PRISMA CLOUD
BY PALO ALTO NETWORKS

클라우드 위협 방어에 대한 비즈니스 사례

핵심 요약

Prisma™ Cloud는 GCP™(Google Cloud Platform), AWS®(Amazon Web Services) 및 Microsoft Azure® 전반에서 효과적인 위협 방어를 지원하는 보안 및 규정 준수 서비스입니다. 이 혁신적인 머신 러닝 지원 접근법은 서로 다른 보안 데이터 세트의 연관성을 조사하여 가장 단편화된 멀티 클라우드 환경에서 포괄적인 가시성을 제공하고, 위협을 탐지하며, 신속하게 대응할 수 있도록 해줍니다. 기업에서는 Prisma Cloud를 통해 퍼블릭 클라우드 컴퓨팅 구축 전반에 걸쳐 규정 준수를 보장하고 보안 작업을 지원할 수 있습니다.

Palo Alto Networks는 클라우드 위협 방어 구현과 관련된 이점, 비용, 문제 및 리스크를 보다 정확하게 이해하기 위해 Prisma Cloud 고객 기반을 대상으로 비용 절감, 비용 지출 방지 등 특정 영역에 대한 설문 조사를 실시했습니다. 고객은 Prisma Cloud를 사용하여 가시성과 보안 거버넌스 확보, 규정 준수 보장, 타사 도구 및 인적 요구 사항 감소, 보안 위반으로 인한 재무 리스크 감소 등의 이점을 누리고 있습니다. 다음은 보고된 이점에 대한 간략한 내용입니다.

핵심 영역	비용 지출 방지	이점
보안 운영	클라우드 상태에 대한 수동 평가 관련 비용 지출 방지	타사 클라우드 상태 평가(예: 침투 테스트)와 관련된 비용, 관리 및 오버헤드 제거
	잠재적인 보안 리스크를 조사하고 해결하는 작업 감소	리스크 순위에 따라 우선순위가 지정된 실행 가능한 알림을 통해 수정 시간 단축
	로그 관리자를 발굴하고 유지할 필요가 없음	자체 개발 또는 타사 SIEM 시스템이 필요하지 않음
	보안 침해로 인한 재무 리스크 감소	클라우드 환경에서 보안 침해로 인한 경제적, 자산 또는 브랜드 손실 가능성을 대폭 완화
규정 준수	기존 규정 준수 제어를 퍼블릭 클라우드에 수동으로 매핑하는 작업이 필요 없음	PCI, NIST, SOC 2, HIPAA, CIS, GDPR과 같은 업계 표준에 따라 기본 제공 규정 준수 보고를 통해 시간, 리소스 및 비용 절약
	감사 검증 요건을 따르는 데 소요되는 인적 수고 감소	
DevOps	기존 보안 제어를 퍼블릭 클라우드에 강제 적용하려고 할 때 발생하는 지연 및 재작업 방지	보안 및 규정 준수 팀에 퍼블릭 클라우드 환경에 대한 지속적인 가시성 제공
		자동화된 수정 작업을 개발 워크플로에 통합

그림 1: Prisma Cloud의 이점

Prisma Cloud 비용-편익 분석의 주요 결과

대표적인 고객 클라우드 환경의 샘플 크기를 토대로 한 Prisma Cloud*의 3년 ROI 추정치는 그림 2를 참조하십시오.

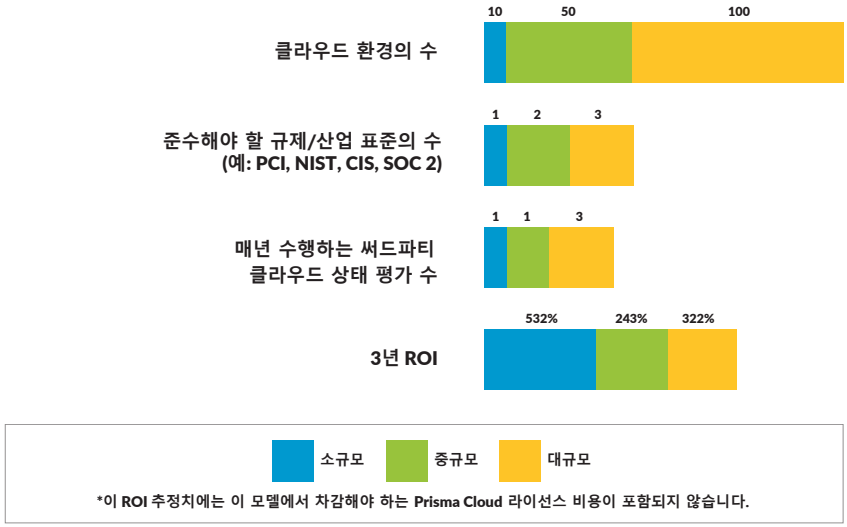

그림 2: 환경 크기에 따른 Prisma Cloud ROI

퍼블릭 클라우드 보안 요건

퍼블릭 클라우드 채택률은 괄목할만한 성장을 이루어 전 세계 퍼블릭 클라우드 서비스 시장은 2018년 1,758억 달러에서 2019년에는 총 2,062억 달러로 17.3% 성장할 것으로 예상됩니다.[1] 하지만 이러한 급격한 성장에는 새로운 리스크가 수반됩니다. Gartner 또한 "2022년까지 클라우드 보안 오류 중 최소 95%는 기업의 실수가 원인이 될 것"[2]이라고 예측하고 있습니다.

클라우드 규정 준수 및 보안을 보장하기 위한 옵션을 평가할 때에는 기존 데이터센터 보안의 용도 변경, 자체 보안 및 규정 준수 옵션 구축 또는 클라우드 네이티브 보안 제품 구입에 대해 논의할 수 있습니다. Cybersecurity Insiders의 2018 Cloud Security Report에 따르면 2018년에 기존 보안 조치가 클라우드에서 자체 조직을 보호하는 데 적합하다고 평가한 기업은 16%에 불과했습니다.

내부에서 제품을 구축한다는 것이 솔깃하게 들릴 수도 있지만 현실과는 동떨어져 있습니다. 수십 개의 클라우드 보안 포인트 제품이 존재하지만, 대부분은 가장 흔하고 시급한 클라우드 보안 문제를 포괄적으로 해결하는 데 효과적이지 못합니다.

- **가시성:** 기업이 모든 자산을 완벽하게 파악하고 정확하게 제어할 수 있는 기존의 온프레미스 데이터센터와 달리 클라우드로의 마이그레이션에는 주요 사각지대가 수반됩니다. 수명이 짧은 클라우드의 특성뿐 아니라 개별 사업부, 여러 지역, 여러 서비스 공급자별로 분할된 소유권으로 인해 자산을 추적하고 리스크를 정확하게 식별하기가 매우 어렵습니다. 간단히 말해, 클라우드용 구성 관리 데이터베이스(CMDB)는 일반적으로 대다수의 기업에 존재하지 않습니다.
- **규정 준수 관리:** 기업이 새로운 기능을 요구하고 개발자가 최신 기술을 채택해야 하는 탓에, 클라우드 서비스 공급자는 매일 플랫폼을 위한 새로운 기능을 출시합니다. 그리고 환경은 시시각각 변하고 있습니다. 이렇게 빠른 변화 속에서 기존 규정 준수 및 규정 제어를 온프레미스에서 클라우드로 매핑하려면 어떻게 해야 할까요? 더 중요한 질문은 '이러한 환경이 항상 규정을 준수했음을 입증하는 감사 친화적인 기록 보고를 어떻게 생성하는가?'입니다.
- **위협 탐지:** 안전하고 깔끔한 환경을 유지하려면 반드시 클라우드에서 다양한 리스크를 발견해야 합니다. 구성 드리프트 탐지, 계정 손상 또는 내부자 위협 식별, 의심스러운 네트워크 트래픽 파악 등이 모두 효과적인 클라우드 위협 방어를 위해 필요합니다. 하지만 기존 보안 도구로는 이 중 어느 것도 수행할 수 없습니다.
- **사고 대응:** 클라우드 환경에 대한 수백 또는 수천 개의 데이터 포인트를 보유하고 있는 것만으로는 클라우드 위협에 효과적으로 대응하지 못합니다. 환경 전체를 보면서 대응할 수 있어야 합니다. 따라서 리소스 구성, 사용자 작업, 네트워크 트래픽, 호스트 취약점/활동, 타사 위협 인텔리전스 소스와 같은 자산에서 가져온 서로 다른 데이터의 상관성을 분석하여 필요한 컨텍스트를 생성해야 합니다. 그래야만 실행 가능한 알림에 대한 충분한 정보를 확보하여 각 문제의 심각도에 따라 우선순위별로 대응할 수 있습니다.

1. Gartner, "Gartner는 2019년에 전 세계 퍼블릭 클라우드 매출이 17.3% 성장할 것으로 예측", 2018년 9월 12일, https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019.
2. Gartner, "Gartner 조사에 따르면 클라우드 컴퓨팅이 새로 떠오르는 가장 큰 비즈니스 리스크", 2018년 8월 15일 https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-says-cloud-computing-remains-top-emerging-business-risk.
3. Cybersecurity Insiders, "2018 클라우드 보안 보고서", 2018년 12월 18일 액세스, https://start.paloaltonetworks.com/cloud-security-report-2018.

자체 클라우드 위협 방어 프로그램 구축이 기업의 인력, 프로세스 및 기술에 의미가 있으려면 이 기본적인 클라우드 보안 과제를 해결해야 합니다. 고려해야 할 또 다른 질문은 다음과 같습니다.

- 위반 또는 구성 오류가 발생할 때 이를 어떻게 알 수 있고 어떻게 대응해야 하는가?
- 맞춤형 제품을 개발하기 위해 필요한 하드웨어와 소프트웨어는 무엇인가?
- 맞춤형 제품을 유지 관리하는 직원을 어떻게 지정하는가?
- 자체 프로그램을 구축하기 위한 9개월에서 24개월의 주기를 수용할 수 있는가?
- 단일 창에서 모든 클라우드 리소스를 모니터링할 수 있는가?
- 클라우드 위협 방어를 설계하고 구축할 적임자가 있는가?
- DevOps 및 SecOps 팀에 미치는 영향은 무엇인가?

Prisma Cloud를 통한 절감 효과 및 이점

Prisma Cloud를 사용하면 여러 영역에서 측정 가능한 절감 효과와 이점을 확보하여 상당한 투자 수익을 올릴 수 있습니다.

규정 준수 유지에 필요한 인적 수고 감소

클라우드 리소스 규정 준수 보고 및 감사는 시간과 비용이 많이 소요되는 어려운 과정입니다. 각 규정 준수 표준에 제어를 매핑하고 필요한 보고서를 생성하는 데는 처음에는 평균 480시간이 소요되는 것으로 추정됩니다. 이후 몇 년 동안 유지 관리, 보고 및 감사 지원에 평균 240시간이 소요됩니다. Prisma Cloud를 사용하면 CIS, NIST, SOC 2, PCI, HIPAA, GDPR과 같은 규정 준수 프레임워크에 클라우드 리소스 구성을 매핑하는 기능을 기본적으로 이용할 수 있습니다. 이를 통해 상당한 리소스를 확보하여 다른 전략적인 작업을 지원할 수 있습니다.

써드파티 클라우드 상태 평가 관련 비용 지출 방지

대부분의 기업에는 클라우드 환경에서 리스크를 정기적으로나 효과적으로 평가할 수 있는 사내 전문 지식이나 도구가 없습니다. 따라서 그러한 기업은 타사 전문가에게 매년 의뢰하여 이 테스트를 실시해야 합니다. 이러한 평가는 컨설턴트에게 클라우드 계정당 3일에서 5일 정도 소요되는 것으로 추정됩니다. Prisma Cloud는 지속적인 보안 모니터링을 통해 써드파티 평가를 수행할 필요를 없애 줍니다.

보안 리스크를 조사하고 해결하는 데 드는 인적 수고 감소

SOC 팀에는 일반적으로 클라우드 서비스 공급자 또는 기타 오픈 소스 보안 도구(예: Amazon GuardDuty®, Security Monkey)에서 생성된 보안 알림을 조사하고 실행할 수 있는 전문성이나 도구가 부족합니다. 이 문제는 기업이 GCP, AWS 및 Azure와 같은 여러 클라우드 플랫폼을 채택하면서 더욱 가중되고만 있습니다.

Prisma Cloud는 모든 퍼블릭 클라우드 환경에서 리스크를 모니터링, 측정 및 우선순위를 지정하는 통합 기능을 보안 운영 센터 팀에 제공함으로써 그러한 과제를 해결해 줍니다. Prisma Cloud 알림에는 개별 리스크의 특성, 이 리스크를 누가 언제 유발했는지, 이 리스크가 환경에 미치는 영향, 익스플로잇 공격 상태, 이 문제를 수정하는 방법에 대한 세부 정보 등 모든 관련 정보가 포함되어 있습니다. 이 정보를 바탕으로 SOC 분석가는 우선순위가 가장 높은 알림에 집중함으로써 DevOps와 대역외 대화에 참가하거나 여러 도구를 사용하여 직접 조사하지 않고도 조치를 취할 수 있으므로 조사 시간이 75% 단축됩니다.

타사 로그 집계 관련 비용 지출 방지

SIEM(Security Information and Event Management) 시스템은 관련 하드웨어 비용 및 이 하드웨어를 관리하는 시스템 관리자 비용 외에도 수집한 데이터의 양에 따라 비용이 발생하기 때문에 사용 비용이 많이 듭니다. Prisma Cloud를 사용하면 이 데이터 집계가 포함되어 엔터프라이즈 SIEM에 관련 알림만 제공할 수 있을 뿐 아니라 스토리지 비용을 95% 절감할 수 있습니다. 따라서 고객은 적어도 한 명의 SIEM 관리자에 드는 비용 외에도 로그 집계에 드는 하드웨어 및 소프트웨어 비용에서 클라우드 환경당 5,000달러의 비용을 절감할 수 있을 것으로 추정됩니다.

보안 침해로 인한 재무 리스크 감소

Ponemon Institute의 "2018년 데이터 침해와 관련된 비용 연구: 전 세계 개요(2018 Cost of a Data Breach Study: Global Overview)에서는 보안 침해로 인해 발생하는 평균 비용은 386만 달러이고, 향후 2년 동안 중대한 침해가 되풀이될 가능성이 27.9%에 달한다고 추정했습니다.[4] 기업은 Prisma Cloud를 통해 클라우드 보안 리스크를 포괄적으로 파악하고, 심층 분석을 사용하여 정확한 리스크 특성과 영향을 신속하게 이해하여 문제를 보다 신속하게 해결할 수 있습니다. Prisma Cloud는 위협과 취약점을 사전에 파악함으로써 운영 첫 해에는 위반 가능성을 최대 50% 줄이고, 상당한 보안 노출이 해결되는 두 번째 해에는 75%까지 줄일 수 있습니다.

4. Ponemon Institute, "2018년 데이터 침해와 관련된 비용 연구," 2018년 7월, https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf.

재무 분석

다음 모델은 이러한 고객 기반 추정치를 통해 세 가지 환경에 대한 상세한 Prisma Cloud 절감 효과를 나타냅니다. 이 ROI 추정치에는 이 모델에서 차감해야 하는 Prisma 라이선스 비용이 포함되지 않습니다.

5  **일일 평균 클라우드 계정당 알림 수**	**$150,000**  **완전히 로드된 FTE 비용**
$250  **타사의 컨설팅 시간당 요율**	**24**  **타사 테스트 작업에서 차지하는 클라우드 계정당 시간**
60  **각 클라우드 알림을 수동으로 조사하고 해결하는 데 소요되는 시간(분)**	**15**  **Prisma Cloud를 통해 각 클라우드 알림을 수동으로 조사하고 해결하는 데 소요되는 시간(분)**

그림 3: 이 모델을 구축하는 데 사용된 가정

10	1	1
클라우드 환경의 수	준수해야 할 규제/산업 표준의 수(예: PCI, NIST, CIS, SOC 2)	매년 수행하는 써드파티 클라우드 상태 평가 수

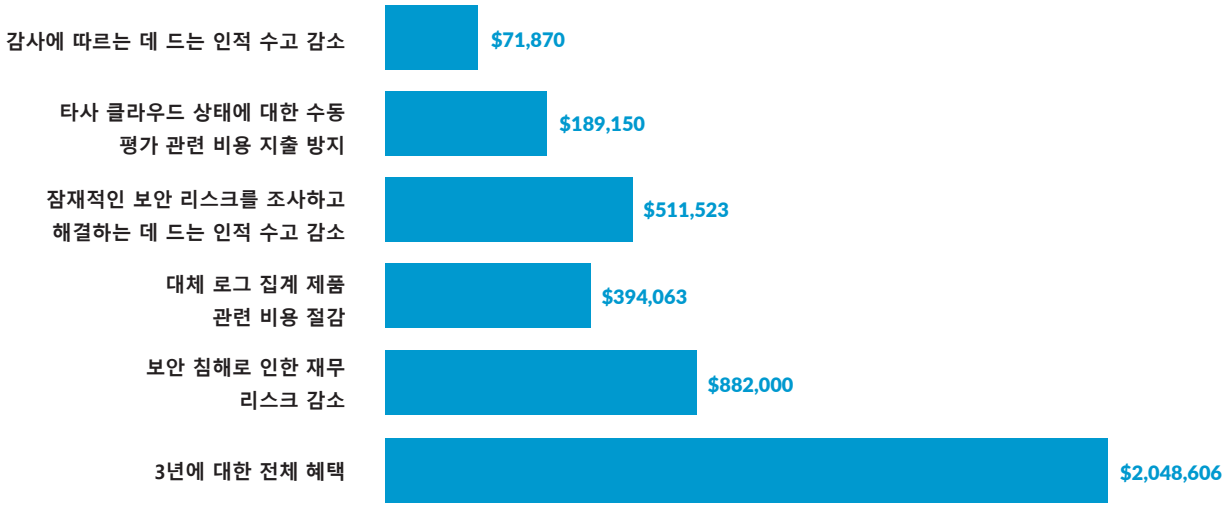

그림 4: 소규모 클라우드 환경 한눈에 보기

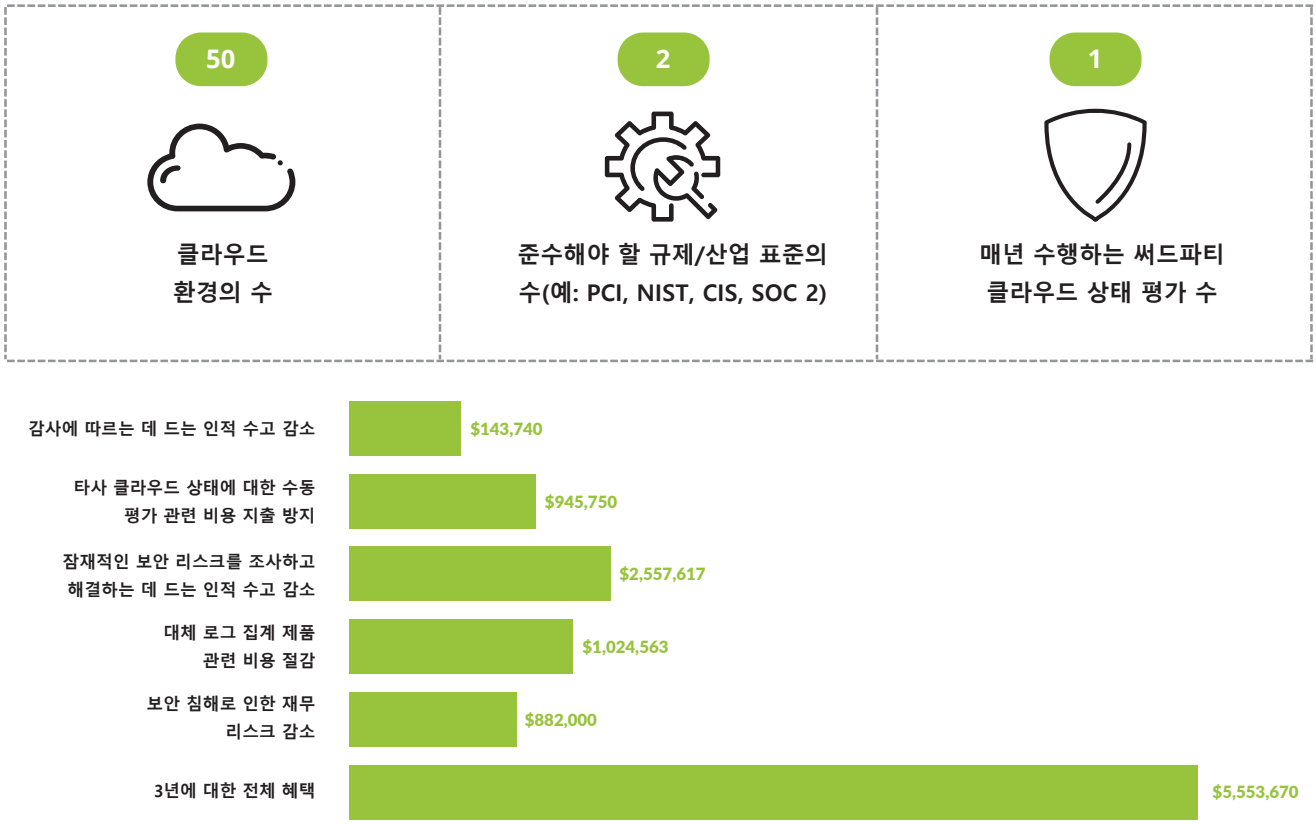

그림 5: 중규모 클라우드 환경 한눈에 보기

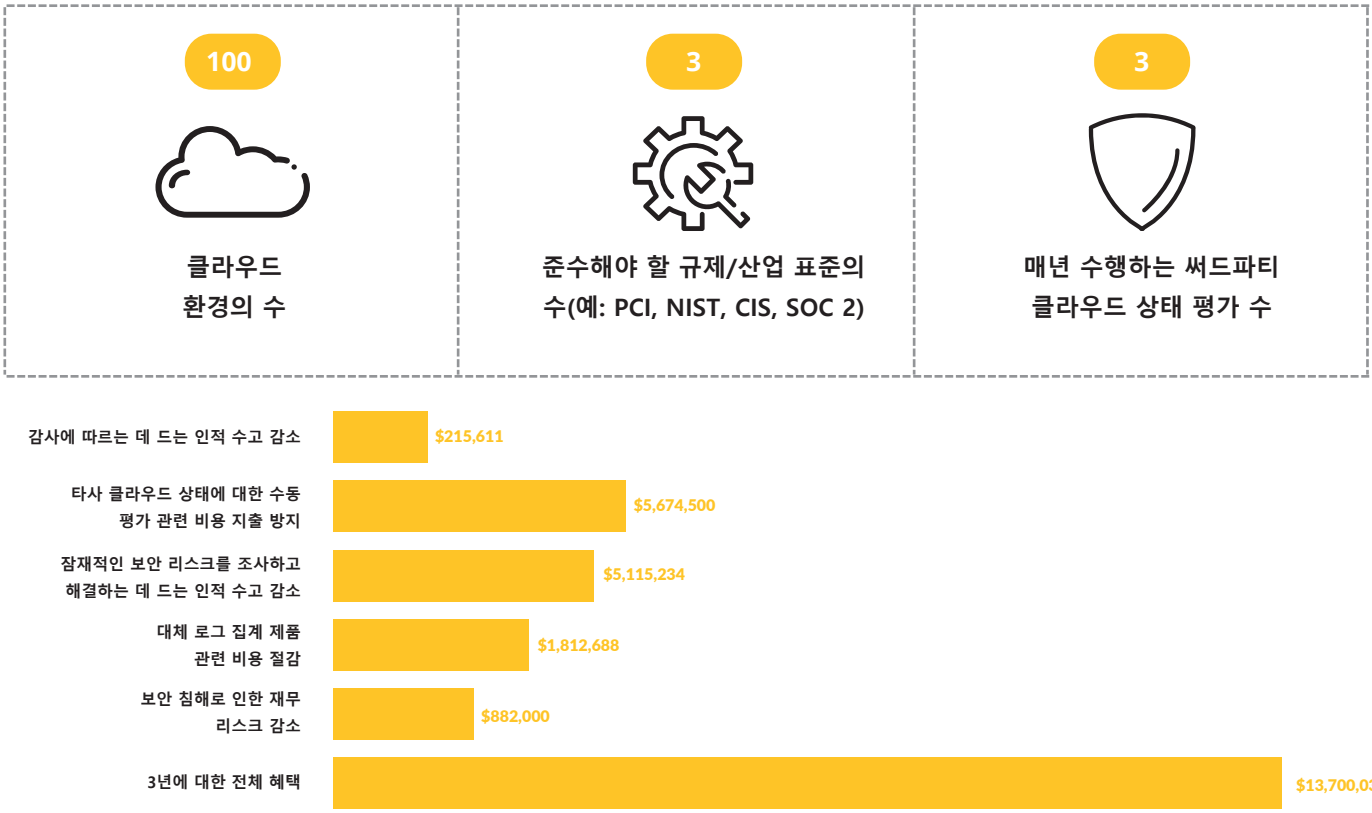

그림 6: 대규모 클라우드 환경 한눈에 보기

결론

Prisma Cloud를 사용하면 규정 준수를 보장하고 강력한 보안 상태를 유지하는 동시에 상당한 비용, 시간 및 리소스를 절약할 수 있습니다. 감사와 관련된 인적 수고 감소, 써드파티 상태 평가, 위협 조사, 타사 도구 관리 등 여러 분야에서 절감 효과가 나타납니다. 아울러, 타사 SIEM과 같은 보조 시스템을 모두 피할 수 있습니다. 가장 중요한 점은 Prisma Cloud를 통해 보안 침해 가능성을 줄여 자산을 보다 강력하게 보호할 수 있다는 것입니다.

무료 30일 평가판에 등록하려면 여기를 클릭하십시오.

PRISMA CLOUD
BY PALO ALTO NETWORKS

3000 Tannery Way
Santa Clara, CA 95054
본사: +1.408.753.4000
영업 부서: +1.866.320.4788
고객 지원: +1.866.898.9087

www.paloaltonetworks.com

the-business-case-for-cloud-threat-defense-wp-080219