



© Copyright IBM Corporation 2013  
 한국아이비엠주식회사  
 (135-270) 서울시 강남구 도곡동 467-12  
 군인공제회관빌딩

TEL : (02)3781-7500  
[www.ibm.com/kr](http://www.ibm.com/kr)

2013년 11월

Printed in Korea  
 All Rights Reserved

IBM, IBM 로고, ibm.com은 미국 및/또는 다른 국가에서 IBM Corporation의 상표 또는 등록 상표입니다. 상기 및 기타 IBM 상표로 등록된 용어가 본 문서에 처음 나올 때 상표 기호(® 또는 ™)와 함께 표시되었을 경우, 이러한 기호는 본 문서가 출판된 시점에 IBM이 소유한 미국 등록 상표이거나 관습법에 의해 인정되는 상표임을 나타냅니다. 해당 상표는 미국 외의 다른 국가에서도 등록 상표이거나 관습법적인 상표일 수 있습니다. IBM의 최신 상표 목록은 [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml) 웹 페이지의 "저작권 및 상표 정보" 부분에서 확인할 수 있습니다.

기타 다른 회사, 제품 및 서비스 이름은 다른 회사의 상표 또는 서비스 표시일 수 있습니다.

이 문서에는 IBM 제품과 서비스를 참조한 경우에도 IBM이 비즈니스를 수행하고 있는 모든 국가에서 해당 제품과 서비스를 제공함을 의미하는 것은 아닙니다.



이제, 보안도 인공지능 시대!  
 IBM QRadar로 미래의 보안까지 대비하세요.

KR2BK01D



통합 & 자동화 보안으로 스마트하게  
 선제적 방어는 물론, 컴플라이언스 대비까지

**인공지능으로 보안하다!**

보안천재, IBM QRadar의 산업별 성공사례

나날이 복잡해지고 지능화되는 보안 위협!

# 선제적 통합 보안 인텔리전스 플랫폼 “저, QRadar에게 모두 맡겨주세요”

## 보안은 왜 인텔리전트해야 할까요?

가상화, 클라우드, 모바일, 애플리케이션, 소셜미디어, 빅데이터 등 다양한 IT 환경에서 수많은 사용자들이 다양한 방법으로 회사의 네트워크에 접속하고 있습니다. 지금 회사의 네트워크에서 어떤 일이 일어나고 있는지 모두 파악하고 계신가요? 어제의 보안기술로 점차 지능화되고 있는 공격을 막아내는 것은 불가능합니다. 이제 지능화되고 다각화되는 보안 공격을 방어하기 위해서는 선제적인 보안 방어를 갖추는 방법밖에 없습니다. 이것이 바로 보안이 인텔리전트해야 하는 이유입니다.

여기, 보안 인텔리전스를 기반으로 한 선제적 통합 보안 플랫폼 IBM QRadar를 통해 보안 위협을 성공의 기회로 전환시킨 기업들의 이야기를 소개합니다.

산업별 성공 사례

금융

 KB 국민은행

04

금융

 하나캐피탈

08

에너지



12

온라인게임



16



IBM  
QRadar  
소개  
20

Why  
IBM  
23

‘보안 인텔리전스(Security Intelligence)’란

다양한 기기로 기업의 네트워크에 접근하는 모든 사용자의 로그 데이터를 실시간으로 취합·분석해 현재의 보안 위협은 물론, 예상되는 보안 위협에도 대응하는 것을 말합니다.

# “금융에서도, 보안에서도, 세계적인 스타기업이 되겠습니다”

KB 국민은행, QRadar로  
보안 인텔리전스를  
실현하다

KB 국민은행은 기존 보안 시스템이 한계에 부딪히면서 보안 강화와 메가 IT 트렌드인 빅데이터를 활용한 새로운 보안 시스템을 구축하고자 하였습니다.

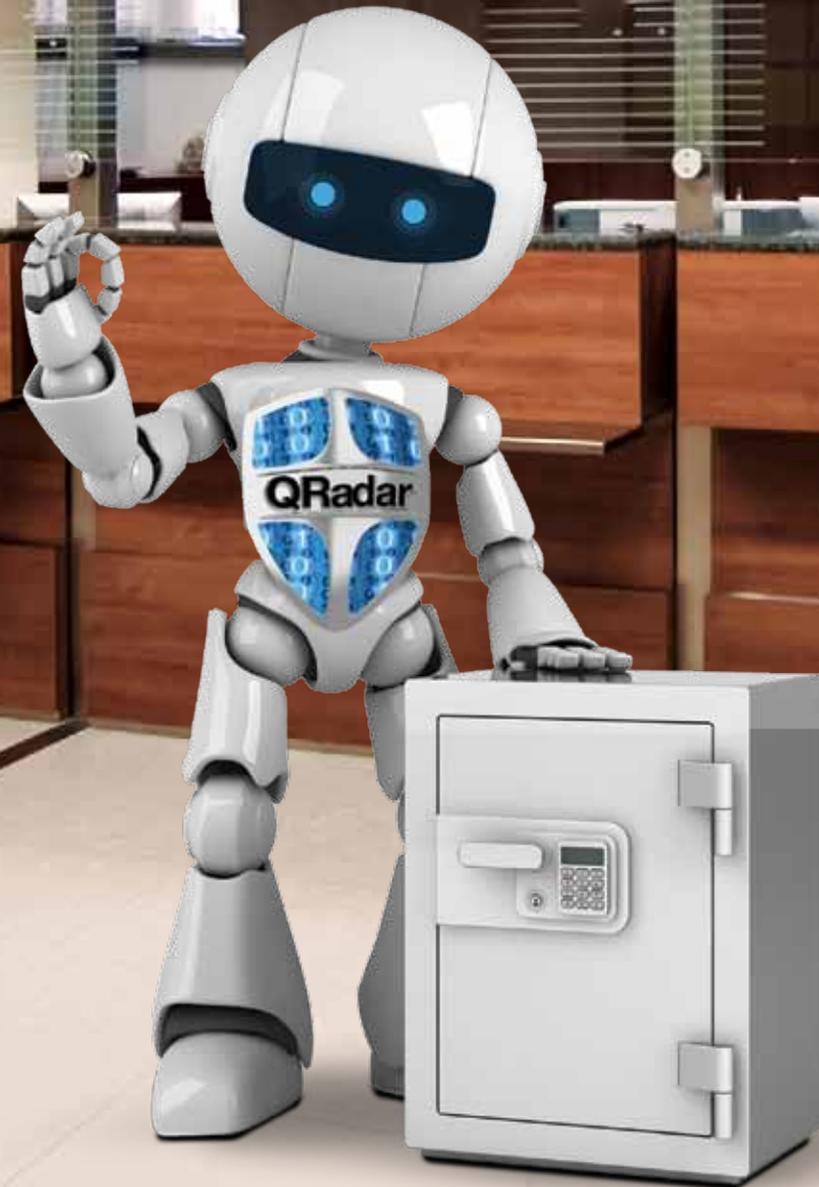
국내외의 수많은 곳에서 발생하는 대용량의 로그분석이 절실하게 필요한 상황에서 보안 리스크 및 관리 비용의 감소를 위한 '보안 인텔리전스'의 구현은 필수불가결한 선택이었습니다.

KB 국민은행은 거래고객, 자산규모 등에서 대한민국 금융을 선도하는 대표적인 금융기업이며 서민생활과 관련된 각종 예금제도를 개발해왔습니다. 세계적인 수준의 내부조직 및 사업 시스템을 보유한 글로벌 금융기관입니다.

산업별  
성공사례-금융  
국민은행



\* KB 국민은행





산업별 성공 사례-금융 / 국민은행

# 은행권 최초! 선제적 위협 관리를 수행하는 보안인텔리전스 시스템 구현



## / Background /

### 기존 보안 시스템의 한계 및 보안 강화의 필요성 대두

KB 국민은행은 최근 들어 대용량의 이기종 장비에서 발생하는 보안 이벤트 로그들이 폭증하고, 이에 따라 보안 위협의 가능성이 높아져 보안 강화의 필요성이 대두되는 상황이었습니다.

기존의 1세대 통합 보안 관리시스템은 DBMS를 이용하면서 대용량 로그 검색 성능이 보장되지 않았고, 다양한 시나리오에 대한 분석 템플릿이 부족하여 한정된 시간 내에 공격 유무를 분석하고 대응하는데 한계를 보였습니다.

특히 위협관리 측면에서는 빅데이터 기술을 활용하여 위협에 대해 선제적으로 대응할 수 있는 기술이 절실한 상태였습니다.

## / Challenge /

### 새로운 보안 시스템에 빅데이터 기술 전략적 적용

대용량 로그 및 트래픽 처리에 빅데이터 기술을 적용하여, 보안 위협 관리에 적극적으로 활용하고 선제적으로 대응하라는 전략적 요청사항이 있었습니다. 이에 따라 대용량의 로그도 실시간 분석이 가능하고 포괄적인 상관 분석도 가능한 보안 정보 및 이벤트 관리(SIEM) 솔루션을 검토하게 되었습니다.

#### •빅데이터 분석 요구

임직원 및 협력사 직원들의 인터넷 사용 시 발생하는 대용량 로그 및 트래픽 정보에 대한 원활한 분석을 위해 빅데이터 기반 기술 사용 요청

#### •컴플라이언스 관리 및 리포팅 시스템 교체 필요

감독기관의 주기적/비주기적인 검사 요청에 따른 대용량 데이터 검색 및 사전 대비

## / Solution /

### 기업 요구사항과 특성에 꼭 맞는 솔루션 제공

KB 국민은행은 기존 보안 관리 솔루션의 한계를 넘어 로그처리 성능, 상관분석 및 룰셋, 선제적 대응 등의 다양한 부분을 만족시킬 수 있는 솔루션을 찾은 끝에 IBM QRadar를 만날 수 있었습니다.

IBM QRadar는 다년간의 보안 관제 경험을 기반으로 다양한 기본 룰셋을 포함한 유연한 룰 적용 엔진을 제공하고 있어 KB 국민은행 특성에 맞는 보안관제 상관분석 룰셋 개발을 매우 용이하게 해 주었습니다.

빅데이터를 활용하여 학습에 기반한 이상징후 패턴 감지가 가능한 분석엔진은 잠재적인 보안 위협에 효과적인 선제적 대응이 가능하도록 해주었습니다.

## / Benefit /

### 보안 리스크 및 관리 비용 감소, 두 마리 토끼를 잡은 효과

KB 국민은행은 IBM QRadar를 통해 대용량 이기종의 IT 보안 로그들을 통합적으로 수집 및 분석 할 수 있는 로그 상관분석 시스템을 구축할 수 있었습니다. 이로써 방화벽, 침입탐지/방지 시스템, 웹 로그 등의 로그를 정규화하고, 수천만 건 이상의 대용량 로그에 대한 상관분석을 수행하여 보다 빠른 대응 및 안전한 로그관리가 가능해졌습니다. 또한 감독기관의 컴플라이언스 요청에 신속하게 대응할 수 있는 체계적이고 효율적인 통합 보안 관리 체계를 수립할 수 있었습니다.

실제 KB 국민은행은 IBM QRadar 구축을 통해 대응 시간 및 노동력 절감을 통해 리스크 비용의 감소, 컴플라이언스 비용 감소 등 여러 가치를 구현했고 그 혜택을 톡톡히 얻고 있습니다. 이제 KB 국민은행은 잠재적인 보안 위협에 효과적으로 대응하는 새로운 통합 보안 관리 체계 구축을 통해 은행권 최초로 선제적 위협 관리를 수행하는 보안 인텔리전스 시스템을 갖추게 되었습니다.

# “서비스면 서비스 보안이면 보안 하나부터 열까지 최고만 제공합니다”

하나캐피탈, QRadar로  
통합 보안의  
길을 찾다

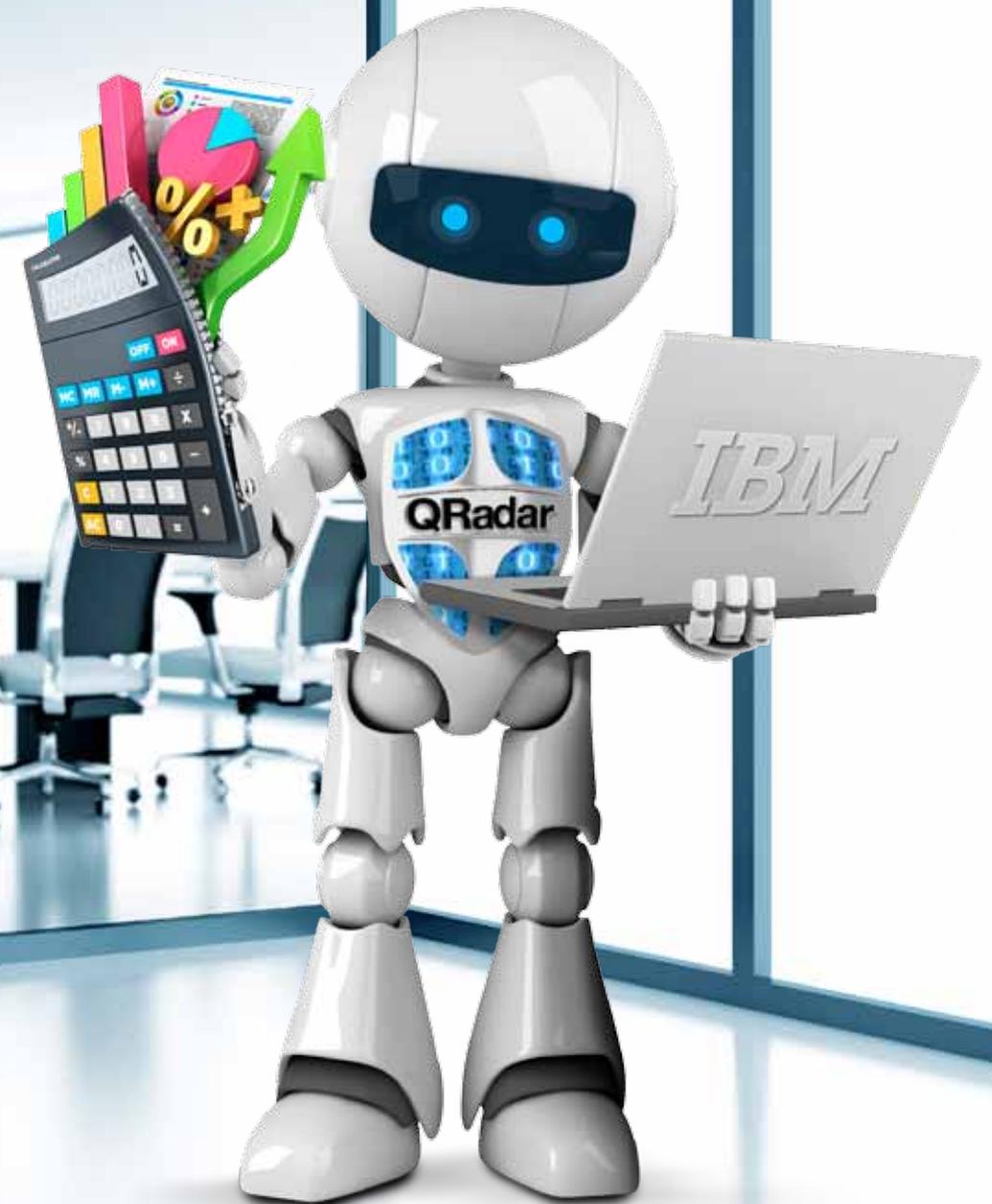
대규모의 IT 시스템을 운영하고 있었던  
하나캐피탈은 상시적으로 발생하는  
대량의 로그를 컴플라이언스 요건에 맞춰  
보다 정교하고 효율적으로 분석해야 했습니다.  
보안사고 예방을 위해서도  
효과적이고 통합적인 모니터링이  
반드시 이루어져야 하는  
상황이었습니다.

초우량 종합 금융 서비스 네트워크 실현이라는 비전 아래 하나캐피탈은 자동차의 리스 및 할부에서부터  
전세자금, 개인신용대출 등 다양한 금융 서비스를 제공하고 있습니다. 하나금융그룹은 새로운 금융  
서비스영역을 개척하고, 해외 금융 네트워크를 확대해 글로벌 금융그룹으로 성장할 것입니다.

산업별  
성공 사례-금융  
하나캐피탈



하나캐피탈





산업별 성공 사례-금융 / 하나캐피탈

# 다양한 보안 위협 상황을 한눈에 감지하는 통합 보안의 가시성 확보



## / Background /

### 컴플라이언스 충족을 위한 통합 보안 시스템의 필요성 대두

하나캐피탈은 전자 보안 시스템, 네트워크 장비, 서버, 애플리케이션, DB 등 상호 연동된 다양한 IT 장비와 시스템에서 발생하는 엄청난 양의 로그 관리에 어려움을 겪었습니다.

전자금융감독규정, 정보통신망법, 개인정보보호법 등 법률적 요구에 따라 하나캐피탈은 컴플라이언스 요건을 만족시키기 위해 방대한 로그를 체계적으로 수집, 저장, 관리하고 모니터링 할 수 있는 통합 로그 관리 및 모니터링 시스템이 필요했습니다.

## / Challenge /

### 효율적인 로그 분석과 효과적인 모니터링 환경 요구

기존 시스템을 통해 로그를 취합, 관리하고 있었지만 대규모 시스템에서 상시적으로 발생하는 방대한 로그를 종합적으로 관리, 분석하는 것은 불가능에 가까운 정도로 까다롭고 어려운 일이라고 판단되었습니다. 또한 단순 패턴 중심의 모니터링으로는 유사한 외부 보안사고에 대한 탐지 정책 수립과 모니터링 표준화에 어려움을 겪을 수 밖에 없었습니다. 덧붙여 보안사고 예방을 위해 각 관리자 및 개발자들에게 효과적인 로그 모니터링 환경을 제공하기도 쉽지 않은 상황이었습니다.

## / Solution /

### 자동화, 맞춤화, 정밀화로 보안 능력 업그레이드

새로운 보안 환경에 대한 요구를 충족시키기 위해 하나캐피탈은 IBM QRadar를 도입해 서버, 네트워크, DB, 보안장비, 백업 및 배치 스케줄러로그를 포함한 다양한 애플리케이션 로그를 실시간으로 편리하게 수집, 저장, 정규화 해주는 'Auto Discovery' 및 로그 소스 확장 기능을 적극 활용하였습니다.

관리자 및 개발자들이 다양한 로그를 목적에 맞게 검색하는데 불편함이 없도록 각 사용 목적에 맞추어 검색용 서치 템플릿을 등록한 'Quick Search' 및 '개인화 대시보드' 기능도 추가하였습니다.

또한 일련의 이벤트가 순차적으로 발생할 때 손쉽게 위협 사실들을 파악할 수 있도록 하는 'Sequence 룰셋'과 'offense' 기능으로 보안 사고를 예방하고 적극적으로 대응할 수 있게 되었습니다.

## / Benefit /

### QRadar를 통해 기대 이상의 보안 능력 확보

하나캐피탈은 IBM QRadar를 통해 수십여 종의 다양한 이기종 로그를 통합하여, 로그 컴플라이언스에 따른 법적 요건을 단기간에 갖출 수 있었습니다. 뿐만 아니라, 개발자들의 직접적인 서버 접근 없이 로그를 조회함으로써, 전산 개발 환경에 대한 보안 수준을 강화할 수 있었습니다.

또한 대시보드를 통해 다양한 이기종 로그들을 직관적으로 확인할 수 있게 됨에 따라 시스템 운영 상황을 보다 손쉽게 파악할 수 있게 되었습니다. 로그를 비롯한 네트워크로부터 Layer 7 가시성을 확보한 QFlow를 수집하고 로그와 함께 포괄적인 상관분석을 수행함으로써 다양한 보안 위협 상황에 대한 명확한 분석과 지속적인 추적 또한 가능해졌습니다.

# “1등급 청정 에너지, 1등급 통합 보안, 세계와 경쟁하는 1등 에너지 기업입니다”

E1, QRadar와 함께  
세계를 무대로  
에너지를 발산하다

E1은 청정 에너지 LPG만큼 완전무결한  
보안 솔루션 구축을 원했습니다.  
지속적이고 정교화된 보안 위협이  
날로 증가하면서 이를 방어하기 위한  
신규 시스템 도입을 결정했으며,  
새로 도입되는 보안 시스템은  
눈에 보이는 위협도, 눈에 보이지 않는  
잠재적 위협도 완벽하게 방어할 수  
있어야 했습니다.

E1은 국내 최초로 대규모 LPG 수입 사업을 추진하여 가스시대의 새장을 연 LPG 산업의 선도기업입니다.  
E1은 무공해 청정 에너지인 LPG의 대중화를 통해 국민의 삶의 질 향상에 기여해 왔으며,  
지속적인 내실경영과 적극적인 시장 개척으로 국내는 물론 해외시장에서도 경쟁력을 확보하여  
세계 LPG 산업의 리더로 성장하고 있습니다.

산업별 성공 사례  
-에너지  
E1





산업별 성공 사례-에너지/E1

# 잠재적인 보안 위협, 보안사고에 대응하는 완벽한 IT 보안 안전지대 구축!



## / Background /

### 개인정보보호법 시행에 따른 법적 컴플라이언스 대응

E1은 LAN, WAN에 대한 사전 점검 결과를 바탕으로, 날로 증가하는 지속적이고 정교화된 보안 위협에 대응하기 위해서 **실시간 위협 탐지를 기반으로 한 새로운 보안 시스템**을 구축하기로 결정하였습니다.

특히 실시간 상관 관계 분석 및 이상 행동 탐지, 리스크 높은 보안 위협 식별, 네트워크/애플리케이션/사용자 활동에 대한 모니터링 및 보고 기능 등 선제적 보안 기능에 초점을 맞춘 **'가장 고도화된 시스템 구축'**이 최우선 과제로 떠올랐습니다.

## / Challenge /

### 수동적 방어가 아닌, 선제적 대응이 가능한 솔루션 요구

E1은 '고객'을 최우선 가치로 두고, 다양한 보안 위협에 적극적으로 대응하기로 결정하였습니다. 이에 따라 내부 사용자 PC가 스팸발송 서버로 악용되거나, 악성코드에 감염되어 C&C 서버와 통신하여 웹 바이러스에 감염되는 경우 이상 트래픽 발생으로 내부 네트워크 서비스가 마비될 수 있으므로 이를 방지하는 것이 무엇보다 중요했습니다.

이를 위해서는 단순 로그 관리 수준을 넘어서, **실시간/선제적 보안 위협 대응을 위한 '보안 정보 및 이벤트 관리(SIEM) 솔루션 도입'**만이 해결책이 될 수 밖에 없었습니다.

## / Solution /

### IBM QRadar, 벤치마크 테스트 결과 가장 우수한 솔루션 증명

E1이 가장 적합한 SIEM 솔루션을 찾기 위해 고려한 사항은 **다양한 벤더의 보안 로그와 네트워크 트래픽을 함께 수집, 처리 분석할 수 있는 기능**이었으며, 무엇보다 이런 다양한 이벤트들을 실시간으로 분석하여 즉시 위협을 감지할 수 있는 기능에 중점을 두었습니다.

**1개월 간 진행된 벤치마크 테스트를 통해 여러 벤더 솔루션의 장단점을 비교 분석**하였으며, 가장 적합한 솔루션으로 IBM QRadar를 선정하게 되었습니다. IBM QRadar는 벤치마크 테스트 시작과 함께 E1이 직면한 다양한 보안 위협을 탐지함으로써 가장 우수한 솔루션으로 선정되었습니다.

## / Benefit /

### 눈에 보이는 위협도, 잠재적인 위협도 모두 방어하는 시스템 구축

IBM QRadar는 **다양한 벤더의 시스템에 대한 로그 분석을 지원**하였을 뿐만 아니라, **행위기반 분석, 비정상 이벤트/트래픽 탐지 등의 분석엔진 기능**을 제공하였습니다. 이를 통해 문제가 있는 스팸 발송 PC, C&C 서버 접속 PC, 웹 감염 PC 등을 실시간으로 탐지하여 사전 조치할 수 있도록 함으로써 보다 신속한 대응을 가능하게 하였습니다.

E1은 IBM QRadar 도입을 통해 기존 솔루션에서 취약했던 잠재적인 보안 위협에 대응하고, 이에 대해 보안 담당자가 실시간으로 대응할 수 있다는 자신감을 갖게 해주었습니다. 또한 직원들의 보안 정책 위반 사례나 남용에 대한 모니터링을 통해 사전조치할 수 있는 체계를 수립하여 서비스 안정화에 기여했습니다.



산업별  
성공 사례  
E1

# “게임에서도, 보안에서도, 새로운 기록 수립에 도전합니다”

Gravity, QRadar로  
보안이라는 중력에  
맞서 비상하다

게임이라는 특성상 네트워크 내외에서  
불법 침입 시도가 지속적으로 이어졌던  
Gravity는 정부의 보안 정책 준수를 위해  
노후된 보안 시스템을 교체해야 했습니다.  
내부인력 만으로도 전문가급의 관리가  
이루어져야 했으며, 잠재적인 위협도  
사전에 예방할 수 있어야 했습니다.

주식회사 Gravity는 대한민국의 게임 개발사이자 배급사이며, 2005년도에 나스닥에 상장되었습니다.  
전세계 76개 국가의 폭넓은 유저층을 확보하고 있는 MMORPG인 라그나로크를 비롯하여,  
다수의 온라인 게임 개발, 퍼블리싱 및 서비스를 수행하고 있는 글로벌 게임사입니다.

산업별 성공 사례  
- 온라인게임  
Gravity





산업별 성공 사례-온라인게임 / Gravity

# 자동화된 패턴 분석, 손쉬운 관리 기능으로 회사 내외부에서 발생하는 불법행위에 대한 가시성 확보



## / Background /

### 개인정보보호법 강화 및 내외부 보안 위협 행위 증가

다수의 불특정 사용자를 대상으로 하는 온라인 게임 특성상 게임 머니 탈취, 고객 서비스망을 통한 고객정보 유출 시도 등 내부 통신망에 대한 불법 해킹 시도가 끊임없이 이어지고 있었습니다.

또한 정부의 개인정보보호법 강화로 이를 준수하기 위한 로그의 통합관리에 대한 요구가 나날이 증가하고 있었습니다.

무엇보다 다수의 개발자를 포함한 내부 직원들의 불법 행동 (P2P 사용, 정보 유출 가능성) 등에 대한 지속적인 모니터링을 할 필요가 있었습니다.

## / Challenge /

### 애플리케이션 위주의 모니터링을 위한 솔루션 필요

이러한 목적을 이루기 위해서 Gravity는 로그 수집에 기반한 애플리케이션 위주의 모니터링 체계를 구축하는 데 초점을 맞추었습니다. 그러나 로그 수집만으로는 충분한 가시성을 확보하기 어려웠으며, 나아가 애플리케이션 모니터링 체계 구축이라는 목적을 달성하려면 대규모 추가 투자가 요구되는 상황이었습니다.

또한 내부 사용자망에 대한 가시성 확보에도 미흡함이 있었습니다. 따라서 이러한 모든 요건들을 만족시키는 솔루션을 찾기 위해 다각적인 검토가 이루어졌습니다.

## / Solution /

### 전문가의 도움 없이도 손쉽게 관리할 수 있는 솔루션 제시

다양한 솔루션을 검토하던 중 Gravity는 IBM QRadar가 모든 요구사항을 충족시키는 유일한 솔루션임을 알게 되었습니다.

IBM QRadar는 보안 장비에서 발생하는 로그들을 통하여 경계선에 대한 모니터링뿐만 아니라, Layer 7 영역에 대한 플로우 정보를 제공하여 네트워크망으로부터 다양한 애플리케이션의 식별 정보 및 사용 패턴을 파악할 수 있는 가시성을 확보할 수 있게 해주었습니다.

다양한 분야의 Default 룰셋을 제공하였고, 관리자가 비즈니스 목적에 적절한 룰셋을 손쉽게 만들 수 있도록 룰셋 마법사를 제공하여 관리편의성을 높여 주었습니다.

## / Benefit /

### 상관관계 분석, 패턴 분석을 통해 보안 운영 효율성 향상

Gravity는 IBM QRadar의 로그, 플로우 정보의 상호 상관관계 분석 및 주기적으로 업데이트되는 보안 DB 정보를 통해 PC의 악성코드 감염 여부 등을 빠르게 파악할 수 있게 되었습니다.

애플리케이션에 대한 직접적인 식별 및 자동화된 패턴 분석을 통하여 회사 정책에 맞지 않는 불법 프로그램 사용 여부, 회사 네트워크를 과도하게 점유하는 헤비 유저 등을 손쉽게 파악할 수 있었습니다. 이를 통해 애플리케이션 Payload에 대한 가시성을 확보하여 회사 보안 정책의 유효성(암호화된 채널 사용을 통한 인증 등)을 직접적으로 검증함으로써 보안 운영의 효율성을 제고할 수 있었습니다.

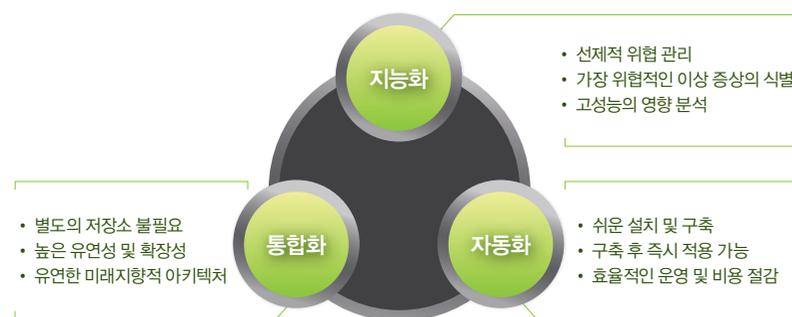


# 세계적인 기업들의 보안을 책임지는 IBM QRadar! 비교하면 비교할수록 선택의 이유가 확실해집니다

## 1

### 기업에 필요한 모든 보안 및 관리- 통합 보안 인텔리전스 플랫폼, IBM QRadar

IBM QRadar는 지능화, 통합화, 자동화를 통해 단순한 로그 수집 및 분석은 물론, 취약점 스캔을 통한 보다 정밀하고 포괄적인 상관관계 분석 및 컴플라이언스 관리를 제공하는 인공지능형 보안 인텔리전스 플랫폼입니다.



## 2

### 통합 콘솔 단일 데이터 아키텍처로 보안은 더 인텔리전트하게, 관리는 더 편리하게!

IBM QRadar는 롤 기반 액세스와 실시간 분석, 인시던트 관리 및 보고에 대한 글로벌 뷰를 제공하고 중앙집중식 사용자 인터페이스는 보안 운영 센터를 위한 탄탄한 기반을 제공합니다.



## 3

### 산업 특성에 따라, 업무 특성에 따라 맞춤 솔루션으로 최적의 보안 시스템 구축

IBM QRadar는 업종별, 기업별 비즈니스 특성에 따라 취약점 관리, 통합 로그관리, 복잡한 이벤트 분석, 네트워크 분석 등의 보안 솔루션을 맞춤형식으로 최적화되도록 구축할 수 있습니다.

제품명	특장점
<b>Log Management</b> 	<ul style="list-style-type: none"> <li>통합 로그관리</li> <li>중소기업/대기업 등 기업규모에 맞도록 적용</li> <li>엔터프라이즈 SIEM으로 업그레이드 가능</li> </ul>
<b>Vulnerability Manager</b> 	<ul style="list-style-type: none"> <li>취약점 스캔</li> <li>취약점 관리</li> <li>취약점 필터</li> </ul>
<b>SIEM</b> 	<ul style="list-style-type: none"> <li>통합 로그, 위협, 위험, 컴플라이언스 관리</li> <li>복잡한 이벤트의 분석 제공</li> <li>자산 프로파일링과 흐름 분석</li> <li>공격 관리와 워크플로우</li> </ul>
<b>Risk Management</b> 	<ul style="list-style-type: none"> <li>사전 위협 모델링 &amp; 시뮬레이션</li> <li>확장 가능한 구성 모니터링과 감사</li> <li>향상된 위협 가시성과 영향 분석</li> </ul>
<b>Network Activity &amp; Anomaly Detection</b> 	<ul style="list-style-type: none"> <li>네트워크 분석</li> <li>비정상 행동 감지</li> <li>SIEM과의 완벽한 통합</li> </ul>
<b>Network and Application Visibility</b> 	<ul style="list-style-type: none"> <li>Layer 7 애플리케이션 모니터링</li> <li>컨텐츠 캡처</li> <li>물리/가상화 환경 지원</li> </ul>



# 더 인텔리전트한 보안의 시작 IBM과 함께 보안 리스크 'Zero'에 도전하세요!

## 3

### IBM 보안 인텔리전스 프레임워크로 360도 전방위 보안의 혜택을 누리보세요

보안 컨설팅에서부터 보안 관리 및 관제 서비스까지, IBM X-Force 보안 연구소의 뛰어난 기술력으로 탄생한 보안 인텔리전스 프레임워크로 다양한 보안 위협에 통합적으로 대비하십시오.



## 1

### 보안 위협의 예측과 예방, 대응과 조치까지 기업의 보안, IBM이 책임지겠습니다

IBM은 기업의 보안 인텔리전스를 위한 IBM 보안 연구소를 중심으로 위협 관리, 취약점 관리, 구성과 패치 관리 등을 입체적으로 지원합니다. 또한, 네트워크와 호스트 침입방지, 네트워크 비정상 패턴탐지, 패킷 포렌식, 데이터 유출방지, 데이터베이스 모니터링, 통합 로그관리, 인시던트 대응 등의 보안 위협 요소에 대한 실시간 대응과 조치가 가능하도록 지원합니다.



## 2

### 전세계 130개국. 보안특허 3000여 건. 보안에 대한 IBM의 노력은 시간과 국경을 초월합니다

IBM은 세계에서 가장 폭넓은 보안 리서치, 개발 및 구축 능력을 제공하고 있습니다. 매일 130여 개의 국가에서 130억 건의 보안 이벤트를 모니터링하고 있으며, 현재 3,000여 건에 달하는 보안 관련 특허를 갖고 있습니다.

- 보안 운영 센터
- 보안 연구 조사 센터
- 보안 솔루션 개발 센터
- 보안 협회 지부

