



보안 위협으로 인한 사업 중단 방지하기



보안은 필수입니다

신용카드 번호. 건강 기록. 사회보장번호. 비밀번호. 귀사의 사업이 대상소비자인지, 환자인지, 시민인지의 여부에 관계없이, 귀사는 개인정보를 보호해야 한다는 기대를 받으며 이것이 필수인 경우가 많습니다.



리스크는 증가합니다

시간이 지남에 따라 리스크는 점점 더 커질 것입니다. 사물 인터넷과 클라우드 기술은 사람과 정보를 전례 없는 방식으로 연결하여 조직에게 과거에는 누릴 수 없었던 운영 통제력과 가시성을 제공합니다. 이에 대한 전망은 흥미롭지만 여기에는 리스크가 따릅니다.

2022년까지 약 500억 대¹의 장치가 상호 연결될 것으로 예상됨에 따라 조직 데이터와 기밀 데이터는 무수히 많은 취약점이 발생할 수 있습니다. 높은 수익성과 낮은 검거 확률로 인해(해커들의 기소율은 5 퍼센트에 불과합니다 ²), 사이버 범죄는 수그러들 기세가 보이지 않습니다.



그 대가는 무엇입니까?

한 건의 유출만으로도 큰 대가를 치르게 될 수 있습니다. 귀사는 생산성과 금전 상의 손실뿐만 아니라 평판까지 위험에 처할 수 있습니다.

그렇다면 무엇을 할 수 있을까요? 보안을 심각하게 생각하십시오. 조직에 보안 프로그램이 마련되어 있다 하더라도 잘못된 생각으로 인해 무결성을 해치고 불필요한 취약성이 발생할 수 있습니다.

\$390만:

데이터 유출 한 건으로 인한 평균 비용³

25,575건의 기록:

데이터 유출 한 건의 평균 규모³

12시간:

88%의 해커가 사이버 보안 방어를 뚫는데 걸리는 평균 시간⁴

197일:

조직이 유출 발생을 파악하는데 걸리는 평균 기간.³

대상:



소매업:

온라인 소매업체 로그인 트래픽의 80%는 도난 데이터를 이용하여 해커들에게 제공됩니다⁵

::::::: 정부/공공부문:

스파이 및 금전적 이득을 위한 주된 목표물로 핵심적인 동기를 제공합니다⁶

두 번째로 큰 해킹 대상 산업으로써 사이버 공격의 15%를 차지합니다⁶

제조업:

최근 몇 년 동안 다른 분야보다 더 높은 수준의 스파이 관련 유출 사건을 경험하였습니다⁶

잘못된 생각으로 귀사의 보안을 약화시키지 마십시오

보안 사고가 자주 발생한다는 사실이 널리 알려졌음에도 불구하고 많은 조직이 보안 문제에 안주하고 있습니다. 안전하다는 착각 속에서 안심하지 마십시오. 스스로 안전하다고 생각하신다면 문제가 나타날 수 있습니다.

"우리 조직은 목표물이 될 정도로 크지 않습니다."

사이버 공격의 43 퍼센트가 작은 기업을 대상으로 이루어집니다.6 해커들은 소규모 기업들의 자원 및 지식 부족을 노립니다. 해커들은 귀사와 연결된 더 큰 기업들에 접근할 수도 있습니다.

"우리는 우리 네트워크로 보호됩니다"

견고한 보안 계획은 여러 층으로 구성되며 끊임없이 진화합니다. 앞문이 닫혀 있어도 도둑들은 열린 창문으로 들어갈 수 있습니다. 실제로 한 연구에 따르면 방화벽과 안티바이러스 등 기존의 대응조치는 거의 해커들을 저지하지 못했으며 엔드포인트 보안 기술이 공격을 막는데 더 효과적이었습니다.4

"우리는 유출 사고가 발생한 적이 없으므로 우리 보안은 괜찮습니다."

유출이 발생했더라도 모를 수 있습니다. 조사에 따르면 한 기업이 유출을 감지하는데 197일이 걸릴 수도 있습니다.3

"우리는 이미 정식 보안 프로그램을 갖추었습니다."

좋습니다. 그 프로그램은 계속 변화하는 위협에 맞추어 계속 발전하고 있습니까? 귀사의 모든 기술에 적용됩니까? 한 번에 끝내는 접근 방식으로는 오늘날의 정교한 사이버 범죄에 대응할 수 없습니다.



"보안은 너무 복잡합니다."

잘 만들어진 보안은 직관적이고 쉽게 구현할 수 있습니다. 직원들에게 원활하게 적용되고 귀사의 IT가 관리할 수 있도록 간소화되었는지 확인하십시오.



"보안은 생산성을 떨어뜨립니다."

보안 시스템이 너무 번잡하다, 통합하기 어렵다, 운영을 지체시킨다는 불만은 흔하게 발생합니다. 하지만 유출은 업무를 완전히 마비시킬 수 있습니다. 해결책은 보안을 포함하여 설계된 기술을 선택하는 것입니다. 그렇게 하여 보안은 생산성을 저해하지 않고 업무를 도울 수 있습니다.



여러 층의 보안으로 조직을 보호하십시오

모든 보안 조치가 귀사의 요구에 부응하는 것은 아닙니다. 기술을 고려할 때, Zebra Technologies에 근본적으로 포함되어 있는 중요한 보안 속성을 고려하고 마음의 평화를 찾으십시오.



기본 탑재된 보호 기능과 성능:

처음부터 기술에 보안과 생산성을 통합한 브랜드를 선택하십시오. 저희 솔루션은 귀사의 성과를 높이는 동시에

고도로 효과적인 여러 보안 프로토콜 및 기능을 통합하고 있음을 알게 되실 것입니다.



자동화 보안 기능:

한때 IT 부서에서 몇 주가 걸려서 처리했던 Wi-Fi® 인증은 이제 자동으로 수행되어 여러분과 여러분의 팀의 안전한 연결을 가속화합니다.

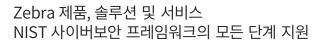


기사를 위한 맞춤 구성: 귀사의 보안 허용범위를 설정하고자 하십니까? Zebra는 귀사나 부서의 필요에 맞게 보안 수준을 조정하는 구성 솔루션으로 이를 쉽게 처리할 수 있습니다.



━ 단순화된 유지보수 및 서비스:

저희 보안 기능, 소프트웨어, 하드웨어는 최소한의 유지보수와 최대한의 가동 시간을 달성하도록 개발되었으며 시험을 거쳤다는 점을 믿어주십시오. 또한 필요하실 때 저희 24 시간 서비스 대응 팀을 이용하실 수 있습니다.



식별	리스크 관리 모니터링 프린터 보안 평가 마법사 전문 서비스	공급망 리스크 관리 보안 위원회
보호	LifeGuard™ for Android 프린터 보호 모드 장치 제어	PrintSecure 업데이트 자동 Wi-Fi Cert 관리 리스크 관리 프레임워크
감지	기업용 프린터 프로필 관리자 보안 모니터링	실시간 감지
대응	장치 관리 위협 감지 대응 조치	침해사고 대응 고객 알림
복구	전문 서비스 강화	확인된 상태로 복구



쉬운 통합:

Zebra와 함께라면 원활하고 빠른 통합이 가능합니다. 귀사의 산업과 애플리케이션을 깊이 이해하는 저희는 이미 귀사의 통합 필요성을 예측하고 충족하도록 솔루션을 설계하였습니다.



지속적인 감시와 지원:

장기간 제공되는 OS 보안 업데이트와 펌웨어 보강, 문제해결, 취약성 평가 및 내부 보안 협력을 함께 이용하십시오.



전세계적으로 인정된 모범 사례 준수:

Zebra는 ISO, 미국 표준기술원(The National Institute of Standards and Technology, NIST), 인터넷 보안 벤치마크 관리 센터(The Center for Internet Security Benchmark Controls) 등 전세계 보안 전문가들이 마련한 모범 사례와 지침을 준수한다는 점을 확인해주십시오. 저희 제품과 솔루션은 조직들이 HIPAA, PCI-DSS 및 GDPR을 준수하도록 지원하는 애플리케이션들에 이용되고 있습니다.



보안 기업 기술 분야의 리더:

기업용으로 Google Android's™ 운영체제를 강화한 브랜드와 함께 협력하여 최대 10년의 보안 OS 지원을 받으십시오. 저희 강화된 기업용 모바일 컴퓨터부터 보안 프린터 및 선구적 기술에 이르기까지, 저희가 하는 모든 일의 중심에는 생산성과 보안이 있다는 것을 아시게 될 것입니다.







炎ZEBRA

저희 보안 표준이 어떻게 귀사의 개선을 도와줄 것인지 알아보십시오.

방문하기: www.zebra.com/product-security

출처:

1. Juniper Research, 2018 2. Carbon Black Incident Response Threat Report(침해사고 대응 위협 보고서), 2018.11. 3. Ponemon Institute, 2018 and 2019 Cost of Data Breach(2018 및 2019 데이터 유출 비용) 4. Black Report, Nuix 2017 5. Shape Credential Spill Report 2018 6. Verizon 2019 Data Breach Investigations Report(데이터 유출 조사 보고서)

Zebra 장치와 기술, 서비스는 귀사의 생산성을 떨어뜨리지 않는 보안을 염두에 두고 설계되었습니다. 저희 보안을 귀사의 일선 직원들이 쉽고 원활하게 적용할수 있음을 알게 되실 것입니다. 구성 가능하며 스마트한 저희 기술을 이용하여실제 현실에서 실시간으로 경영 목표와 보안의 균형을 이루실 수 있습니다. 귀사의사업과 기술 전략을 최고의 수준에 이르도록 도와줄 Zebra를 믿어주십시오.

ZEBRA 및 양식화된 얼룩말 머리는 전세계 여러 관할지에 등록된 Zebra Technologies Corporation의 상표입니다. 다른 모든 상표는 각 소유자의 자산입니다. ©2019 Zebra Technologies Corporation 및/또는 계열사 판권 소유.