IBM Security

IBM

데이터 위치와 상관없이 클라우드 환경에서 구매 및 배포 가능한 보안 솔루션

이제 클라우드 또는 하이브리드 모델로 이전하는 기업은 규제 준수와 첨단 위협 탐지를 효율적으로 수행할 수 있습니다

IBM Security 백서

네트워크에 대한 가시성을 제공하는 IBM QRadar

오늘날 데이터 및 네트워크 보호는 어떤 규모의 기업에서도 쉽지 않은 과제입니다. 거의 매일 새로운 취약점이 발견됩니다. 어떤 악성코드에 대한 탐지 스크립트가 만들어지는 즉시 새로운 악성코드 변종이 개발됩니다. 게다가 사이버 범죄자들은 전문 지원 팀까지 갖춰진 사전 패키지 형태의 익스플로잇 킷을 다크넷에서 구입할 수 있습니다. 보안 분석가 입장에서는 네트워크의 경계를 방어하도록 설계된 몇 개의 포인트 솔루션만으로는 충분하지 않습니다. 뛰어난 가시성, 안목, 감각을 통해 뭔가 잘못되면 이를 파악할 수 있어야 합니다.

IBM® QRadar®가 그 역할을 훌륭하게 해냅니다. 누가 언제 어디서 무엇을 하고 있는지 보여주는 광범위한 기능으로 데이터와 네트워크를 보호합니다. 대시보드 및 첨단 시각화 기능을 통해 수천 또는 수백만 건의 개별 인시던트로부터 의심되는 장애에 관한 간략한 지표를 생성하여 보여주고, 의심스러운 활동이 있으면 그 세부 기록을 보존하여 향후 분석할 수 있게 합니다. 그뿐만 아니라 첨단 로깅 기능 및 리포트 생성 툴을 활용하여 규제 준수 보고 의무와 같은 기본 요건을 신속히 이행할 수 있습니다.

그리고 이제 IBM QRadar on Cloud에서는 하드웨어와 소프트웨어를 직접 구축하거나 유지보수할 필요 없이, QRadar가 수집하는 인텔리전스를 활용하는 데 집중하면 됩니다. 귀사의 팀에서 현재 상황을 모니터링하므로 귀사가 계속 통제권을 갖습니다. 귀사의 환경을 조사하고 탐지 기능을 정밀 조정하며 다른 팀과의 긴밀한 협업을 통해 모든 위협 탐지 및 대응 기술을 강화하십시오.

QRadar 클라우드 솔루션으로 1초에 최대

80,000

건의 이벤트를 처리합니다.[1]

▸ 여기를 클릭하여 IBM QRadar on Cloud에 관해 자세히 알아보세요

1 "IBM Security Intelligence on Cloud onboarding," *IBM Knowledge Center.*

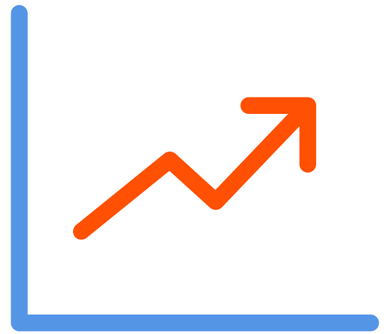
규제 요건과 보안 요건을 동시에 충족

아마도 귀사는 간단한 공격을 차단하기 위해 네트워크의 경계에 기본적인 보안 기능을 구축했을 것입니다. 그러나 대부분의 엔드포인트에는 보안 허점이 있으며, 참지 못하고 악성 링크를 클릭하는 사용자도 있습니다. 각종 디바이스 및 인증 정보가 자주 감염되면서 데이터 유출 경로가 되고 그로 인해 비즈니스가 중단되기까지 합니다.

먼저 규제 요건에 대해 생각해 볼까요? 이 요건을 이행하려면 시스템 및 데이터를 효과적으로 통제하고, 모두 안전하게 보호받고 있음을 문서로 입증해야 합니다. 보안 분석 시스템을 구축하면 보안 팀의 규제 준수 보고와 관련된 워크로드를 줄일 수 있습니다. 이 시스템을 통해 더 수월하게 올바른 형식의 종합 보고서를 작성하고 감사하기 편리한 형식으로 네트워크 관련 정보를 수집, 큐레이션, 검토할 수 있기 때문입니다.

중요 데이터가 생성, 저장, 전송되는 내부 환경의 복잡성을 생각해 보시기 바랍니다. 현대화된 네트워크는 각종 자산으로 구성되는데, 이러한 자산이 익스플로잇 공격의 대상이 되는 보안 허점을 수반하곤 합니다. 여기에는 네트워크의 다양한 운영 체제, 서버에서 라우터, 스위치에서 방화벽에 이르는 각종 하드웨어, 웹 기반 또는 기타 애플리케이션 소프트웨어 등이 포함됩니다. 이러한 각각의 요소 때문에 네트워크 전체를 보호하기가 더 어려워지며, 사이버 범죄자는 네트워크에 접근하기 위해 가장 약한 고리를 노립니다.

데이터 수집 및 규제 준수 보고 시스템의 구축은 쉬운 편이지만, 감사 기관을 만족시키고 귀사의 중요 데이터를 보호하는 것은 결코 만만치 않습니다. 더 발전된 시스템, 이를테면 IBM Sense Analytics Engine™ 기반 QRadar를 활용한다면, 더 철저히 준비된 상태에서 일상의 활동뿐만 아니라 조사 및 사고 대응이 요구되는 비정상적인 네트워크 침해사고까지 효과적으로 관리할 수 있습니다.



2015년에 해킹 사고가 9년 만에 최고를 기록하여2014년 대비

8.4%

증가했습니다.[1]

▸ 여기를 클릭하여 현재 기업을 위협하는 여러 요인에 관한 IBM X-Force®의 인사이트를 만나보세요

1 "Identity Theft Resource Center Breach Report Hits Near Record High in 2015," *Identity Theft Resource Center,* 2016년 1월.

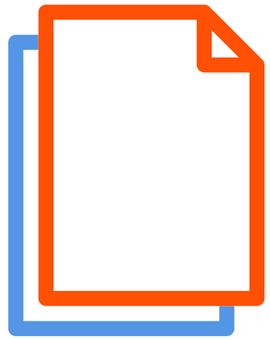
규제 준수 및 보안을 뒷받침할 깊이 있는 인사이트 확보

악성코드를 탐지하고 제거하며 서브넷 보호를 위한 방화벽 규칙을 설정하는 것이 중요합니다. 귀사가 경계 보안에 투자한 이유도 여기에 있을 것입니다. 그러나 보안 분석 소프트웨어의 전제가 되는 기본 개념은 인터넷에 연결된 어떤 경계에서도 100% 보안을 보장할 수 없고 기업에서 행동 변화 및 이상 요인을 탐지할 수 있어야 한다는 것입니다.

보안 분석을 추가하는 방법 중 하나는 대규모 설비 투자 예산 및 데이터센터 공간을 확보한 다음 몇 주 또는 몇 개월에 걸쳐 온프레미스 솔루션을 구축하는 것입니다. 그 과정에서 귀사의 팀이 서비스 자동 업데이트를 예약하고 위협 인텔리전스 피드를 구성하며 네트워크 검사 일정을 생성하고 데이터 보존 기간을 정의합니다. 이 모든 과정을 거쳐야 투자에서 큰 가치를 창출할 수 있습니다.

또 다른 방법은 보안 데이터 게이트웨이를 구축한 다음 월간 운영비를 내고 전문가에 의해 구축되고 관리되는 클라우드 환경에 보안 데이터를 보내는 것입니다. 이 클라우드 모델에서는 귀사가 통제권을 갖습니다. 그리고 귀사의 실무팀은 소프트웨어 패치 적용 및 데이터 백업 작업보다 환경을 모니터링하고 위협 탐지 규칙을 튜닝하고 규제 준수 또는 관리 보고서를 맞춤 구성하는 데 집중할 수 있습니다.

곧 Jackie Jones가 오후 2:32에 시카고에서 로그인했다는 식의 단순한 로그 이벤트에 시간을 빼앗기지 않고 행동의 변화를 나타내는 알림, 이를테면 Jackie Jones가 같은 주의 어느 날 오전 3:07에 동남아시아에서 다시 로그인했다는 알림을 받게 됩니다. 불필요하게 시간을 빼앗는 요소가 사라지므로, 해당 변화에 대한 합당한 설명(예: Jackie의 출장)이 있는지 아니면 뭔가 문제가 생겼는지 여부를 충분한 시간을 갖고 밝혀낼 수 있습니다.



QRadar에서 생성하는

1,500

종 이상의 사전 정의된 보고서 유형을 통해 규제 준수부터 취약점 관리까지 다양한 영역을 지원할 수 있습니다.[1]

- IBM 백서에서 QRadar에 관해 자세히 알아보세요.

1 Lee Bell, "IBM builds QRadar Security Intelligence in the cloud," *The Inquirer,* 2015년 4월.

본격적인 규제 준수 대비

QRadar on Cloud는 비즈니스 중심 기능으로서 큰 역할을 해냅니다. 데이터를 보호하고 그러한 보호를 뒷받침하는 보안 관행 및 이벤트에 관한 기록을 감사 가능한 형식으로 준비함으로써 기업이 정부 및 산업 규정을 준수하도록 지원합니다. 이러한 요건을 이행하지 않으면, 부과되는 과징금이 악성코드로 인한 데이터 유출 못지않게 기업의 발목을 잡을 수 있습니다.

소비자의 개인 정보 및 금융 정보를 보호하고 기업의 투명성을 강화하기 위해 마련된 각종 요건 및 모범 기준이 고객 및 기업 데이터를 수집, 저장, 보호하는 방식에 적용됩니다.

SOX(Sarbanes-Oxley), PCI DSS(Payment Card Industry Data Security Standard), HIPAA(Health Insurance Portability and Accountability Act), 유럽연합의 GDPR(General Data Protection Regulation)을 비롯한 여러 규정을 지키지 않을 경우 해당 기업은 민형사상 처벌을 받고 신용카드 사용이 금지되는 등 비즈니스에 큰 타격을 줄 여러 위험을 감수해야 합니다.

과징금의 부담을 논외로 하더라도, 규제 준수를 보장하는 프로세스를 통해 네트워크 노드에서 데이터 저장, 암호화, 보호의 모범 사례들이 뿌리내리게 할 수 있습니다. 규제 준수를 달성하는 워크플로우 및 스토리지 아키텍처가 구현된 인프라를 설계하고 유지보수하는 일은 어떤 소프트웨어로도 대체할 수 없지만, QRadar on Cloud는 규정 불이행을 찾아내 해결하여 데이터 및 애플리케이션을 정상적인 상태로 유지하도록 지원합니다.

HIPAA 위반 시 형사 처벌을 받고 위반 건당 최대

5만 달러

의 벌금(연간 150만 달러 한도)이 부과될 수 있습니다.[1]

▸ 이 백서에서 규제 준수를 위해 해야 할 일과 하지 말아야 할 일을 알아보세요.

1 "HIPAA Violations and Enforcement," *American Medical Association*. 2016년 7월 26일 화요일 액세스

면밀한 데이터 모니터링으로 새로 등장하거나 진화하는 위협에 대응

어떤 보안 위협은 보안의 개별 요소를 다루는 전문 툴을 사용하여 전술적으로 접근할 수 있습니다. 이러한 방식은 정의된 위협 및 알려진 문제점을 해결하는 데 유용하며, 대응 전략도 선택적으로 네트워크 포트를 차단하거나 단발성 악성코드를 제거하거나 식별된 취약한 자산에 패치를 적용하는 등 단순한 편입니다.

하지만 QRadar 소프트웨어는 모든 보안 인텔리전스 모듈이 공유하는 더 방대한 보안 데이터를 수집하므로 포인트 솔루션보다 훨씬 더 큰 가치를 제공할 수 있습니다. 귀사의 네트워크에서 일반적인 데이터 흐름을 관찰하고 그 임계값을 계산한 다음 이 임계값을 넘어서는 이벤트를 자동으로 감지하여 귀사 보안 팀에 알립니다. 임계값 규칙을 통해 비정상적으로 큰 아웃바운드 데이터 전송, 애플리케이션의 대역폭 사용 변화 또는 뜻밖의 IT 주소에서 일어나는 의심스럽게 많은 로그인 시도를 찾아낼 수 있습니다.

또한 QRadar는 사용자 ID, 출발지 및 목적지 IP 주소, 어떤 활동이 발생한 지리적 위치를 비교하면서 연관 이벤트를 파악합니다. 이와 같이 연결된 이벤트로부터 컨텍스트를 파악하여 실제 공격과 단발성의 새로운 행동을 더 확실하게 구별합니다. 그뿐만 아니라 *비사용(non-use)* 패턴도 찾습니다. 이를테면 특정 서비스나 자산이 갑자기 사라질 때입니다. 이는 자산이 (어쩌면 악성코드로 인해) 오프라인 상태이거나 QRadar가 기준선에서 벗어나는 사용자 행동을 탐지했음을 의미할 수 있습니다.

의료 서비스 분야에서 발생하는 의료 기록 데이터

유출

사고의 가장 큰 원인은 범죄형 공격입니다.[1]

▸ 여기를 클릭하여 IBM X-Force에서 수집하는 심층 보안 지식에 대해 알아보세요.

1 "Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data," *Ponemon Institute*, 2016년 5월.

클라우드 기반 보안 소프트웨어로 새로운 비용 모델 채택

소프트웨어가 IT 및 기업 운영에 중요한 역할을 할 수 있지만, 대부분 기업에서는 보안 소프트웨어를 자체적으로 운용할 경우 추가 워크로드가 발생하여 핵심 보안 업무에 걸림돌이 될 수 있습니다. 보안 팀이 수행해야 하는 여러 업무를 줄이고 간소화한다는 점이 클라우드 기반 대안을 선택하는 대표적인 동기 중 하나입니다.

게다가 현지(on-site)에서 하드웨어를 직접 호스팅할 경우 최초 사양 구성부터 최종 폐기까지의 라이프사이클이 또 다른 부담으로 작용할 수 있습니다. 대개 충분한 예비 부품을 확보해야 하고, 하드웨어 선택 시 유지보수를 염두에 두어야 하기 때문입니다. 이 모두 이미 쉴 틈 없이 일하는 현지 팀의 책임이 되곤 합니다.

더 우수한 보안을 실현하려면 일정 수준의 인적 자원 및 기술 자원이 필요하기 마련이지만, 클라우드 기반 호스팅 솔루션을 선택하면 보안 팀이 일상적인 일에 쓰는 시간과 관련 비용을 절약하여 분석 및 계획에 재투자할 수 있습니다. 시스템 업그레이드 및 애플리케이션 오류 수정은 전문가가 원격으로 처리할 수 있어 현지 IT 인프라에 지장을 주지 않습니다. 클라우드 애플리케이션의 특징 중 하나가 원격 액세스인 만큼 귀사의 현지 팀원이 새로운 소프트웨어 기능을 추가하기 위해 따로 시간을 내어 직접 서버를 설치하고 프로비저닝할 필요 없습니다. 이러한 요소를 종합하여 평가하면, 클라우드 기반 솔루션은 현지 자원을 과잉 프로비저닝하는 부담 없이, 빠듯한 일정(대개 몇 주 또는 며칠)으로도 도입하고 확장할 수 있습니다.

QRadar on Cloud 인프라는 신뢰할 수 있는 IBM 전문가가

24x7

모니터링합니다. [1]

- IBM 백서에서 클라우드 소프트웨어 도입으로 비용을 절감하는 방법을 자세히 알아보세요.

1 "IBM QRadar on Cloud," *IBM Corp.*, 2015년 4월.

보안 투자로 변화 및 성장에 대비

여느 기술과 마찬가지로 보안 툴도 혼자서 제 기능을 하는 경우는 거의 없습니다. 여러 툴을 연계하여 활용하면 변화무쌍한 위협 환경을 더 효과적으로 다룰 수 있으며 특정 기능을 추가할 수도 있습니다. 여기에는 귀사가 이미 도입한 경계 방어 툴도 포함됩니다.

QRadar on Cloud는 지난 10여 년간 개발된 500여 가지의 통합을 활용하면서 온프레미스 클라이언트의 요청을 처리하고 타사 솔루션과 연계하여 보안 인텔리전스 플랫폼을 보완합니다. 클라우드 구축 및 배포를 담당하는 숙련된 전문가 팀은 새로운 지원 모듈을 개발하지 않고도 귀사의 자산 및 애플리케이션으로부터 데이터를 수용하기 시작합니다. 대부분의 고객은 계약 체결 후 며칠 내로 가치를 누리기 시작합니다.

예컨대 IBM X-Force Threat Intelligence 연구를 통해 수집한 보안 데이터도 귀사의 QRadar on Cloud에 문제없이 계속 통합되므로, 진화하는 위협 요소 및 확인된 공격뿐만 아니라 지금까지 보고되지 않은 취약점까지 포괄하는 수백 테라바이트 규모의 정보를 활용할 수 있습니다.

IBM Security App Exchange에서 새로운 확장 기능 또는 앱을 다운로드하고 설치하여 네트워크 모니터링 기능을 확장할 수 있으며, IBM 클라우드 유지보수 팀이 이러한 기술 확장을 지원합니다. 이와 같이 지원되는 확장 기능이 이미 수십 개에 달합니다. 그중에는 새로운 가상화, 통합, 패치, 맞춤형 규칙도 있고 IBM QRadar User Behavior Analytics 앱과 같은 완전한 형태의 새로운 앱도 있습니다. 이 사이트의 모든 내용은 IBM Security가 *Ready for IBM Security Intelligence* 검증 프로세스를 통해 점검합니다.

QRadar는 각종 로그 이벤트 및 네트워크 플로우 데이터를

500여 개

애플리케이션 및 디바이스로부터 수집할 수 있습니다.[1]

▸ IBM Knowledge Center에서 QRadar 플러그인 및 확장 기능에 대해 자세히 알아보세요.

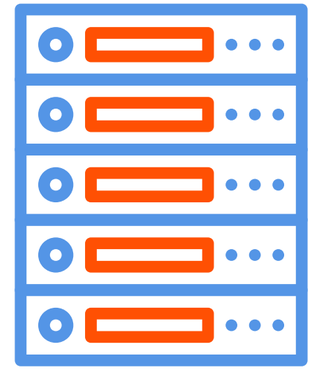
1 "Introducing the IBM Security App Exchange," *IBM Corp.*, 2015년 12월.

필요할 때 가동되는 확장 가능하고 유연한 인프라 구축

SaaS(Software as a Service)를 도입하면 확장성 및 유연성 측면에서 유리합니다. 온사이트 인프라에 구애받지 않고 용량을 변경할 수 있고 내부 인력 가용성에 크게 의존하지 않아도 되기 때문입니다. 2가지 규모 변동 시나리오를 통해 클라우드에 구축된 보안 분석 소프트웨어의 장점을 제대로 이해할 수 있습니다.

계절성: 대부분 기업은 워크로드의 주기적인 변동을 겪습니다. 그러한 변화 중 일부는 정확한 시점까지는 아니더라도 그 범위를 어느 정도 예측할 수 있습니다. 기존 소프트웨어 구매 모델에서는 최악의 상황(즉 가장 바쁘거나 수요가 많은 시기)을 가정하고 구매하는 것이 유일한 옵션일 때가 있습니다. 즉 일반적인 사용량보다 더 많은 하드웨어 용량을 구매하기 마련입니다.

사세 확장: 인수, 합병 또는 기타 형태의 확장을 계획 중인 기업 역시 필요 용량이 늘어날 경우에 대비하여 불필요하게 과다 구매를 해야 하는 상황에 처하곤 합니다. 하지만 클라우드 기반 구축에서는 필요에 따라 소규모로 용량을 추가 구매하거나 반납할 수 있습니다. 이 인프라는 클라우드에서 가동되고 용량 변동을 염두에 두고설계되었으므로 로컬에서 소프트웨어를 변경할 필요가 없습니다. 고객이거의 개입할 필요 없이 언제든 신속하게 용량을 늘리거나 줄일 수 있습니다.



안정적인 비즈니스 운영을 위해 실제 필요량의 최대

5배

에 달하는 데이터센터 공간을 확보한 기업이 많습니다.[1]

▸ 분석가 보고서에서 클라우드로 비즈니스 데이터를 이전하는 것의 재무적 타당성을 살펴보십시오.

1 David Linthicum, “Cloud Economics – Are You Getting the Bigger Picture?” *Cloud Technology Partners*, 2016년 5월.

IBM QRadar on Cloud의 실용적인 기능 활용

클라우드 기반 소프트웨어로 온프레미스 구축 시 부담해야 했던 상당한 인프라 비용을 줄일 수 있습니다. 이를테면 내부 인력이나 컨설턴트를 투입하여 범위를 결정하고 프로비저닝하고 테스트하기 위해 들인 시간과 비용입니다. IBM QRadar on Cloud는 수천 건에 달하는 온프레미스 QRadar 구축 사례에서 축적한 경험을 활용하여 귀사 환경에 필요한 사항을 해결합니다. 이 경험을 바탕으로 클라우드에서 속도를 낼 수 있습니다.

QRadar on Cloud를 구축하면 이미 개발한 모니터링 기능을 계속 활용하거나 확장할 수 있을 뿐만 아니라 분석가가 위협 인텔리전스 데이터를 이해하거나 기존 자산 보호에 전문성을 발휘하는 데 더 많은 시간을 보낼 수 있습니다. 온프레미스 보안 소프트웨어를 유지하거나 조정할 필요가 없습니다. 자동 소프트웨어 업데이트 및 온디맨드 확장 방식의 QRadar on Cloud는 예측 가능한 월 단위 운영 비용을 부담하면 되므로 IT 보안 팀의 업무가 훨씬 더 간소화됩니다.

[이 동영상](#)에서 QRadar on Cloud에 대해 자세히 알아보세요.

QRadar on Cloud를 구축하면 귀사에 필요한 전문성, 기능, 확장성을 모두 갖추게 됩니다. 이 시스템은 다음과 같은 기능으로 엔터프라이즈급 분석을 지원합니다.

- 웹 브라우저 접근성
- 데이터 수집, 상관성 분석, 리포팅 기능 – 규제 준수 지원
- 넉넉한 EPS(Event Per Second) 최대 한도 - 전 세계에 수백 개 사업장을 운영하는 고객의 요구 해결
- 고가용성 시스템 구성 - 거의 중단 없는 가용성 실현
- IBM Security App Exchange에서 제공하는 앱, 애드온, 확장 기능
- X-Force Threat Intelligence 피드 - 진행 중인 상황에 대한 정보 제공

또한 자체 보안 팀이 시간 또는 전문성 측면에서 제공하기 어려운 기능이 필요한 기업을 위해 선택형 부가 관리 서비스도 제공합니다.

클라우드 전략을 갖춘 기업은 그렇지 않은 기업보다

22%

더 적은 비용을 보안에 지출합니다.[1]

1 “Buying Intentions Survey: Security,” *Nucleus Research*, 2016년 2월.

왜 IBM인가?

IBM Security 솔루션은 하드웨어, 소프트웨어, 서비스 통합 오퍼링으로 기업이 보안 위협 및 취약점을 차단, 탐지하고 효과적으로 대응하도록 지원합니다. 심층 분석 및 신뢰받는 IBM Security 전문성이 뒷받침하는, 업계 최고 수준의 확장형 툴로 구성된 IBM 포트폴리오에서 광범위한 보안 인텔리전스를 제공합니다.

QRadar on Cloud 역시 동일한 기반 기술을 활용하여 로그 관리, 네트워크 플로우 분석, 실시간 및 이력 분석, 취약점 관리 기능을 제공하므로, 어떤 규모의 기업도 아웃소싱 방식으로 QRadar 보안 인텔리전스 인프라를 도입, 구축, 관리할 수 있습니다. 이 솔루션은 IBM Cloud Data Center에서 호스팅하고 전 세계에 서비스됩니다.

또한 QRadar On Cloud는 개방형 프레임워크이므로 IBM Security App Exchange에 게시되는 솔루션과 손쉽게 통합할 수 있습니다. 파트너들은 IBM Security App Exchange를 통해서 IBM Security 제품의 애플리케이션, 보안 애플리케이션 확장 기능, 향상된 기능을 공유할 수 있습니다. QRadar on Cloud를 이용하는 보안 팀은 (기본 라이센싱 조건을 초과하지 않는 한) 기존 호스팅 계약의 변경 없이 셀프 서비스 모델을 통해 각자 편리한 방식으로 솔루션을 다운로드하고 설치할 수 있습니다.

추가 정보

클라우드 기반 IBM QRadar Security Intelligence Platform에 대해 자세히 알아보려면 IBM 영업대표 또는 IBM 비즈니스파트너에게 문의하거나 아래 사이트를 방문하시기 바랍니다.

ibm.com/kr-ko/marketplace/hosted-security-intelligence

IBM Security 소개

IBM Security는 가장 발전되고 통합된 엔터프라이즈 보안 제품 및 서비스 포트폴리오를 제공합니다. 세계적 명성의 X-Force 연구소가 지원하는 이 포트폴리오는 기업이 종합적으로 인프라, 데이터, 애플리케이션을 보호하는 데 필요한 보안 인텔리전스를 바탕으로 ID 및 액세스 관리, 데이터베이스 보안, 애플리케이션 개발, 위험 관리, 엔드포인트 관리, 네트워크 보안 등을 지원하는 솔루션을 제공합니다. 이러한 솔루션을 선택한 기업은 효과적으로 위험을 관리하고 모바일, 클라우드, 소셜 미디어, 기타 엔터프라이즈 비즈니스 아키텍처에 적합한 통합 보안을 구현할 수 있습니다. IBM은 세계에서 가장 광범위한 보안 연구, 개발, 서비스 조직을 운영하면서 매일 130여 개국에서 150억 이상의 보안 이벤트를 모니터링하고 있으며, 3,000개 이상의 보안 특허를 보유하고 있습니다.

더불어 IBM 글로벌 파이낸싱에서는 다양한 지불 옵션을 통해 비즈니스 성장에 필요한 기술 도입을 지원합니다. IT 제품 및 서비스의 도입부터 폐기까지 포괄하는 종합 라이프사이클 관리를 제공합니다. 자세한 정보는 ibm.com/financing 사이트를 방문하시기 바랍니다.

IBM

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
2017년 1월

WGW03245-KRKO-01