

리테일 산업을 위한 IBM BigFix 엔드포인트 관리



온사이트 IT 지원이 없는 경우에도
규정 준수를 강화하고 비용 절감

주요 내용

- 광범위하게 분산된 환경 전체에서 엔드포인트 관리
 - PCI 보안 표준 준수 강화
 - POS 디바이스를 비롯한 다양한 운영체제 및 디바이스에 대한 중앙 집중식 제어 확보
 - 인터넷을 통해 간헐적으로 연결된 로밍 엔드포인트 관리
-

리테일 산업의 분산된 특성은 고객에게는 매우 유용하고 판매자에게는 기회이지만, IT에는 골칫거리입니다. 모든 매장마다 IT 직원을 배치할 수 있는 리테일 기업은 거의 없습니다. 기업이 서버에서 POS(Point of Sale), 셀프 서비스 키오스크, 데스크톱 컴퓨터, 로밍 노트북까지 전 세계에 분포된 수많은 컴퓨팅 디바이스를 관리하려면 어떻게 해야 할까요?

네트워크 전체에 변경 사항을 구현하려면 어떻게 해야 할까요? 이러한 변경의 결과를 실시간으로 보려면? 네트워크에 연결된 디바이스와 연결되지 않은 디바이스를 검색하려면? 데이터 유출, 보안 침해 및 불법 장비를 통한 액세스로부터 보호하려면 어떻게 해야 할까요?

특히 리테일 기업이 지불 카드 산업 데이터 보안 표준(PCI DSS : Payment Card Industry Data Security Standards)을 준수하려면 어떻게 해야 할까요? 보안, 취약점 관리, 패치 관리, 엔드포인트 보안 등에 대한 규제를 준수하도록 각 디바이스를 구성하려면 어떻게 해야 할까요?

다음 예는 두 회사가 이러한 문제를 어떻게 해결했는지 보여줍니다.

한 대형 소매상의 IT 관리자는 PCI DSS 평가가 필요한 사업 부문의 수가 거의 세 배로 증가하면서 규정 준수 사항을 매뉴얼로 수집하고 비교하는 노동 집약적 절차를 몇 주씩 수행해야 하는 상황에 직면했습니다. 새로운 엔드포인트 관리 솔루션을 구현함으로써 시스템 업데이트를 자동화하고 감사 절차를 대폭 개선할 수 있었습니다.



또 다른 리테일 기업에서는 모니터링 소프트웨어에서 다수의 오탐(False Negative) 경보가 발생함에 따라 보고서에 허가받지 않은 변경 사항이 포함되었는지 확인해야 했습니다. 새로운 엔드포인트 관리 솔루션을 구현함으로써 서버 및 POS 변경에 대한 신뢰성을 제공하고 오탐 비율을 80% 줄일 수 있었습니다.

이 두 회사는 BigFix® 기술 위에 구축된 IBM BigFix 엔드포인트 관리를 구현했습니다. 이 솔루션의 분산 엔드포인트 관리를 위한 중앙 집중식 자동화 기능은 규정을 준수하고 안전하며 응답성을 갖춘 리테일 환경을 지원하도록 가시성과 제어를 제공합니다.

점점 더 복잡해지는 리테일 에코시스템 지원

시스템 및 정보가 이전보다 훨씬 더 많이 사용되고 통합되고 지능적이 된 상황에서 고객 기대, 리테일 기회 및 공급망의 복잡성이 새로운 단계에 진입했습니다. 고객은 제품뿐 아니라 판매 기업의 가격과 경쟁사의 가격을 잘 알고 있습니다. 리테일 기업은 고객 행동과 시장 동향에 대해 더 많은 정보를 수집하고 있으며, 공급망은 더 넓은 범위에 걸쳐 더 많은 망으로 연결되고 있습니다.

이러한 광범위한 에코시스템을 지원한다는 것은 수천 개의 컴퓨팅 디바이스를 유지해야 한다는 뜻입니다. 해당 디바이스는 빠르고 원활하게 작동하여 성공에 필요한 일관성 있는 고객 경험과 효과적인 비즈니스 운영을 제공해야 합니다.

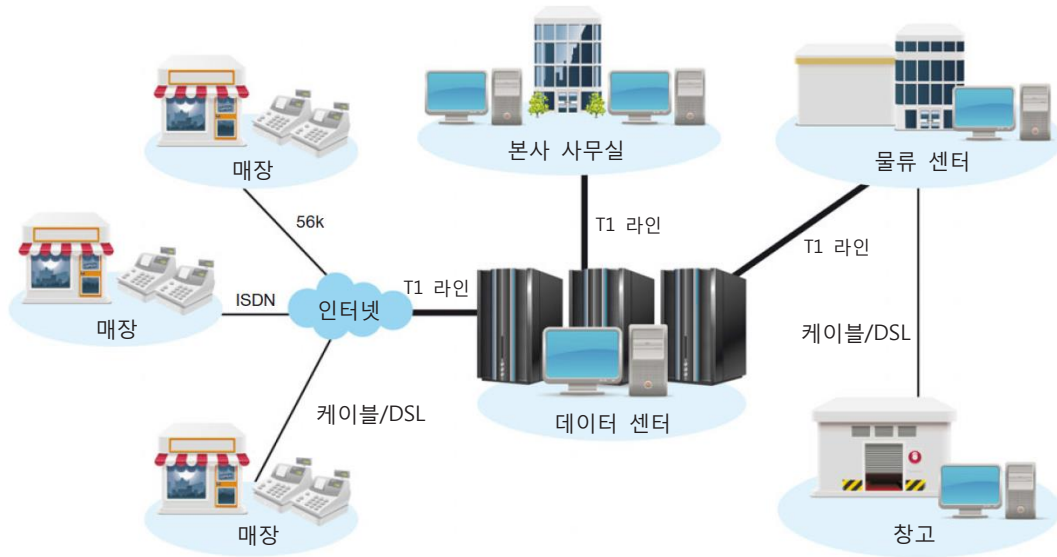
예를 들어, 국내 리테일 기업에서 비수기 동안 필요 없는 대량의 컴퓨터와 POS 터미널을 쓰지 않고 보관하기로 합니다. 일 년 중 판매가 급증하는 시점에, 보관하고 있던 시스템을 서비스에서 사용할 수 있도록 신속하게 제공해야 합니다. 디바이스를 찾고 목록을 만들어야 합니다. 가능한 한 빠르게 새로운 소프트웨어 버전을 설치하고, 패치 및 업데이트를 적용하고, 회사의 기술 및 규정을 준수하는 최신 상태로 만들어야 안전하게 거래할 수 있는 준비가 완료됩니다.

독특한 과제에 직면한 리테일 환경

리테일 환경은 효과적이고 효율적인 엔드포인트 관리라는 다음과 같은 과제에 직면해 있습니다.

- **각기 다른 인프라와 다양한 디바이스.** 리테일 엔드포인트에는 대부분 서버 및 데스크톱뿐만 아니라 POS 터미널, 금전 등록기에 내장된 PC, 키오스크, 무선/모바일 재고 추적 장비가 있습니다. 이러한 디바이스는 Microsoft® Windows, Linux®, Unix®, Mac 등 다양한 운영 체제에서 실행되는 경우가 많습니다.
- **"언제나 사용 가능한" 가용성에 대한 요구.** 각 매장에 설치된 디바이스는 본사, 물류 센터 및 공급업체에 다양한 정보를 다시 전달하는 프론트엔드 데이터 수집 노드의 역할을 합니다. 이러한 디바이스는 대부분 미션 크리티컬 디바이스로, 이 디바이스 없이는 비즈니스 거래가 이루어질 수 없습니다. 작업을 빠르고 투명하게 완료 및 검증하려면 공급망 인프라의 고가용성이 필수적입니다.
- **끊임없이 증가하는 규정 준수 요구 사항.** PCI DSS가 가장 일반적인 리테일 규정 준수 표준이지만, 리테일업체에서 Sarbanes-Oxley, HIPAA(Health Insurance Portability and Accountability Act), FCRA(Fair Credit Reporting Act) 및 기타 요구 사항을 준수해야 하는 경우가 많고 있습니다. 일반적인 규정 준수 활동은 대부분 지속적으로 수행되기보다는 예정된 감사에 대한 대응으로 이루어지는 경우가 많아 빠듯한 시간 내에 시스템이 규정을 준수하도록 만들어야 합니다.
- **비용 및 효율성 부담.** 리테일 경쟁은 낮은 비용의 제품 또는 서비스 공급자를 중심으로 이루어질 때가 많습니다. 비용 절감을 실현해야 하는 부담을 안고 있는 경영진에게 있어서 IT 투자는 대개 우선순위가 낮은 사항입니다. 하지만 수동으로 이루어지는 노동 집약적 IT 절차는 엔드포인트 관리 비용을 높이고 효율성을 떨어뜨립니다.
- **낮은 시스템 가시성.** 분산 환경에서는 각 엔드포인트에 무엇이 설치되었는지, 새로운 소프트웨어가 제대로 제공되고 설치되었는지, 패치가 필요한 엔드포인트가 어디인지 알기 어렵습니다. 가시성이 낮으면 규정 준수를 관리하기 어렵습니다. 이로 인해 기업이 허가 받지 않은 소프트웨어 또는 불필요한 소프트웨어에 대한 지출 등 기술 및 비즈니스 위험에 노출될 수 있습니다.

리테일 환경용 IBM BigFix 엔드포인트 관리



- **느린 구현 및 응답 시간.** 리테일 네트워크가 지역, 국가 또는 전 세계에 분산되어 겨우, 인프라를 유지 관리하기가 쉽지 않습니다. 인프라는 종종 대역폭이 낮고 지연 시간은 높은 네트워크에서 실행되는 경우가 많습니다. 그 결과 소프트웨어 배포와 같은 시스템 관리 작업이 사용 가능한 대역폭 중에서 상당 부분을 차지하여 네트워크 성능, 최종 사용자 생산성 및 비즈니스 거래 기능이 저하됩니다.

다양한 POS 디바이스 관리

특히 오프라인 매장을 운영하는 비즈니스는 리테일 인프라가 지점별로 컴퓨터 몇 대에 광범위하게 분산되어 있습니다. IBM BigFix 엔드포인트 관리는 다양한 플랫폼 및 디바이스 전체에서 여러 작업을 수행하는 중앙 집중식 관리 솔루션으로 통해 이러한 문제를 해결합니다.

BigFix 엔드포인트 관리의 통합 콘솔과 사용이 편리한 그래픽 사용자 인터페이스는 모든 엔드포인트를 추적하고, 각 엔드포인트에서 정확히 어떤 솔루션이 실행되고 있는지 보여주고, 이러한 정보를 사용하여 업그레이드, 변경 제어 및 기타 자산 관련 지출에 대한 예산 수립과 보안 의사 결정을 최적화할 수 있는 가시성을 제공합니다.

네트워크 연결성과 관계없이 단일 관리 서버에서 최대 250,000개의 엔드포인트를 지원할 수 있는 BigFix 엔드포인트 관리는 네트워크 성능이나 최종 사용자 생산성을 저하시키지 않고 자산 관리, 소프트웨어 재고 및 배포, 취약점 평가, 자동화된 맬웨어 방어, 규정 준수 및 정책 적용, 전력 절약 및 패치 관리를 수행하는 데 이상적인 플랫폼입니다.

POS 시스템이 대부분인 환경에서 BigFix 엔드포인트 관리는 POS 디바이스의 방대한 수량과 다양성으로 인해 발생하는 커다란 문제에 직면합니다. 엔드포인트 관리는 미숙한 직원이 무작위로 실행하는 재부팅, 매우 낮은 대역폭, 모뎀과 위성 등 불안정한 연결, 별도의 다운로드 및 제어 채널 등 리테일 산업 특유의 환경을 극복해야만 합니다.

관리 시스템은 POS 디바이스의 세금 테이블을 하루만 0으로 설정했다가 다시 일반 세율로 전환하는 "세금 공휴일"과 같은 리테일 산업 특유의 절차를 지원할 수 있어야 합니다. 리테일 기업에는 변경을 대규모로 감사하고 적용할 수 있는 BigFix 엔드포인트 관리 같은 도구가 필요합니다.

PCI DSS 규정 준수 문제 해결

시스템 관리에 익숙하지 않은 다수의 사용자와 금전 등록기, POS 터미널, 키오스크, 소형 재고 추적 디바이스 등 수많은 전문 기술이 혼재하는 환경에서 규정 준수는 까다로운 과제입니다. 사용자가 디바이스를 사용하면서 매장 또는 레스토랑을 운영하거나 고객을 지원하는 본연의 업무에 집중하지 못하게 되면, IT 관리 및 유지 보수가 중단되거나 위반될 가능성이 있습니다. 이러한 경우 그 어느 때보다 중앙 집중식 관리가 필요합니다.

규정 미준수로 인해 발생하는 결과는 상당히 클 수 있습니다. 고객은 자신의 개인 정보가 보호되지 않는다고 생각하는 매장이거나 레스토랑을 다시 찾지 않습니다. PCI 커뮤니티 내에서 신용 카드 회사는 규정을 준수하지 않는 매장에 벌금을 부과하거나 카드 사용을 중단시킬 것입니다.

BigFix 엔드포인트 관리는 리테일 업체가 PCI DSS 규정을 준수하는 데 필요한 가시성과 제어를 제공합니다. 이 솔루션은 엔드포인트에 상주하는 데이터 및 관련 요구 사항에 다음과 같은 주요 이점을 제공합니다.

- 비용이 많이 들고 감사에 집중된 규정 준수 활동이 아닌, 지속적인 규정 준수
- 며칠 또는 몇 주 만에 빠르게 배포되어 단일 관리 서버 및 콘솔에서 최대 250,000개의 엔드포인트를 지원
- 검증된 성능으로, 많은 리테일 기업에서 대역폭은 낮고 지연 시간은 긴 연결을 통해 간헐적으로 원격 연결되는 디바이스를 관리할 수 있도록 지원

BigFix 엔드포인트 관리를 사용하면 디바이스 유형과 상관없이 중요한 정보를 보관하는 엔드포인트를 보호하고 관리할 수 있습니다. 또한, 각 지점에서 사람이 직접 정보를 수집하거나 각 시스템에서 시간이 오래 걸리는 스캔을 수행할 필요 없이 낮은 대역폭 연결에서도 효율적으로 규정 준수 보고서를 생성할 수 있습니다. 지속적인 평가 및 조치를 통해 느리고 대응적인 규정 준수 및 감사 절차를 빠르고 효과적인 프로세스로 바꿀 수 있습니다.

사례 연구: 수백 개 지점에서 규정 준수

O'Charley's, Inc.는 미국에서 350개가 넘는 지점을 운영하는 레스토랑 그룹으로, 비용 효과적인 보안 및 시스템 관리가 언제나 중요한 우선순위였습니다. PCI 보안 표준 준수는 보안 목표의 핵심이지만, 레스토랑에 설치된 2,100개의 PC와 PC 기반 POS 터미널을 관리하면서 소프트웨어, 패치 및 업데이트를 직접 설치하도록 전국에 기술자를 파견해야 하는 어려운 문제에 직면하게 되었습니다.

O'Charley's 데이터 센터는 리테일 환경에서 흔히 볼 수 있듯이 상대적으로 느린 56k 데이터 회선으로 레스토랑에 연결되어 있었기에 원격 관리 및 애플리케이션 처리가 더 복잡했습니다. O'Charley's는 며칠 만에 분산된 모든 장비에 BigFix 엔드포인트 관리 솔루션을 배포하여 중앙에서 관리하는 시스템을 구축하여 원격 관리가 가능해지고 IT 워크로드 및 관련 비용을 절감할 수 있게 되었습니다.

엔드포인트에서 규정 준수 요구 사항 충족

BigFix 엔드포인트 관리는 다음과 같은 PCI DSS 표준 요구 사항을 처리합니다. 각 요구 사항에는 구현과 검증이라는 두 가지 작업이 필요합니다. BigFix 엔드포인트 관리는 명시된 요구 사항에 대하여 이러한 작업 중 하나 또는 둘 다를 지원합니다.

| 설명 | 솔루션 구성 요소 | 구현 | 검증 |
|--|--|----|----|
| 인터넷을 통해 기업의 네트워크에 접속하는 데 사용하는 모바일 및/또는 직원 소유의 컴퓨터에 개인 방화벽 소프트웨어 구현합니다. | 고정된 데스크톱이든 이동 가능한 노트북이든 관계없이 개인 방화벽 기능을 통해 일관적인 정책 적용 및 시스템 보호를 보장합니다. | √ | √ |
| 네트워크에 시스템을 설치하기 전에 항상 암호, SNMP 커뮤니티 스트링 같이 공급업체에서 제공하는 기본값을 변경합니다. | 구성 관리를 통해 기업 및 PCI 데이터 보안 표준 준수를 평가하고 적용할 수 있습니다. | | √ |
| 모든 시스템 구성 요소에 대해 알려진 모든 보안 취약점을 포함하고 업계에서 허용하는 시스템 강화 표준과 일치하는 구성 표준을 개발합니다. | 구성 관리에 불필요한 서비스 및 프로토콜을 제거하여 프로덕션 시스템을 강화하는 등의 보안 매개변수가 포함됩니다. | √ | √ |
| 악성 소프트웨어의 영향을 주로 받는 모든 시스템(특히 개인 컴퓨터 및 서버)에 맬웨어 방지 소프트웨어를 배포합니다. | 다양한 맬웨어 방지 옵션은 실시간 가시성, 확장성 및 통합 관리를 제공합니다. | √ | √ |
| 모든 맬웨어 방지 메커니즘을 최신으로 유지하고, 적극적으로 실행하며 감사 로그를 생성하도록 합니다. | 맬웨어 방지 기능은 안티바이러스 업데이트 날짜가 임박하거나 이미 경과한 엔드포인트가 어디인지를 IT에 알려줄 뿐 아니라 표준이 아닌 불법 애플리케이션을 실행하는 엔드포인트도 IT에 보고하도록 관리를 통합합니다. | √ | √ |
| 안전한 시스템 및 애플리케이션을 개발하고 유지 관리합니다. | 취약점, 패치 및 보안 구성 관리와 관련한 기능은 최고의 성능을 제공합니다. | √ | √ |
| 보안 시스템 및 프로세스를 정기적으로 테스트합니다. | 보안 구성 및 취약점 관리 기능에는 심각도 점수를 통한 호스트 기반 취약점 분석, 보안 구성 기준에 대한 준수를 정의하고 액세스하는 기능, 비정상적인 상황 또는 불법 활동이 의심되는 경우에 대한 경보를 설정하는 기능 등이 포함됩니다. | | √ |

자세히 알아보기

IBM BigFix 엔드포인트 관리에 대한 자세한 정보를 확인하려면 해당 지역의 IBM 담당자 또는 IBM 비즈니스파트너에게 문의하거나 <http://www-03.ibm.com/software/products/ko/endpoint-manager-family>

를 방문하시기 바랍니다.



© Copyright IBM Corporation 2015
한국아이비엠주식회사

(07326) 서울시 영등포구 국제금융로10
서울국제금융센터 (Three IFC)

TEL : (02)3781-7800
www.ibm.com/kr

2015년 8월

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 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.



Please Recycle

법적 요구사항을 준수하는지 확인해야 할 책임은 고객에게 있습니다. 고객의 영업에 영향을 줄 수 있는 모든 관련 법률 및 규정과 이러한 법률을 준수하는데 필요한 모든 조치를 식별하고 해석하기 위해 적절한 법률 고문의 자문을 구하는 것은 전적으로 고객의 책임입니다. IBM은 법률 자문을 제공하지 않으며 IBM의 서비스 및 제품은 고객이 관련 법률 및 규정을 준수하고 있음을 진술하거나 보증하지 않습니다.