났으며 아울러 이전에 파악했던 추이가 한층 발전하는 양상을 보이고 있다.

ESI(enterprise security intelligence)의 조기 채택: SAST (및 동적 애플리케이션 보안 테스트[DAST]) 벤더들 간에는 애플리케이션 보안 시장이 발전하여 ESI를 가능하게 하는 도구 (enabler)가 될 것이라는 새로운 이해의 관점이 대두되고 있다. ESI는 *보안 인텔리전스를 명시적인 결과물(deliverable)*로 인식하고 이 인텔리전스를 기업의 IT 보안 및 위험 관리 프로그램의 전략적인 보안 목표로 정하는 개념이다. ESI는 향상된 정확도와 광범위한 보안 검출 및 보호와 최적의 보안 및 위험 관리를 제공하는 것을 목표로 한다.

ESI를 가능하게 하는 것은 (1) 기술의 상호작용 및 상관관계, (2) 정보의 통합 및 상관관계라는 두 가지 중요한 요소에 입각하고 있다. 여러 보안 기술들의 상호작용을 통해 *향상된 정확도와 광범위한 보안 검출 및 보호*를 제공하고 비즈니스 상황 데이터의 통합과 상관을 위한 향상된 정확도와 광범위한 보안 정보를 제공하는데 주안점을 둔다. 이러한 데이터들이 결합되어 *최적의 보안 및 위험 관리*를 가능하게 하는 *상황 평가(contextual assessment)*를 제공한다. 기업들은 보안 시스템이나 솔루션을 개발할 때 ESI 개념을 핵심 아키텍처 원칙으로 적용해야 하며, 기술 벤더들이 보안 도구나 플랫폼(SAST 포함)을 개발할 때도 마찬가지여야 한다:

그림 1. SAST에 대한 Magic Quadrant



출처: Gartner (2010년 12월)

2010년 12월 기준

1. SAST 및 DAST 상호작용: ESI 개념의 기본적인 요소 중의 하나는 여러 기술들의 상호작용이다. 지난 18개월 동안 우리는 SAST 및 DAST 기술/서비스를 (직접 또는 제휴를 통해 간접적으로) 제공하는 일류 애플리케이션 보안 솔루션 공급업체들이 이 기능을 제공하고 있는 것을 확인했다. 보다 발전된 솔루션은 SAST 및 DAST 기술의 상호작용에 상관된 결과의 후속 분석을 제공한다. 이러한 두 테스트 기술간의 상호작용 및 상관관계는 상당한 이점을 제공한다. SAST 및 DAST 기술을 사용하면 분리된 어느 하나를 사용하는 경우보다 더 많은 소프트웨어 수명주기(SLC)의 단계(예: 프로그래밍, 테스트 및 운영)를 분석할 수 있다. 무엇보다도 하나의 기술로 추정된 취약성을 다른 기술로 확인하거나 반증할 수 있으므로 분리된 기술의 사용과 관련된 오탐(false positive : 취약점이 아닌데 취약점으로 찾아내는 것) 및 미탐(false negative : 취약점인데 찾아내지 못하는 것)을 줄여 검출의 정확도를 높일 수 있다. 이러한 방향으로 오퍼링을 발전시키고 있는 벤더들은 다음과 같다:

- AppScan SAST 및 DAST 기술을 보유한 IBM
- HP와 제휴하고 있는 SAST와 자사의 DAST를 보유한 Fortify Software (Fortify는 2010년 하반기에 HP에 인수되었다)

- 2011년에 SAST 및 DAST 서비스의 상호작용을 계획하고 있는 Veracode

2. ESI의 또 다른 기본적인 요소는 보안 정보와 상황 정보(contextual information)의 통합 및 상관관계다. 테스트된 애플리케이션의 비즈니스/컴플라이언스/지적 재산권 등의 측면을 정의하는 상황 정보와 더불어, SAST (및 DAST) 기술로 수집된 보안 분석 결과는 영구적인 리포지토리에 보관해야 하며, 그렇게 함으로써 상황 위험(contextual risk) 평가 및 최적의 위험 관리를 위한 조회가 가능해지며 그 평가에 입각한 비즈니스 의사결정을 내릴 수 있게 된다. 예를 들어, Checkmarx 및 Veracode와 같은 벤더들은 리포지토리 및 조회 기능을 제공하기 시작하였다.

우리는 향후 벤더들이 IAM(identity and access management), 네트워크 보안, 데이터베이스 보안 등과 같은 여타 보안 기술로부터 얻은 보안 정보를 추가할 수 있을 것으로 예상한다. SIEM(Security information and event management) 기술은 다양한 소스(예: 네트워크, IAM, Endpoint Protection)의 다양한 보안 스캐너 및 모니터에서 보안 정보를 수집하는데 결정적인 역할을 할 것이며, 애플리케이션 보안 기술이 분석 및 애플리케이션 모델을 SIEM 기술에 통합하는 능력이 점점 중요해질 것이다.

서비스로서의 보안 테스트와 클라우드로의 진화:
Gartner는 서비스로서의 보안 테스트가 선행투자 비용을 줄이고 제한된 내부 리소스를 증대시키는 것과 같이, 기업에 여러 가지 이점을 가져다 준다고 생각한다. Checkmarx 및 Veracode와 같은 벤더들은 서비스로서의 SAST 기능만을 제공하고 있다 (Checkmarx는 제품 라이센싱도 제공하고 있지만, 선호하는 모델은 아니다). HP 및 IBM과 같은 벤더들은 세계적으로 전문적인 클라우드 기반 서비스 역량을 갖추고 있으며, 기술 라이센스 판매 외에 SAST 서비스를 제공하고 있다.

서비스로서의 테스트는 애플리케이션 보안 시장에 점점 더 현저한 영향을 미치고 있다. 예를 들어, SAST 제품을 이용하여 자사의 보다 민감한 애플리케이션을 사내에서 테스트하고, 다소 민감하지 않은 애플리케이션은 SAST 서비스를 이용하여 테스트하거나 배포된 애플리케이션을 서비스로서 테스트하거나 사내 SAST 제품을 이용하여 개발중인 애플리케이션을 테스트하는 등, 기업들이 SAST 벤더의 제품 및 서비스를 사용하는 것을 선호한다는 이야기를 점점 더 많이 듣고 있다.

클라우드 및 서비스로서의 보안(security-as-a-service) 오퍼링은 자사 소유의 하드웨어 및 소프트웨어를 구입/유지보수하는 대신에 그 각각의 하드웨어 및 소프트웨어를 보유하고 있는 클라우드 SAST 벤더들의 서비스를 사용하게 되므로 자본을 절약하는 등의 여러 가지 이유로 기업에게 더 매력적이다. 기업들은 또한 클라우드가 제공하는 각각의 SAST 서비스를 받을 경우, 자체 인적 자원의 채용, 교육 및 관리에서도 절감을 기대하고 있다.

또 다른 비용 절감 요인은 기업 고객들이 사용한 서비스에 대해서만 지불하는 "종량제(pay per play)" 원칙을 클라우드 서비스 공급업체로부터 기대할 수 있다는 점이다. 이로써 대기업뿐만이 아니라, 자사 소유의 기술 제품을 구입할 수는 없지만 각각의 서비스에 대하여 지불할 능력이 있는 중소기업도 클라우드를 이용할 수 있게 된다.

클라우드는 도입 장벽을 낮춘다: 이제 기업들은 대규모 서비스를 시행하기 전에 기술/서비스를 시용해볼 수 있다. 클라우드는 또한 지리적으로 분산된 여러 위치 간의 교량 역할을 해준다. 배포된 애플리케이션의 대량의 수주 잔량을 신속하게 끝낼 수 있다는 점이 외부 서비스/클라우드 서비스 공급업체를 이용하는 또 다른 이유다. 서비스의 일환으로, SAST 공급업체들은 스캔 결과의 인적 필터링에 의한 기술과 다소 연관된 오탐의 수를 줄여야 한다.

SAST를 포함한, 애플리케이션 보안 서비스에 대한 클라우드 기반의 모델은 수 많은 문제를 야기하게 될 것이다. 그 중의 하나는 소스 또는 바이너리 코드에 서비스 공급업체가 접근할 수 있고 기업의 애플리케이션 취약성을 서비스 공급업체가 속속들이 알 수 있다는 점이 우려된다. 또한, 일례로 검출에는 서비스로서의 SAST를 이용하면서, 사내 프로그래머가 개선(예: 소프트웨어 픽스)을 실시해야 하는 등 취약성 검출 위치와 취약성 개선 위치 간에는 차이가 있다. 또한, 검출은 클라우드 전문가에 의해 이루어지지만, 개선은 기업의 직원에 의해 이루어지는 등 조직 상에도 차이는 존재한다. 개선이 없는 검출은 전혀 의미가 없다. 따라서, 이러한 차이를 줄여 나가는 것이 매우 중요해 질 것이다.

기업과 클라우드 서비스 공급업체는 이러한 프로세스에 대한 통제를 정의하고 확립해야 한다. 기업이나 클라우드 서비스 공급업체 중 어느 누구도 전적으로 검출-개선 프로세스를 갖추지 못하게 될 것이므로, 경계를 정하고 기본 계약, 피드백 및 협업을 확립하는 것이 불가결하다. 기업과 클라우드 서비스 공급업체는 프로세스가 동기식일지 아니면 비동기식일지, 예를 들면 클라우드 서비스 공급업체가 동기식으로 (예: 매월 마지막 날) 또는 비동기식으로 (예: 새로 개발중인 애플리케이션의 다음 버전이 준비되면 SAST 테스트를 실시) SAST 테스트를 실시할 지와 같이 상세 프로세스를 결정해야 한다.

클라우드와 사내 프로세스는 통합되어야 한다. 예를 들면, 클라우드가 실시한 보안 테스트 결과를 사내에 위치한 또는 사내에서 접근 가능한 버그 추적 시스템에 입력하여, 사내 전문가가 그 결과를 알고 개선 활동을 실시할 수 있어야 한다. 통합 프로세스를 자동화하고 투명화 하는 것이 가장 바람직하다. 예를 들어, 새롭게 프로그램화된 애플리케이션의 모듈이 완성되면 클라우드 SAST 공급업체에 의해 SAST 테스트가 자동으로 시작된다.

보안 및 품질 기술 오퍼링의 결합: 이전부터 애플리케이션 품질 테스트에 전문적이었던 일부 벤더들은 자사의 테스트 도구 포트폴리오에 애플리케이션 보안 테스트를 추가하여 왔다. 이러한 벤더 중의 일부는 SAST 벤더를 인수하였으며, 품질 및 보안을 통합한 포트폴리오를 고객들에게 제공하기 위해 노력하여 왔다. 일례로, Rational 애플리케이션 플랫폼을 보유한 IBM은 2007년에 AppScan DAST 기술을 그리고 2009년에는 Ounce Labs SAST 기술을 추가하였으며, Quality Center 플랫폼을 보유한 HP는 DAST 기술을 제공하는 ASC(Application Security Center) 플랫폼의 마케팅을 시작하였으며, 2010년에 인수한 Fortify SAST 기술을 판매할 예정이다. 또한, Parasoft는 수 년 동안 자사 소유의 품질 테스트 기술과 결합된 SAST 및 DAST 보안 테스트 기술을 제공해 왔다.

주력 분야인 품질 테스트와 더불어 일부 보안 테스트 역량을 갖춘 여타 애플리케이션 품질 테스트 벤더들(예: Coverity)은 순수 SAST 주력 벤더들(예: Armorize Technologies)과 제휴하여 품질 및 보안 결합 테스트 포트폴리오를 제공하기 시작하였다. 품질 및 보안 테스트 기능 간의 기술 통합 수준은 두 분리된 제품을 단순히 묶어서 판매하는 대부분의 마케팅 활동에서부터 품질 및 보안 테스트 결과를 동일한 리포지토리에 기술적으로 통합하여, 결과를 상관시키고 분석할 수 있는 수준(예: Coverity와 Armorize의 제휴)에 이르기까지 차이가 있다.

SLC 플랫폼과의 SAST 통합: 애플리케이션 개발 전문가들이 프로그래밍 단계의 초기에 SAST 도구를 이용하여 보안 취약성 검출 및 개선을 수행하고 빌드/테스트 단계를 거쳐 테스트에 운영 전문가가 개입할 수도 있는 실사용/운영 단계에 이르는 SLC 프로세스의 경우 애플리케이션 보안 테스트가 적절하다. 대부분의 기업들은 SLC 플랫폼과 치밀하게 통합된 SAST 기능을, 특히 아주 적은 비용으로 SLC 플랫폼에 그러한 기능을 포함시키는 것을 선호할 것이다. SAST를 서비스로서의 소프트웨어(SaaS) 또는 클라우드로 구매하더라도 개선을 위한 SLC 프로세스/플랫폼과 치밀하게 통합하는 것이 바람직하다.

Magic Quadrant 개요

- Gartner의 2009년 " SAST에 대한 Magic Quadrant"에서 시장의 두 리더는 전용 SAST 포인트 솔루션을 공급했던 신생 벤더인 Fortify와 Ounce Labs였다. 그 이후, Ounce Labs는 IBM이 2009년에, Fortify는 HP가 2010년에 인수하였다. 이 인수는 두 세계 최대 IT 벤더들의 리소스를 이 포인트 솔루션 벤더들의 혁신 및 사고의 리더십과 결합시켰다.

소규모의 혁신적인 포인트 솔루션 벤더 중의 하나였던 Veracode도 리더 사분면으로 자리를 옮겼다. 이러한 변화는 SAST 시장이 아직 본격적인 보급기(Plateau of Productivity)에 도달하지 않았으며 여전히 발전하고 혁신을 거듭하고 있다는 강력한 반증이다.

이 세 리더들은 모두 애플리케이션 보안을 자사의 전략적인 목표로 삼았다. 이들은 자사 애플리케이션 보안 플랫폼의 ESI 기능을 강화하고 있으며, 특히 세 업체 모두 DAST 기술을 제공하고 있으며, SAST 및 DAST 상호작용 및 상관관계에 진전을 이루었다. 또한, 리포지토리, 조회 및 상황 평가(contextual assessment)와 같은 여타 ESI 기능의 개발에도 노력을 기울이고 있다. Veracode는 서비스로서의 SAST로 혁신의 리더였으며 SaaS/클라우드를 자사의 유일한 전달 모델로 만들었다. IBM과 HP는 예전부터 제품 중심이었으나 SaaS/클라우드를 우선순위로 삼았고 현재 SaaS/클라우드에 중점을 두고 있다.

애플리케이션 보안 분야에서 자사의 비전과 실행 능력을 입증한 IBM은 광범위한 포트폴리오의 애플리케이션 보안 솔루션을 제공하고 있다. 2009년 Ounce Labs의 인수로 SAST 기술을 확보하기 전에, IBM은 2007년에 Watchfire를 인수하여 DAST 기술을 확보하였다. 양사 모두 IBM의 조직, 문화 및 기술 포트폴리오에 성공적으로 통합되었다. 아울러, IBM은 데이터베이스 활동 모니터링 및 데이터 마스킹 기술을 위해 인접 애플리케이션 보안 부문을 인수하였으며 이로써 IBM은 자사 고객들의 훨씬 광범위한 애플리케이션 및 데이터 보안 요구사항에 부응할 수 있었다.

HP가 2010년 Fortify를 인수하면서 애플리케이션 보안 테스트 시장에서의 HP의 비전을 더욱 분명히 했지만, 견실한 실행을 통해 이러한 비전을 실현하고 Fortify를 자사의 문화, 제품 및 서비스 오퍼링에 통합할 수 있다는 HP의 능력에 대한 입증이 요구된다 (HP가 2007년에 인수한 일류 DAST 벤더인 SPI Dynamics와의 통합은 그 잠재력을 최대한으로 발휘하지 못했다). HP는 단지 애플리케이션 보안만이 아니라, 자사의 모든 보안 오퍼링을 아우르는 명확한 보안 전략이 결여되어 있다.

Veracode는 리더들 가운데서 유일한 신생 벤더이다. 업계 최대인 두 벤더들과 경쟁하려면, 견실한 매출 및 고객 성장을 지속적으로 입증해야 할 것이다. Veracode의 혁신적인 서비스로서의 보안 오퍼링은 자사의 안정성을 입증할 수 있는 다소간의 여유를 제공하며, 여러 클라우드 서비스 공급업체의 소프트웨어에 대한 제3자 보안 테스트 및 인증과 같은 추가 기회를 제공하고 있다. Veracode는 대안 중의 하나는 대규모 보안/클라우드 서비스 공급업체(예: Google이나 Amazon과 같은 범용 클라우드 서비스 공급업체, 또는 Symantec과 같이 SaaS/클라우드로 거듭나고자 하는 보안 서비스 공급업체)로의 인수를 고려해 볼 수 있다.

- HP와 IBM이 SAST 시장의 메이저 업체와 리더가 되면서, 전체 시장에 대한 실행 및 비전 역량에 대한 기대치가 높아져 Gartner의 2009년 "SAST에 대한 Magic Quadrant" 이래 일부 여타 벤더들의 기대치가 낮아지는 변화를 보였다. Klocwork는 틈새시장 기업 사분면으로 이동하였으며, 도전자로 남아 있었던 Parasoft와 Coverity는 도전자와 틈새시장 기업의 구분선 가까이로 이동하였다. IBM과 HP의 인수는 Klocwork, Coverity 및 Parasoft가 이 시장에서의 실행 및 비전 역량에 있어 IBM과 HP에 도전하는 것을 더욱 더 어렵게 만들었다. 이러한 인수는 또한 Veracode가 자사의 DAST 테스트 기능을 강화하여, 경쟁력을 유지할 지속적인 성장을 입증해야 하는 부담을 안겨 주었다.

Coverity, Klocwork 및 Parasoft의 주된 차이는 그들이 애플리케이션 보안 및 품질 테스트의 통합된 시각을 가져왔고, 주로 품질 테스트에 주력해 왔다는 점이다. 이 세 업체는 자사의 품질/기능 테스트 제품의 기존 고객들에 대한 보안 테스트 제품의 판매에 주력하고 있다. 보안 시장에서, Coverity, Klocwork 및 Parasoft는 정보 보안 전문가들의 관심을 끌기에 부족하고 보안 커뮤니티에서 브랜드 인지도와 영향력이 부족하다는 어려움을 안고 있다. 경쟁력을 유지하기 위해서는 전문적인 소프트웨어 및 하드웨어 벤더 외에도 주류 기업들의 보안 요구사항에 부응하는 역량을 확대하고, 보안 매출 증가에 주력해야 할 것이다. 또한, 강력한 DAST 기능과 SaaS/클라우드 오퍼링으로 관심을 끌어야 하며, 설치 기반 이외의 자사 오퍼링에 대한 매력을 강화해야 할 것이다.

- Klocwork 외에도, Armorize와 GrammaTech 등의 두 틈새시장 기업이 있다. 두 벤더들은 이 Magic Quadrant에 처음이며, 두 기업 모두 다른 방면에서 이 시장에 진입하였다.

Armorize는 SAST와 WAF(Web application firewall) 및 웹 애플리케이션 안티-해커(anti-hacker) 경보 모니터링 기능과 같은 여타 보안 기술을 제공하고 있는 보안 주력 벤더다.

Armorize는 독보적인 보안 벤더를 지향하고 있으나, 현재로서는 회사 인지도가 부족하며 보다 완전한 기술 및 서비스를 갖추지 못해 어려움을 겪고 있다 (예를 들면, DAST 기술과 SAST SaaS/클라우드 서비스를 제공하지 않고 있다).

GrammaTech는 통합 품질/보안 뷰(품질에 주안점을 둔)를 갖춘 벤더다. 이 회사는 방위, 항공전자공학 및 정보 등과 분야의 전문 애플리케이션에 대한 C/C++ 소스 및 바이너리 코드 테스트의 심층 분석을 전문으로 하고 있다. 이 회사는 자사 기술 오퍼링의 범위보다는 깊이에 주안점을 두면서, 그 분야의 고객들을 위한 정적 분석에서 동종 최고 벤더가 되기를 바라고 있다.

- 선구적인 기업(Visionary) 사분면에는 자사의 기술 및 비즈니스에서 사고의 리더십을 보여주고 있는 Checkmarx가 유일하다. 기술적으로, 이 회사는 스캔된 애플리케이션의 정규화된 모델과 그 분석 결과를 영구 리포지토리에 저장함으로써 맞춤형 질의 및 영향 분석을 가능하게 하는 새로운 기술을 ESI에 처음으로 채용하고 있다. 비즈니스 측면에서, Checkmarx는 salesforce.com이라는 신흥 소프트웨어 플랫폼 벤더로 활동영역을 넓혀, salesforce.com, 그 파트너 및 사용자들이 플랫폼으로 업로드 하는 애플리케이션 코드를 분석하고 있다. 클라우드 플랫폼의 보안 문제 해결은 클라우드 플랫폼 공급업체 및 그 사용자들의 우려와 관심이 커지고 있는 부문이다.

시장 정의/설명

SAST는 보안 취약성의 척도가 되는 코딩 및 설계 조건에 대한 애플리케이션 소스 코드, 바이트코드(bytecode) 또는 바이너리를 분석하기 위한 기술이다. 컴파일러와 매우 유사하게, SAST 도구는 애플리케이션의 코드를 행 단위로 분석한 다음, 정보 흐름을 분석하고 잠재적 보안 취약성을 나타내는 조건을 조사한다. 런타임 상태에서 애플리케이션을 분석하는 DAST 도구와는 반대로, 비 런타임 상태로 애플리케이션을 분석할 때 SAST 도구를 사용한다.

애플리케이션 개발 프로세스의 초기에 보안 취약성을 사전에 검출하면 추후 애플리케이션을 실제로 사용하면서 취약성을 개선하는 것에 비해 적은 비용이 소요되며, 애플리케이션과 그 데이터의 전반적인 보안 노출을 줄일 수 있다. 이러한 도구를 통합하려면 개발 프로세스 변경과 문화적인 변화가 필요하기 때문에, SAST 기술과 그 채택이 본격 보급기에 접어들려면 5년 이상이 소요될 것이다.

SAST는 애플리케이션을 개발하거나 구입하는 모든 IT 조직에 의무적인 요구사항이 되어야 한다. 원칙적으로는, 전체 SLC에 걸쳐 애플리케이션 취약성 검출을 실시해야 한다. 애플리케이션 보안 기량 및 리소스가 부족한 기업들은 서비스로서의 애플리케이션 보안 테스트를 고려해 보아야 할 것이다. 오탐 및 미탐은 항상 문제가 된다. 따라서, 기업들은 검출 및 개선 활동이 SLC의 단위 테스트, 빌드 또는 품질 보증(QA) 단계에서 시작되는 고신뢰성, 고심각성 취약성에 우선 주안점을 둘 수 있도록, 도구를 미세 조정해야 할 것이다.

아웃소싱 애플리케이션 개발의 경우, 기업들은 계약의 일부로 외부 서비스 공급업체들이 SAST를 수행하고 테스트를 실시했다는 증거를 제출하도록 요구해야 할 것이다.

엔터프라이즈 클라우드 컴퓨팅을 채택하는 기업과 엔터프라이즈 클라우드 컴퓨팅 서비스 공급업체들은 클라우드로 업로드될 애플리케이션의 SAST와 클라우드 서비스(예: 데이터베이스 또는 애플리케이션 관리 서비스)를 제공하는 소프트웨어의 SAST를 실시해야 한다.

기업들은 자사의 애플리케이션 보안 벤더들에게 ESI 기반 솔루션, 특히 여러 보안 기술 및 정보 상호작용, 통합 및 상관관계를 제공하는 솔루션을 제공할 것을 요구하기 시작해야 한다. 특히, 기업들은 일반적으로 취약성 검출의 범위와 정확도가 더 높은 SAST 및 DAST 기술 상호작용 및 상관관계를 갖춘 솔루션을 모색해야 한다. 또한 기업들은 애플리케이션의 비즈니스 가치나 애플리케이션이 처리하는 콘텐트의 민감성과 같은 상황 정보를 보완할 수 있는, 영구 리포지토리에 SAST, DAST 및 여타 보안 정보를 통합할 수 있는 솔루션을 모색해야 한다. 그러한 리포지토리는 정보 조회 및 분석이 가능한, 예를 들면 SAST 및 DAST 벤더들과 협력하여 SIEM 벤더들이 제공할 수 있는 솔루션이어야 한다.

계약 협상 시에, 기업들은 이 시장의 지속적인 통합을 고려하고 포인트 솔루션이 결국 플랫폼으로 대체되고 발전하고 있는 클라우드 컴퓨팅의 패러다임으로 보완될 것임을 예상해야 한다. 또한 기업들은 서비스로서의 보안이 주류가 될 것임을 예상해야 할 것이다.

SAST를 사용하면 얻을 수 있는 가장 결정적인 효과로 애플리케이션 취약성의 잠재적 악용 위험을 최소화할 수 있다는 점을 들 수 있다. 이 기술을 채택하면 해커가 찾아내기 전에 기업들이 애플리케이션에 내재된 취약성을 검출할 수 있다. 여느 다른 보안 투자와 마찬가지로, 비용 및 위험 분석을 실시해야 한다. SAST의 주목적이 비용 절감이 아니라 위험 저감이기 때문에, 명확한 투자수익율을 산출하기란 어려울 것이다. 조기에 취약성을 발견하면 비용을 절감할 수 있지만, 이 또한 SAST 채택에 필요한 프로세스 변경 및 문화적 변경 비용에 대하여 비교 평가해야 한다. 장기적으로는, 보안 테스트 자동화 및 서비스로서의 보안 테스트 조달 등에서 또 다른 비용 절감이 이루어질 수 있을 것이다.

포함 및 배제 기준

이 Magic Quadrant에 대하여, 우리는 다음과 같은 포함 및 배제 기준을 설정하였다:

- 벤더들은 SAST 보안 테스트 제품이나 서비스, 또는 이상적으로 두 가지 모두를 제공해야 한다.
- 벤더들은 시장에 진출한지 18개월 이상이 되어야 한다.
- 벤더의 매출은 1,000,000 달러를 상회하거나 자사 제품/서비스를 배치하여 실운영 중인 고객 수가 최소 20개 이상이어야 한다.
- 신생 벤더들은 입증된 자금 확보 능력을 갖추고 있어야 하며, 최소 12개월의 영업준비금을 보유하고 있어야 한다.
- 오픈소스 SAST 오퍼링은 본 Magic Quadrant에 고려되지 않았다. 현재, 상용 오퍼링에 비하여 엔터프라이즈급 기능이 훨씬 뒤처져 있다.

추가

- Armorize Technologies
- Checkmarx
- GrammaTech

제외

- SAST 시장에서 철수를 결정한 Compuware.
- 본 Magic Quadrant에 관하여 조사 중이던 2010년에 HP에 인수된 Fortify. 본 조사에서 우리는 Fortify와 HP를 한 회사인 HP로 취급하고 있다.
- 비록 Visual Studio로 아주 기초적인 SAST 기능을 제공하고 있지만 상용 오퍼링에서는 경쟁력이 없으며 그러한 기능에 대하여 자사 고객들에게 제3자 생태계를 소개하는 Microsoft.
- 2009년 IBM에 인수된 Ounce Labs.

평가 기준

실행 능력

제품/서비스: 이는 SAST 시장에서 경쟁하는 벤더의 핵심 제품 및 서비스다. 여기에는 현용 제품/서비스 기능, 품질 및 특정 등이 포함된다. 우리는 경쟁력 평가에 있어 입증된 성능, SAST 매출 규모, SAST 고객 수와, 설치 사용 SAST 제품의 수, SLC 제품 설치 기반 이외에 대한 매력, 폭넓은 사용자(예: 프로그래머, QA/테스트 전문가)에 대한 매력, 정보 보안 전문가에 대한 매력, SAST 이외의 기술(애플리케이션 보안 여부와 무관)에 대한 매력, 제공 중인 제품과 SaaS/클라우드 서비스 등에 높은 점수를 부여하고 있다.

또한 벤더들의 제품 시장점유율과 "마인드 셰어(mind share)"도 평가한다.

전반적인 실행 가능성 (비즈니스 단위, 재무, 전략, 조직): 이는 조직 또는 비즈니스 단위의 전반적인 재무건전성, 회사가 SAST 오퍼링과 보다 광범위한 애플리케이션 보안 분야에 지속적인 투자를 할 가능성, SAST 전문지식, 벤더가 인수/제휴 거래에 성공을 거둘 가능성 등에 대한 평가다.

영업 활동/가격 책정: 우리는 SAST 성장률, 회사의 글로벌 리치(global reach), 가격 모델, 제품/서비스/지원 번들링 등을 감안한다. 또한 벤더의 모든 판매 전 활동 역량과 그 활동을 뒷받침하는 조직의 역량을 검토한다. 여기에는 거래 관리, 가격 및 협상, 판매 전 지원, 전세계 판매 채널의 전반적인 효과성 등이 포함된다.

시장 대응성 및 실적: 우리는 기회가 나타나고, 경쟁사들이 움직이며, 고객들의 요구사항이 발전하고 시장 역학이 변화하면서 벤더가 대응하고, 방향을 전환하고, 유연해지며, 경쟁에서 이길 수 있는 능력을 조사한다. 또한, 시장 인지도, 보안 전문가들 간의 벤더의 평판과 영향력, 기업의 기능 요구사항에 대한 벤더의 SAST (및 보다 광범위한 애플리케이션 보안) 오퍼링의 일치 여부, 시장이 요구할 때 새로운 혁신적인 기능을 제공한 벤더의 실적 등을 평가한다.

고객 경험: 이는 실운영 환경에서의 제품의 기능에 대한 평가다. 평가에는 배치, 운영, 관리의 편의성, 안정성, 확장성 및 벤더 지원 역량이 포함된다. 또한 고객이 평가 대상 제품으로 성공을 거둘 수 있는 관계, 제품 및 서비스/프로그램 등이 포함된다. 특히, 여기에는 고객이 기술 지원을 받는 방식과, 고객과 협력하여 제품이나 서비스를 커스터마이징하고, 고객이 요청한 특정 기능을 개발하며, 개인화된 고객 지원을 제공하려는 벤더의 의지가 포함된다 (표 1 참조).

표 1. 실행 능력 평가 기준

평가 기준	가중치
제품/서비스	높음
전반적인 실행 가능성 (비즈니스 단위, 재무, 전략, 조직)	높음
영업 활동/가격 책정	표준
시장 대응성과 실적	높음
마케팅 활동	채점 안함
고객 경험	표준
운영	채점 안함
출처: Gartner (2010년 12월)	

비전의 완전성

시장 이해도: 우리는 벤더가 고객들의 요구사항을 이해하여 이를 제품과 서비스로 전환할 수 있는 능력을 평가한다. 시장 이해도에서 최고 등급을 보인 SAST 벤더들은 다음과 같은 분야에서 고객의 요구사항에 적응하고 있다: SAST에 대하여 고객이 필요로 하는 대부분의 기능을 결합하는 단일 도구 제공, SAST를 뛰어넘는 애플리케이션 보안 기술 범위의 포괄성, SAST 외에 DAST의 제공, SAST가 다루는 엔터프라이즈급 범위의 프로그래밍 언어 (일명 "커버되는" 프로그래밍 언어), 여러 보편적인 SLC 플랫폼과의 SAST 도구 본연의 통합 편의성, 전사적 통합, 분석, 보고 및 규칙 관리, 가장 심각한 고신뢰성 취약성에 주력할 수 있는 사용자 친화적인 편의성, 서비스로서의 보안 및 클라우드 전달, 제공중인 제품 및 서비스.

마케팅 전략: 전사적으로 일관성 있게 전달되고 웹사이트, 광고, 고객 프로그램 및 포지셔닝 선언(positioning statement) 등을 통해 구체화되는, 명확하고 차별화된 일련의 메시지. 우리는 보안 시장에 대한 헌신을 명시하고, 자사의 소구 대상을 명확하게 정의하며, 적절한 제품/서비스의 패키지를 판매하는 벤더들에게 높은 점수를 부여한다.

오퍼링 (제품) 전략: 제품 개발 및 전달에 대한 벤더들의 접근방식을 평가한다. 이는 보안 분석에 대한 벤더의 주안점, 최첨단(즉, Type A) 기업의 요구사항 충족과 Type B 및 Type C 기업의 요구사항 충족 간에 적절한 균형, 일반적인 기업의 요구사항 충족과 특수 고객(예: 하드웨어 벤더 및 임베디드 애플리케이션 벤더)의 요구사항 충족 간에 적절한 균형 등을 다룬다.

혁신: 이 항목에서, 우리는 중요한 고객 요구사항을 독자적으로 다루는 방식으로 벤더가 경쟁 제품과 차별화된 솔루션을 개발하고 공급하는지를 평가한다. 우리는 ESI를 가능하게 하여, 보안 커버리지의 범위와 정확도를 높이고, 고급 분석, 상황 평가 및 최적의 보안과 전사적인 위험 관리 의사결정을 위한 지원을 가능하게 하는 벤더들에게 높은 점수를 부여한다. 또한, 보안 코드 테스트를 보다 정확하게 만드는 (예를 들면, 오탐 및 미탐 비를 줄이는) 방법을 개발하는 벤더들에게 높은 점수를 부여한다. SAST 외에 DAST와 SAST 및 DAST의 상호작용 및 상관관계, 바이너리 코드 분석, 애플리케이션 보호 기능 (예: WAF와 유사한 기능), 거버넌스, 위험 및 컴플라이언스(GRC)와 SIEM 기술의 통합, 혁신적인 전달 방식 (예: 서비스로서의 보안 테스트 및 클라우드 컴퓨팅), 클라우드 플랫폼을 위한 SAST, 모바일 플랫폼을 위한 SAST 등을 제공하는 벤더들에게 높은 점수를 부여한다 (표 2 참조).

표 2. 비전의 완전성 평가 기준

평가 기준	가중치
시장 이해도	높음
마케팅 전략	표준
영업 전략	채점 안함
오퍼링 (제품) 전략	높음
비즈니스 모델	채점 안함
수직/산업 전략	채점 안함
혁신	높음
지리적 전략	채점 안함
출처: Gartner (2010년 12월)	

리더 기업

리더 기업은 실행 및 비전의 균형 잡힌 진보를 보여준다. 그들의 행동으로 인해 시장의 모든 벤더 및 솔루션에 대한 경쟁 기준의 수준이 높아지며, 리더 기업은 업계의 선두를 달리는 경향이 있다. 리더 기업의 전략은 애플리케이션의 보안에 주안점을 두며, 그 오퍼링은 SLC 내의 애플리케이션 보안 전문가들의 요구사항에 부응하고, 그 브랜드는 애플리케이션 보안 부문에 널리 인식되어 있다. 리더 기업들은 SAST 기능을 초월하여 보다 광범위한 애플리케이션 보안 규범을 포함하고 있다. 동시에, 리더 기업들은 이 발전하는 시장에서 비교적 대규모 고객 및 매출을 확보할 수 있다. 일류 벤더들이 모든 고객들의 기본적인 선택은 아니며, 반드시 리더 기업으로부터 구입하는 것이 당연하다고 여기지 않아야 한다. 일부 고객들의 경우에는 다른 사분면의 벤더가 자사 특유의 요구사항을 더 잘 다룰 수도 있을 것이다.

도전자 기업

도전자 기업은 일반적으로 애플리케이션 품질 테스트 분야에서 애플리케이션 보안 분야로 진출하였으며, 품질 및 보안에 대하여 통합된 시각을 가지고 있다. 애플리케이션 품질에 주력하며, 반면에 보안은 부차적인 우선순위다 (그러나 중요성이 커지고 있다). 도전자 기업들은 자사의 "애플리케이션 품질" 고객에게 애플리케이션 보안을 판매할 수 있지만, 설치 기반을 벗어나면 보안 브랜드 인지도 문제에 부딪히게 된다. 도전자 기업들은 사용자들의 일반적인 요구사항에 부응하는 견실한 제품을 보유하고 있다. 그들은 광범위한 애플리케이션 보안 제품 및 서비스와 고급 기능보다는 기본적이며, "만족스러운" 기능의 경쟁에 앞서 있다. 한정된 문제의 해결에는 도전자 기업들이 효율적이면서도 편리한 선택안이 될 수 있다.

선구적인 기업

선구적인 기업은 차세대 제품에 중요한 역할을 하게 될 최첨단/"동종 최고"의 기능에 투자하며, 구매자들이 보다 우수한 보안 확실성을 조기에 접할 기회를 제공한다. 선구적인 기업은 시장의 기술 개발 과정에 영향을 미칠 수 있지만, 시장 리더에 비해 자신들의 비전을 실행할 수 있는 능력이 부족하다. 기업들은 동종 최고의 기능을 갖추기 위해 일반적으로 선구적인 기업을 선택한다. 여타 벤더들은 선구적인 기업을 혁신의 지표와 사고의 리더십으로 지켜보면서, 그들의 기술을 모방하거나 이러한 벤더를 인수하려는 시도를 한다.

틈새시장 기업

틈새시장 기업들은 특정 구매자들의 요구사항에 부응하는 실행 가능하며 신뢰할 만한 솔루션을 제공한다. 틈새시장 기업들이 최종후보자 명단에 들어갈 가능성은 적지만, 자사의 주력 부문에 일치하는 비즈니스 사례 및 기술 사례에 대하여 고려될 경우에는 가능성이 매우 높다. 틈새시장 기업들은 전체 시장의 부분을 다룰 수 있을 것이며, 종종 리더들보다 훨씬 효율적으로 다룰 수 있다. 기업들은 어느 정도 중요한 기능이나 특정 벤더의 전문지식에 주안점을 두거나 그 벤더와 관계를 맺고 있는 경우에 틈새시장 기업들을 선택하는 경향이 있다.

벤더별 강점과 유의사항

Armorize Technologies

강점

- 보안에 상당히 주력하고 있다. 특히, 웹 애플리케이션의 정적 코드 분석에 주력하고 있다.
- 웹 애플리케이션 개발에 널리 쓰이는 동적 프로그래밍 언어인 Hypertext Preprocessor(PHP)를 분석한다 (이 언어를 제공하는 유일한 다른 벤더들이 시장 리더들이다).
- SAST를 포함한 일련의 오퍼링을 제공하고 있지만, 그 폭을 넓히고 있다. SAST 도구 외에도 Armorize는 WAF와 멀웨어 경보 및 모니터링 서비스를 제공하고 있다.
- 자사의 원래 SAST 오퍼링은 어플라이언스 기반이었지만, Armorize는 현재 사내 라이센스 소프트웨어를 통해 SAST 을 제공하고 있다.
- Armorize는 Coverity와 제휴하여, 품질 및 보안 기능 결합 세트를 제공하기 시작하였다.
- Armorize는 아시아 태평양 지역에 강력한 프레즌스를 가지고 있으며, 유럽 및 미국에서의 프레즌스 강화에 몰두하여 왔다.
- Armorize 고객들은 자사 SAST 기술 평가 시에 오탐 비율이 낮다고 전한다.

유의사항

- Armorize는 소규모의 벤처캐피탈 지원 벤더다.
- Armorize는 DAST 오퍼링이 없으며, 결합 SAST/DAST 오퍼링 또는 SAST/DAST 상호작용/상관관계를 위한 제휴를 하지 않는다.
- Armorize는 SAST SaaS/클라우드 오퍼링이 없다.
- Armorize는 시장 영향력과 기업의 정보 보안 전문가들 사이에서 회사 및 브랜드 인지도가 부족하다.
- Armorize의 Coverity와의 제휴는 아직 그 결과를 지켜보아야 한다.
- Armorize는 Java, C#, VB.NET 및 PHP 등의 분석 프로그래밍 언어로 범위가 한정되어 있다.

Checkmarx

강점

- Checkmarx는 분석된 소스 코드를 영구 스토리지에 저장되는 단일 공통 언어 모델로 변환하여, 반복 질의 및 영향 분석을 가능하게 한다. 애플리케이션을 변경하지 않은 경우, 추가 애플리케이션 테스트를 실시할 필요가 없다. 새로운 공격의 패턴으로 질의를 수정하면, 새로운 공격에 대한 취약성에 대하여 애플리케이션을 간단하게 테스트할 수 있다.
- Checkmarx는 비교적 광범위한 지원 언어를 제공하고 있다. Apex(salesforce.com이 사용), Java, C#, VB.NET 및 VB6로 작성된 코드를 분석하며, 아울러, 가용성이 제한적인 C 및 C++ 분석을 위한 애플리케이션을 보유하고 있다 (2010년 말에 정식 출시 예정).
- Checkmarx는 서비스로서의 보안 테스트/클라우드 비즈니스 모델을 주로 제공하고 있으며, 제품 라이센스도 제공하고 있다.

유의사항

- Checkmarx는 소규모의 벤처캐피탈 지원 벤더다.
- Checkmarx는 시장 영향력과, 기업의 정보 보안 전문가들 사이에서 회사 및 브랜드 인지도가 부족하다.
- Checkmarx는 DAST 제품 또는 서비스가 없으며, SAST/DAST 결합 오퍼링 또는 SAST/DAST 상호작용/상관관계를 위해 DAST 벤더들과 제휴를 하지 않는다.
- 지원하는 분석 언어가 시장 리더들에 비해 적다.

Coverity

강점

- Coverity는 품질 및 보안 문제에 대하여 애플리케이션을 테스트한다.
- Coverity는 전문 소프트웨어 및 하드웨어 벤더들과 하드웨어 임베디드 애플리케이션에 대한 정적 코드 분석의 입증된 공급자다.
- Coverity는 런타임 시에 애플리케이션을 장애를 유발할 수 있는 멀티스레드 Java 애플리케이션의 레이스(race) 조건과 데드록(deadlock)을 검출하고, 애플리케이션 전반에 걸쳐 감염된 데이터 흐름을 추적하는 동적 스레드 분석 도구를 제공한다.
- Coverity는 Armorize와의 제휴 하에, 보고 및 분석을 위해 Coverity 도구의 품질 및 보안 테스트 결과를 Armorize의 보안 테스트 결과와 통합하고 있다.
- Coverity의 영업 및 마케팅은 북미를 벗어나 유럽 및 아시아 태평양지역으로 확대되고 있다.

유의사항

- Coverity는 애플리케이션 품질에 주력하고 있고 애플리케이션 보안은 주력 분야가 아니며 Armorize와의 제휴로 보완하고 있다.
- Coverity는 DAST 제품이나 서비스가 없으며 SAST 및 DAST 결합 오퍼링 또는 SAST 및 DAST 상호작용/상관관계를 위해 DAST 벤더들과 제휴를 하지 않는다.
- Coverity는 SaaS/클라우드 오퍼링이 없다.
- Coverity의 Armorize와의 제휴는 아직 그 결과를 지켜봐야 한다.
- Coverity가 지원하는 분석 프로그래밍 언어가 적다: C, C++, Java 및 C#.
- Coverity는 시장 영향력과 기업의 정보 보안 전문가들 사이에서 회사 및 브랜드 인지도가 부족하다.

GrammaTech

강점

- GrammaTech는 품질 및 보안에 대하여 통합된 관점을 지니고 있다.
- 항공우주 및 방위 산업의 소프트웨어 엔지니어들에게서 철저한 정적 분석에 대한 견실한 평판을 얻고 있다.
- 소스 코드 분석 외에도 바이너리 코드 분석을 실시한다 (Veracode는 진정한 바이너리 코드 분석을 제공하는 유일한 또 다른 벤더다).
- GrammaTech는 미국 및 캐나다에 직접 판매망을 갖추고 있다. 유럽과 아시아 태평양지역에는 대리점 망을 갖추고 있다.

유의사항

- GrammaTech는 보안 분야에 그다지 주안점을 두지 않는다. SQL 주입 및 XSS(cross-site scripting)과 같이 매우 심각한 취약성을 검사하지 않는다.
- 지원하는 분석 언어가 C 및 C++ 만으로 적다 (비록 소스 코드 분석과 바이너리 코드 분석을 실시하지만).
- Java 및 .NET 언어를 지원하지 않으며, 대부분의 엔터프라이즈 애플리케이션에 쓰이고 있는 Java 및 .NET 언어를 조만간 추가할 계획도 없다.
- GrammaTech는 기본적인 엔터프라이즈급 통합 및 보고 기능을 갖추고 있다.
- SaaS/클라우드 오퍼링이 없다.
- DAST 제품이나 서비스가 없으며, SAST/DAST 결합 오퍼링 또는 SAST/DAST 상호작용/상관관계를 위해 DAST 벤더들과 제휴를 하지 않는다.
- GrammaTech는 시장 영향력과 기업의 정보 보안 전문가들 사이에서 회사 및 브랜드 인지도가 부족하다.

HP (Fortify Software)

강점

- HP는 Gartner의 2009년 "SAST에 대한 Magic Quadrant"에서 선두 벤더였던 Fortify Software를 인수한 결과 리더 사분면으로 이동하였다. HP의 원래 SAST 제품인 DevInspect는 매각되었다. Fortify의 일련의 애플리케이션 보안 제품들은 HP의 SAST 플래그십이 되었다.
- SAST 외에도 HP Fortify 360은 애플리케이션 내에 상주하여 취약한 곳을 보호하고 애플리케이션 활동에 관한 보고와 모니터링도 가능한 일종의 "소프트웨어 방화벽"인 런타임 애플리케이션 보호 기술(RTA[Real-Time Analyzer])을 제공한다.
- HP Fortify 360은 또한 취약성 검출의 정확도를 높이는 기술(PTA[Program Trace Analyzer])도 제공하며, 이로써 테스터들은 일례로, 애플리케이션에 악의적인 데이터를 동적으로 입력하고 악의적인 데이터 및 로직 흐름을 관찰하여 애플리케이션의 보안 통제를 분석하고 추가/다른 통제의 필요성 여부를 파악할 수 있다.
- HP Fortify 360 기술은 단일 스튜디오로 통합되어 있지만, HP의 DAST 기술은 여전히 별개의 오퍼링으로 판매되고 있다.
- HP Fortify 360은 가장 광범위한 프로그래밍 언어를 지원한다: C, C++, Java, C#, VB.NET, COBOL, ColdFusion, Transact-SQL, PL/SQL, VB6, PHP 및 Python.
- HP Fortify 360 기술은 HP, IBM 및 Microsoft 등의 것과 같이 가장 널리 쓰이고 있는 SLC 플랫폼에 통합되어 있다.
- HP Fortify 360은 SAST 시장에서 마인드 셰어(mind share) 및 시장 점유율 리더로 인정되고 있다.
- HP Fortify 360은 미국, 유럽 및 아시아 태평양지역의 고객 등 대규모의 세계적인 SAST 설치 기반을 보유하고 있다.
- 2009년 이후로, HP와 Fortify는 SAST/DAST 상호작용 및 상관관계 기능을 제공하고 발전시켜 왔다. 이 오퍼링은 여전히 제공되고 있으며 앞으로도 끊임없이 성숙하고 한층 강화될 것으로 예측된다.

- HP Fortify 360 기술은 SaaS/클라우드 전달 모델로 제공되고 있다.

유의사항

- HP는 Fortify 팀과의 문화적 차이를 해결하고 Fortify를 HP 조직에 통합해야 한다.
- 여타 DAST 공급업체와 Fortify의 제휴가 단계적으로 철회되고 HP의 DAST 기술로 대체될 것으로 보인다.
- HP는 HP Quality Center 기술과 Fortify의 오퍼링을 포함한 보안 테스트 기술의 통합에 대한 로드맵을 제시해야 한다.
- HP는 자사의 SAST/DAST 기술 상호작용의 향후 발전에 대한 로드맵을 제시해야 한다.
- HP Fortify 360은 그 가격 모델이 일반적으로 도구를 사용할 개발자를 요하므로, 모든 SAST 벤더 중에서 가장 많은 비용이 소요되는 경향이 있다.
- HP는 품질 테스트 분야(테스트/QA 단계에서는 DAST를 주로 사용)에 대규모의 설치 기반을 보유하고 있지만, SAST 테스트가 주로 사용되는 SLC에는 대규모 설치 기반이 없다.
- 일부 고객들은 Fortify의 공격적인 판매 방식과 라이센싱 관행에 불만을 표시하였다. HP의 인수 이후에는 어떤 방식으로 변화할 지에 대해서는 분명하지 않다.
- 소프트웨어 업데이트에 대한 유지보수비 외에도 Fortify는 지속적인 언어 취약성 업데이트에 대하여 별도 비용을 청구하고 있다. Fortify는 지속적인 언어 팩 업데이트에 대하여 별도로 비용을 청구하는 유일한 벤더다. HP의 인수 이후에는 어떤 방식으로 변화할 지에 대해서는 분명하지 않다.
  .

IBM

강점

- IBM은 SAST 및 DAST 기술을 제공하고 있다.
- IBM Rational은 SAST 및 DAST 스캔 결과를 상관시키는 AppScan Reporting Console을 제공한다.
- IBM은 자사의 SLC 설치 기반을 활용하여, SAST 및 DAST 도구를 통합하고 Rational 및 Eclipse 플랫폼 고객들에게 판매하기에 매우 유리한 입장에 있다.
- IBM은 데이터 마스킹 및 데이터베이스 활동 모니터링 기술을 (인수를 통해) 추가 함으로써, 보다 광범위한 애플리케이션 보안의 비전을 보여주었다. 이러한 기술들은 SAST 또는 DAST 제품의 일부가 아니며, 오히려 보다 광범위한 애플리케이션 보안 포트폴리오의 일부다.
- IBM은 뛰어난 영업력, 글로벌 서비스 조직 및 세계적인 제휴 네트워크를 갖춘, 세계 최대 다국적 기업이다.
- IBM은 잠재적으로 손상된 데이터 소스를 확인하고 애플리케이션 전반에 걸쳐 그 흐름을 추적하는 혁신적인 스트링 감염 분석(taint analysis)을 제공하고 있다.
- 고객들은 IBM의 가격이 가장 유사한 경쟁사인 HP/Fortify에 비해 합리적이라고 판단하고 있다.
- IBM은 상당한 종류의 분석 프로그래밍 언어를 지원한다: Java, C, C++, C#, VB.NET, VB6, PHP, Perl 및 ColdFusion.

유의사항

- IBM Global Services가 제공하고 있는 애플리케이션 보안 테스트/침입 테스트에 대한 매니지드 서비스와 중복되고 고객에 혼동을 줄 가능성이 있다.
- IBM이 SAST 및 DAST 상호작용에 관한 연구에 착수하였지만, 아직 마무리되지 않았다.
- IBM이 지원하는 프로그래밍 언어가 HP에 비해 적다.

Klocwork

강점

- Klocwork는 애플리케이션의 품질 및 보안 문제에 대한 테스트를 실시한다.
- Klocwork는 하드웨어 벤더 및 하드웨어 임베디드 애플리케이션에 대한 정적 코드 분석의 입증된 공급업체다.
- Klocwork는 모바일 디바이스, 소비자 가전, 의료, 통신, 군사 및 항공우주 분야의 전문 소프트웨어 엔지니어링 시장에서 입증된 공급업체다.

유의사항

- Klocwork는 시장 영향력과, 기업의 정보 보안 전문가들 사이에서 회사 및 브랜드 인지도가 부족하다.
- Klocwork는 일반적인 기업의 SAST(및 광범위한 애플리케이션 보안) 요구사항(소프트웨어 엔지니어링 고객들의 요구사항과 정반대인)을 충족함에 있어 뒤처져 있다.
- Klocwork는 DAST 기술을 제공하지 않으며, DAST 테스트와 SAST/DAST 간의 상호작용/상관관계를 위해 DAST 벤더들과 제휴를 맺지 않고 있다.

- Klocwork는 SaaS/클라우드 서비스를 제공하지 않는다.
- 임베디드 시스템에 주력하고 있기 때문에 Klocwork가 지원하는 분석 프로그래밍 언어가 적다: C, C++, Java 및 C#.

Parasoft

강점

- Parasoft는 애플리케이션의 품질 및 보안 문제에 대한 테스트를 실시한다.
- Parasoft는 SAST 및 DAST 솔루션을 제공하고 있으며, SAST 및 DAST 분석을 상관시키는 기능을 갖추고 있다.
- Parasoft는 기능 테스트, 부하 테스트, 프로토콜 테스트 및 협업 코드 검토를 위한 일련의 도구를 제공한다.
- Parasoft가 지원하는 언어는 비교적 많다: C, C++, Java, C# 및 VB.NET.
- Parasoft는 20년 이상 이 시장에 몸담아 왔으며, 인터페이스 테스트 벤더로서 그 신뢰성을 입증하였다.
- 2009년, Parasoft는 특히 보안 테스트 전문가를 대상으로 한 보안 테스트 오퍼링을 출시하였다.
- Parasoft는 자체 자금으로 설립된 개인 기업이며, 수익성이 있는 기업으로 알려지고 있다.
- 지리적으로 Parasoft의 영업 및 마케팅 지역은 북미를 벗어나 유럽 및 아시아 태평양 지역까지 도달하였다.

유의사항

- Parasoft는 시장 영향력과 기업의 정보 보안 전문가들 사이에서 회사 및 브랜드 인지도가 부족하다.
- Parasoft는 애플리케이션 보안 보다는 애플리케이션 품질에 주안점을 두고 있다.
- 보안 분야에서 Fortify (현 HP) 및 Veracode와 같은 신생 벤더들이 단 몇 년 내로 달성했던 고속 성장을 Parasoft는 보여주지 못했다.
- Parasoft가 DAST 기능을 제공하고 있지만, DAST 공급업체로서의 Parasoft는 SAST와 SAST 및 DAST의 상호작용을 제공하고 있는 DAST 시장 리더인 IBM과 HP에 한참 뒤쳐져 있다.
- Parasoft는 서비스로서의 SAST 보안 테스트/클라우드를 제공하지 않고 있다.
- Parasoft가 지원하는 분석 언어는 시장 리더들에 비해 적은 편이다.

Veracode

강점

- Veracode는 애플리케이션 보안에 주력하고 있으며, SAST 및 DAST 기술을 제공하고 있다.
- Veracode는 서비스로서의 보안 테스트 비즈니스 모델을 최초로 선보였으며, 이 분야에 혁신을 일으켰다.
- Veracode의 SaaS/클라우드 모델은 자체적인 애플리케이션 보안 테스트를 실시하기에는 애플리케이션 보안 기량과 리소스가 부족한 기업, 다수의 테스트 애플리케이션으로 신속하게 확장할 필요가 있는 기업과 애플리케이션 개발 및 테스트 프로세스가 지리적으로 분산되어 있는 기업들에게 매력적일 것이다.
- Veracode는 Magic Quadrant에서 C/C++용 원시 바이너리 코드의 SAST에 대한 상용 구현을 제공하는 유일한 두 벤더 중의 하나다 (나머지 하나는 GrammaTech). 일부 다른 벤더들은 Java 및 .NET 애플리케이션에 대한 바이트코드 분석만을 제공하고 있다.
- SAST 기술은 항상 Veracode의 소유였던 반면에, DAST 기술은 NT Objectives로부터 라이센스를 취득하였다. 2011년 초에 Veracode는 라이센스 DAST 기술을 자사 내부적으로 개발한 DAST 기술로 대체할 예정이며, 이는 Veracode의 플랫폼에 자연스럽게 통합될 것이다.
- Veracode의 전문가들이 자동 분석 결과를 고객에게 전송하기 전에 검토하므로 오탐의 수를 줄인다.
- Veracode는 특히 ISV 소프트웨어(예: 패키지/재고 상용품) 및 클라우드 소프트웨어 테스트를 위한 제3자 독립 소프트웨어 테스트 서비스를 제공하고 있다. Veracode는 테스트를 통과한 소프트웨어에 대하여 자사의 "검증(VERAFIED)" 인증서를 발급한다.
- Veracode는 Windows Mobile 및 BlackBerry 모바일 플랫폼에 대한 지원을 제공하고 있다.
- Veracode는 자사의 분석 결과(와 일부 애플리케이션 관련 비즈니스 맥락)를 질의가 가능한 영구 리포지토리에 저장한다. 애플리케이션이 변경되지 않은 경우, 질의를 위해 추가 애플리케이션 테스트를 실시할 필요가 없다. 하지만, 고객들이 테스트된 애플리케이션 모델을 조회할 수 없다.
- Veracode는 EMC의 보안 사업 부문인 RSA의 GRC system Archer와의 통합 기능을 갖추고 있으며, 이는 애플리케이션 위험 콘텐트를 Archer SmartSuite Framework로 제공하여 Veracode 및 Archer 고객들의 GRC 프로세스 관리를 지원한다.

- Veracode는 가상 머신 컨테이너 내에 캡슐화된 바이너리를 분석할 수 있다.
- 고객의 보안 및 프라이버시를 보장하기 위해, Veracode는 자사 서비스를 자사 내에 호스팅하지 않고, SAS 70 Type II 호스팅 시설에 호스팅하며 보안 및 기밀성에 대하여 Ernst & Young이 매년 실시하는 독립적인 SysTrust Certification을 받고 있다.
- Veracode는 고객들이 Veracode 원격 테스트 결과를 고객의 사내 통합 개발 환경, 빌드 시스템 및 버그 추적 시스템에 통합할 수 있는 API와 플러그인을 제공한다.
- Veracode는 다음 프로그래밍 언어의 분석을 지원한다: Java, C, C++, C#, VB.NET, PHP 및 ColdFusion (Java로 컴파일된).

유의사항

- Veracode는 소규모의 벤처캐피탈 지원 신생 벤더다.
- Veracode는 퓨어 플레이(pure-paly) 애플리케이션 보안 테스트 서비스 공급업체다. 일반적으로 제품으로 자사 기술을 판매하지 않는다 (하지만 한가지 예외로, 정보 커뮤니티의 정부 고객을 위한 사내 서비스를 구현하였다). 다른 리더들은 자사의 기술을 제품 및 서비스로 판매하여, 어느 한 가지나 두 가지 모두를 원하는 고객들의 요구사항을 충족하고 있다.
- 테스트를 위해서는 고객들의 바이트/바이너리 코드를 Veracode의 테스트 사이트로 업로드해야 한다. Veracode는 자사 서비스의 유일한 공급업체이며, 즉 일반적인 오퍼링으로서 일부 기업의 사내에 설치하여 기업 스스로 실행할 수 있는 "사설" Veracode 기능이 없다.

일부 기업들은 자사의 민감한 소프트웨어 자산과 정보에 접근할 수 있는 Veracode와 같은 외부 엔티티를 원하지 않을 수도 있다. 코드(소스 코드가 아닐지라도)를 보여주는 것은 일부 기업들에게 민감한 사안이 될 수 있다.

- Veracode의 검출 기능은 언어, 플랫폼, 칩셋 및 OS 특유의 기능이며, 따라서 플랫폼 상의 모든 바이너리를 지원하는 것은 아니다.
- NT Objectives의 기술을 대체하는, Veracode가 내부적으로 개발한 DAST 기술은 아직 입증되지 않았다.
- Veracode SAST 및 DAST 상호작용 기능은 2010년 말로 예정되어 있다.
- Veracode는 자사 클라우드 플랫폼 상에서 원격으로 애플리케이션을 테스트하여, 검출된 취약성에 관한 중앙집중식 보고를 제공하지만, 고객들은 자사 현장에서 각각의 취약성 개선 작업을 수행한다. 따라서, Veracode의 고객들은 Veracode 보고를 자사의 애플리케이션 개선 시스템에 통합하는 프로세스를 갖추어야 한다.
- Veracode가 지원하는 분석 프로그래밍 언어가 다른 시장 리더들에 비해 적다.

벤더의 추가 또는 제외

우리는 시장 변화에 따라 Magic Quadrant 및 MarketScope에 대한 우리의 포함 기준을 검토하여 조정하고 있다. 이러한 조정의 결과로, 여느 Magic Quadrant 또는 MarketScope의 벤더 조합이 시간이 지나면서 바뀔 수 있다. 어느 해에 어느 Magic Quadrant 또는 MarketScope에 나타난 벤더가 그 다음 해에 반드시 나타나지 않는 것은 우리가 그 벤더에 대한 판단을 바꾸었다는 것을 의미한다. 이는 시장 변화로 인하여 평가 기준이 변경되었거나 벤더의 주력분야가 바뀐 것이 반영된 결과일 수 있다.

평가 기준의 정의

실행 능력

제품/서비스: 정의된 시장에서 경쟁/종사하고 있는 벤더가 제공하는 핵심 제품 및 서비스. 여기에는 시장 정의에 정의되어 있고 그 하위기준에 상술되어 있는 바와 같이, 본연 또는 OEM 계약/제휴를 통해 제공하는 현용 제품/서비스 기능, 품질, 일련의 기능 및 기술 등이 포함된다.

전반적인 실행 가능성 (비즈니스 단위, 재무, 전략, 조직): 실행 가능성에는 조직 전반의 재무건전성, 비즈니스 단위의 재무 및 실무 성과, 개별 사업 단위가 제품에 지속적인 투자를 하고 지속적으로 제품을 공급하며 조직의 제품 포트폴리오를 첨단 기술로 발전시킬 가능성에 대한 평가가 포함된다.

영업 활동/가격 책정: 벤더의 모든 판매 전 활동 역량과 그 활동을 뒷받침하는 조직. 여기에는 거래 관리, 가격 책정 및 협상, 판매 전 지원 및 영업 채널의 전반적인 효과성이 포함된다.

시장 대응성과 실적: 기회가 발생하고, 경쟁사들이 움직이며, 고객들의 요구사항이 발전하고 시장 역학이 변하면서, 벤더가 대응하고, 방향을 전환하고, 유연해지며, 경쟁에서 성과를 올릴 수 있는 능력. 이 기준은 벤더의 대응 이력도 고려한다.

마케팅 활동: 시장에 영향을 미치고, 브랜드 및 회사를 홍보하며, 제품에 대한 인지도를 제고하며, 구매자들의 생각에 제품/브랜드 및 기업에 대한 긍정적인 인식을 심어주는 기업의 메시지를 전달하기 위한 프로그램의 명확성, 품질, 창의성 및 유효성. 광고, 홍보 이니셔티브, 사고의 리더십, 입 소문 및 영업 활동을 조합하면 이 "마인드 셰어(mind share)"를 높일 수 있다.

고객 경험: 고객이 평가 대상 제품으로 성공을 거둘 수 있는 관계, 제품 및 서비스/프로그램 등이 포함된다. 특히, 여기에는 고객이 기술 지원 또는 계정 지원을 받는 방식이 포함된다. 또한, 보조 도구, 고객 지원 프로그램(과 그 품질), 사용자 그룹의 가용성, 기본 계약 등이 포함될 수 있다.

운영: 기업이 자사의 목표와 의무를 충족할 수 있는 능력. 여기에는 기량, 경험, 프로그램, 시스템과 기업이 지속적으로 효과적이며 효율적인 운영을 지속할 수 있게 하는 여타 매개체 등을 포함한 기업 조직의 품질이 포함된다.

비전의 완전성

시장 이해도: 벤더가 구매자들이 원하고 필요로 하는 것을 이해하여 이를 제품 서비스로 전환하는 능력. 최고의 비전을 보여주는 벤더들은 구매자들이 원하고 필요로 하는 것에 귀를 기울이고 이해하여 추가적인 비전으로 이를 구체화하거나 강화할 수 있다.

마케팅 전략: 전사적으로 일관성 있게 전달되고 웹사이트, 광고, 고객 프로그램 및 포지셔닝 선언 등을 통해 구체적이고 명확하며 차별화된 메시지.

영업 전략: 적절한 직간접 판매망, 마케팅, 서비스 및 홍보 회사를 이용하여 시장 도달 범위와 깊이, 전문지식, 기술, 서비스 및 고객 기반을 확대하는 제품 판매 전략.

오퍼링 (제품) 전략: 벤더들이 현재와 미래의 요구사항을 맵핑시킬 때, 차별화, 기능성, 방법론 및 일련의 기능을 강조하는 제품 개발 및 전달에 대한 벤더들의 접근방식.

비즈니스 모델: 벤더들의 기본적인 비즈니스 제안의 건전성과 논리.

수직/산업 전략: 수직 시장을 포함한 개별 시장 부문 특유의 요구사항에 부응하도록 리소스, 기술 및 오퍼링을 배치하는 벤더의 전략.

혁신: 투자, 통합, 방어 또는 선점을 위해 직접적이고 연관성이 있으며 보완적이고 시너지 효과를 창출할 수 있는 리소스, 전문지식 또는 자본의 배치.

지리적 전략: "본국" 또는 본거지를 벗어난 지역에서의 특유한 요구사항에 부응하도록, 직접 또는 그 지역 및 시장에 적합한 파트너, 채널 및 계열사를 통해 리소스, 기술 및 오퍼링을 배치하는 벤더의 전략.