솔루션 개요

데이터 보호에 대한 인식 전환 필요

중요 데이터가 이동하는 경우에도 데이터를 보호해야 합니다.

Symantec™

소개

클라우드 시대가 본격적으로 시작되었습니다. 데이터는 끊임없이 이동하고 사용자는 어디서든 데이터에 액세스합니다. 이러한 디지털 세상에서 효과적으로 경쟁하기 위해서는 중요 데이터를 외부 사용자와 간단하게 공유하는 한편 지속적으로 데이터를 보호해야 합니다.

그러나 기존 보안 툴로는 이러한 데이터를 제대로 보호하기 어렵습니다.

- 2016년은 데이터 유출 사고가 2015년 대비 **40%** 증가한 기록적인 해였습니다.
- 2016년에 총 **1,209**건의 데이터 유출 사고가 발생했으며 그중 초대형 사고는 **15**건에 해당하고 **11억** 개의 신원 정보가 공개되었는데, 이는 2015년 **5억 6,400만** 개의 두 배에 달합니다.

또한 데이터 유출 시 평균 4백만 달러의 비용이 발생합니다. 이러한 피해는 경제적 손실에서 끝나지 않습니다. 고객의 신뢰 및 기업의 평판에 타격을 입히고 기업이 규정 위반에 따른 과징금 및 처벌을 받을 수 있습니다.

자세히 보기
2016년, 기록적인 데이터 유출 사고의 해

반드시 파악해야 할 3가지 사항

1. 중요 데이터가 어디에 있으며 그중 온프레미스 및 클라우드에 저장되어 있는 데이터는 얼마나 됩니까?

2. 누가 데이터에 액세스하고 그로 인해 어떤 리스크가 발생합니까?

3. 데이터가 잘못된 사람의 수중에 들어갈 경우 어떻게 보호합니까?

제대로 파악하지 못하는 기업들

기업에서는 종종 어떤 데이터가 중요한지 여부는 고사하고 데이터가 어디에 있는지조차 모르는 경우가 많습니다. 일반적으로 데이터는 정확하게 분류되지 않으며 올바르게 처리되지 않습니다.

- **실제로 보안 전문가의 2/3는** 회사의 중요 데이터가 어디에 있는지 제대로 파악하지 못한 상태입니다.
- **절반이 넘는** 기업에서 데이터에 대한 리스크를 완전히 파악하지 못하고 있습니다.

자세히 보기
IT 보안 전문가가 밤잠을 설치게 하는 11가지 데이터 문제

클라우드로 데이터를 보낼 때 해야 할 일

- 중요 데이터가 있는지 여부를 파악합니다.
- 일관된 보호를 제공합니다. 수동 프로세스는 오류가 자주 발생합니다.
- 종합적인 데이터 리스크 상황을 파악하고 어떤 활동 또는 사용자에게 조사가 필요한지 확인합니다.
- 제3자 또는 로밍 사용자와 관련된 리스크를 방지하면서 보호 대상 컨텐트에 대한 액세스를 허용합니다.
- 사용자 계정 감염 여부 확인 등 신원 검증의 무결성을 유지합니다.
- 데이터가 회사 네트워크에서 벗어나 잘못된 사람이나 조직의 수중에 들어간 경우에도 보호합니다.

Information-Centric Security, 새로운 접근 방식

보안 리스크를 관리하려면 보다 향상된 데이터 보호 방식이 필요합니다. Symantec Information-Centric Security 모델은 네트워크와 데이터 센터뿐 아니라 데이터도 보호합니다. 데이터가 여러 위치로 이동하고 많은 사용자에 의해 공유되는 동안 이를 추적하고 보호하면서 데이터 유출 리스크를 줄입니다.

시만텍은 DLP(Data Loss Prevention), 태깅(분류), CASB(Cloud Access Security Broker), 암호화, 분석, ID 인증 등 각종 데이터 보호 기술로 구성된 최고의 포트폴리오를 통해 통합적인 정보 중심 보안 모델을 완성합니다. 시만텍은 다양한 기능을 통합하여 효과적으로 보호하고 워크플로우를 자동화하며 가치 있는 데이터 자산에 대한 가시성을 제공합니다.

자세히 보기
시만텍 2017년 인터넷 보안 위협 보고서(ISTR)

중요 데이터는 자동으로 보호

Symantec™ Data Loss Prevention을 통해 중요 데이터가 무엇인지, 이러한 데이터가 제대로 보호받고 있는지 확인할 수 있습니다. 사무실에서나 이동 중이거나, 또는 클라우드 등 언제 어디서 데이터에 액세스하더라도 즉시 중요 데이터를 검색하여 모니터링하고 보호할 수 있습니다.

Symantec Data Loss Prevention은 데이터를 찾아 중요 데이터인지 여부를 확인하고 그에 대한 정책을 추가합니다. 이를테면 중요도가 매우 높은 특정 데이터는 외부로 전송할 경우 반드시 암호화하도록 정책을 설정할 수 있습니다. Data Loss Prevention은 클라우드 애플리케이션, 엔드포인트, 데이터 저장소, 이메일 및 웹 통신 등 다양한 채널을 통합적으로 모니터링하고 제어합니다.

"시만텍은 양식 탐지, 이미지 분석, 필적 인식 등 광범위한 데이터 유출 시나리오를 다룰 수 있는 첨단 기능을 활용하는 업계 최고의 통합 중요 데이터 탐지 기술을 제공합니다."

— **"Magic Quadrant for Enterprise Data Loss Prevention", Gartner, 2017년 2월**

인간의 지능을 활용하여 중요 데이터 탐지

DLP(Data Loss Prevention)가 데이터 지문 인식부터 이미지 분석까지 각종 자동화된 데이터 탐지 기술의 강력한 조합을 제공하지만 올바른 정책이 정의된 경우에만 제 기능을 할 수 있습니다. 정책이 수립되기 전에 중요 데이터가 생성되었다면 시만텍은 데이터 소유자가 데이터를 분류할 수 있게 합니다. Symantec Information Centric Tagging을 통해 직원들이 중요 데이터를 식별하고 분류하는 것이 가능하므로 보호의 범위를 확장하여 아직 정책이 적용되지 않은 중요 데이터까지 보호할 수 있습니다. 또한 Information Centric Tagging은 이메일 및 문서에 자동 워터마크를 적용하여 분류 레벨 및 보호 상태를 시각적으로 표시하는 방법으로 데이터 보호를 자동화합니다.

이러한 복합적인 방식을 통해 더 확실하게 지능적으로 데이터를 자동 탐지할 수 있습니다.

중요한 인사이트로 위험한 행위 규명

리스크 모니터링 및 이해는 반드시 필요합니다. Symantec Information Centric Analytics(Bay Dynamics 기술 기반)는 엔터프라이즈 환경의 사이버 리스크를 풍부한 컨텍스트 정보와 함께 통합적으로 조명합니다. Symantec Data Loss Prevention 보안 이벤트 데이터에서 상관관계를 분석하고 중요 데이터를 추출하여 사용자 행위에 대한 인사이트를 발굴함으로써 장기적인 보안 위협 및 위험 활동이 무엇인지 밝혀냅니다. Information Centric Analytics를 통해 방대한 보안 알림을 분석하고 우선 순위에 따라 리스크를 가중시키는 행위를 보여주는 사용자 목록을 생성하여 데이터 유출 또는 계정 도용 위험에 대한 레질리언스를 강화할 수 있습니다. 그러면 보안 위반 발생 가능성이 낮아지고 데이터 보호 규정에 대한 컴플라이언스가 향상됩니다.

클라우드의 보안 솔루션

CASB(Cloud Access Security Broker) 솔루션인 Symantec CloudSOC로 클라우드 애플리케이션 및 서비스에서 보안과 컴플라이언스를 유지할 수 있습니다. 이 솔루션은 섀도우 IT, 즉 IT 팀이 지원하지 않는 하드웨어 또는 소프트웨어에 대한 가시성을 제공하며 클라우드 애플리케이션의 데이터를 관리하고 클라우드 계정을 노리는 보안 위협을 차단합니다.

Symantec CloudSOC는 Symantec Data Loss Prevention 탐지 정책을 확장하여 Microsoft® Office 365®, Box, Dropbox 등 60여 개 클라우드 애플리케이션에서 사각 지대를 없앱니다. Symantec Data Loss Prevention과 CloudSOC의 통합으로 업계 최고의 시만텍 DLP(Data Loss Prevention) 엔진을 통해 클라우드 데이터를 검사하고 일관성 있는 정책 제어를 적용할 수 있습니다.

자세히 보기
Symantec Data Loss Prevention – CloudSOC를 통해 클라우드 지원 시작

암호가 취약점

확인된 전체 데이터 유출 사고 중에서 약한 암호, 기본 암호 또는 도용된 암호를 노린 해킹으로 인한 사건이 여전히 80% 이상을 차지했습니다. 그렇다면 적합한 사용자만 중요 기업 데이터에 액세스할 수 있도록 강력하게 제한하는 방법을 사용하면 어떨까요? 적합한 사용자도 잘못을 저지를 수 있습니다. 일례로 2016년에 Facebook 설립자이자 CEO인 마크 주커버그의 Twitter 및 Pinterest 계정이 해킹당했는데, 해커들의 주장에 따르면 암호 사용이 허술했기 때문입니다.

또한 강력한 암호를 사용하더라도 추가 인증 단계로 강화한다면 계정 도용 리스크를 대폭 줄이고 보다 편리한 사용자 경험을 제공할 수 있습니다.

더욱 강력해지는 암호화

데이터를 암호화하는 경우 유출 위험으로부터 보호할 수 있지만 생산성에 영향을 미치곤 합니다. 또한 복호화 키를 관리하는 방식에 따라 원격 데이터 액세스가 어려울 수 있습니다. 이처럼 번거롭고 불만스러운 경험 때문에 사용자들은 섀도우 데이터 시스템에 관심을 가지게 됩니다. 게다가 암호화된 데이터를 복호화한 사용자가 모든 액세스 권한을 갖게 되므로 (실수로 또는 고의적으로) 부적절하게 데이터를 공유할 수도 있으며, 그 경우 확실하게 제어할 방법이 없습니다.

Symantec Information Centric Encryption은 누가 데이터에 액세스하는지 모니터링하면서 더 우수한 사용자 경험을 제공합니다. 또한 동적으로 보호를 관리하고 원격으로 사용자 액세스를 제어할 수도 있습니다.

- **거부:** 개인 정보에 대한 모든 액세스는 소급적으로 거부합니다.
- **통합:** DLP(Data Loss Prevention) 및 CASB(Cloud Access Security Broker) 기술과 통합하여 중요 데이터를 탐지하고 적절하게 보호합니다.
- **보호:** 중요 데이터가 어디로 이동하든지 보호합니다.
- **제한:** 간편한 ID 기반 암호 복호화 기능을 통해 적합한 사용자에게만 데이터 액세스 권한을 부여합니다.
- **모니터링:** 누가 데이터에 액세스하는지 모니터링합니다.
- **파악:** 비정상적인 액세스 행위를 파악합니다.
- **제어:** 데이터 위치에 관계없이 언제라도 파일 액세스를 차단하여 제어합니다.

자세히 보기
2016년 Verizon 데이터 유출 조사 리포트

다중 인증으로 무단 액세스 차단

또 하나의 중요한 보안 단계는 데이터 수신자의 신원을 확인하고 직원이 언제 어디서나 어떤 디바이스에서도 안전하게 작업할 수 있도록 보장하는 것입니다.

Symantec Validation ID and Protection Service는 편리한 다중 인증 및 리스크 기반 인증 방식으로 네트워크, 애플리케이션, 클라우드에 대한 무단 액세스를 차단하여 데이터가 잘못된 사람이나 조직의 수중에 들어가지 않도록 보호합니다. 이를테면 직원이 LinkedIn 계정과 Salesforce 계정에 동일한 암호를 사용할 경우 발생하기 쉬운 계정 도용을 방지합니다.

자세히 보기
누구나 편리하게 사용할 수 있는 엔터프라이즈급 인증

"Gartner Magic Quadrant"는 시만텍을 10년 연속 데이터 유출 방지 부문의 리더로 선정했습니다. Forrester Research도 시만텍을 리더로 평가했습니다.

강력한 보안으로 비즈니스 보호

강력한 통합을 기반으로 하는 시만텍의 정보 중심 보안 방식은 데이터 공유가 끊임없이 이루어지는 현재 환경에서 안정적으로 비즈니스를 수행할 수 있도록 지원합니다.

자세한 내용은 현지 시만텍 세일즈 담당자 또는 비즈니스 파트너에게 문의

go.symantec.com/ICS

Symantec Information-Centric Security의 구성 요소

- **데이터 유출 방지:** 중앙 정책 제어로 모든 채널의 중요 데이터 탐색
- **Information Centric Tagging:** 사용자 중심의 데이터 태깅으로 분류 및 보호 강화
- **Information Centric Analytics:** 중요 데이터에 액세스하는 위험한 사용자 식별
- **CloudSOC:** 기존 데이터 유출 방지 정책, 워크플로우, 탐지 기능을 클라우드 애플리케이션으로 확장
- **Information Centric Encryption:** 정책 기반 암호화와 ID 액세스 통합
- **Validation and ID Protection Service:** 다중 인증으로 중요 데이터에 대한 액세스 보호

시만텍 소개

글로벌 사이버 보안 분야를 선도하는 시만텍은 기업, 정부 기관 및 개인의 중요한 데이터가 어디에 있든 안전하게 보호될 수 있도록 지원한다. 시만텍은 엔드포인트, 클라우드, 인프라 전반을 정교한 공격으로부터 방어할 수 있는 전략적인 통합 솔루션을 전 세계 기업과 기관에 제공하고 있다. 또한, 전 세계 5천만 이상의 개인사용자와 가정에서 시만텍 노턴 제품과 라이프록(LifeLock) 제품을 이용해 가정과 다양한 기기에서 디지털 라이프를 보호하고 있다. 시만텍은 세계 최대 규모의 민간 사이버 인텔리전스 네트워크를 통해 고도화된 지능형 위협을 탐지하고 고객들을 보호한다. 보다 자세한 정보는 시만텍 웹사이트(www.symantec.co.kr)와 페이스북, 트위터, 링크드인을 통해 확인할 수 있다.

Symantec™

서울시 강남구 테헤란로 152 강남파이낸스센터 28층 | TEL: 02-3468-2000 | FAX: 02-3468-2001 | www.symantec.co.kr