Symantec Data Loss Prevention for Cloud

클라우드의 데이터 검색, 모니터링, 보호

데이터시트: 데이터 유출 방지

대부분의 기업에게 있어 온사이트 애플리케이션을 클라우드로 이전하는 것은 민첩성을 높이고 비용을 절감하는 현명한 방법입니다. 하지만 중요한 기업 정보에 대한 가시성과 통제력을 유지하면서 클라우드의 이점을 활용하려면 어떻게 해야 할까요?

Symantec Data Loss Prevention(DLP) for Cloud Storage 및 Cloud Prevent for Microsoft Office 365는 클라우드 기반 스토리지 및 이메일을 위해 강력한 검색, 모니터링, 보호 기능을 제공하여 이러한 문제를 해결합니다.

- **Symantec DLP for Cloud Storage**는 안전한 협업을 지원하고 기업 사용자들이 Box에 저장 및 공유하는 모든 중요 파일에 대해 심도 있는 가시성을 제공합니다.
- **Symantec DLP Cloud Prevent for Microsoft Office 365**는 Office 365: Exchange Online과의 원활한 통합을 통해 안심하고 클라우드로 이메일을 마이그레이션하도록 지원하며 기업 사용자들이 보낸 중요 이메일을 면밀하게 모니터링하고 제어합니다.

모든 Symantec DLP 제품은 통합 관리 콘솔과 강력한 리포팅 툴을 제공하며, 이를 통해 중앙에서 데이터 유출 정책을 관리하고 인시던트를 재조정하며 DLP의 가치를 측정할 수 있어 편리합니다.

클라우드 스토리지

DLP for Cloud Storage는 강력한 컨텐트 검색 기능을 제공하므로 Box Business 및 Enterprise 계정을 손쉽게 검사할 수 있습니다. 여기서는 어떤 중요한 기업 정보가 저장되고 어떻게 사용되는지, 누구와 공유되는지 면밀하게 모니터링합니다. 뿐만 아니라 DLP for Cloud Storage는 Box 파일에 시각적 태그를 지정하고 직관적인 온라인 포털인 Symantec DLP Self-Service Portal을 통해 인시던트 재조정을 지원하는 방법으로 사용자가 정책 위반을 스스로 해결할 수 있게 합니다.

주요 특징

- 정규식 및 키워드, DB와 문서의 지문 인식, 학습과 같은 고급 컨텐트 인식 탐지 기술을 활용하여 Box 파일의 사용을 정밀하게 제어
- Box 및 DLP Self- Service Portal을 통해 사용자의 자율적인 문제 해결 지원
- 직관적인 관리 콘솔(Symantec DLP Enforce)에서 간편하게 클라우드 데이터 유출 정책을 관리하고 자동으로 인시던트 재조정

Cloud Prevent

DLP Cloud Prevent for Office 365는 Exchange Online을 위한 강력한 컨텐트 모니터링 및 보호 기능을 제공하여 더 신속하게 클라우드 이메일을 도입할 수 있도록 지원합니다. Cloud Prevent가 사용자에게 정책 위반을 알리고 안전한 이메일 전달을 위해 암호화 게이트웨이로 리디렉션하며 실시간으로 이메일을 차단하여 중요 데이터의 유출을 방지하므로 적시에 중요 기업 정보를 탐지하고 적절한 조치를 취할 수 있습니다. Cloud Prevent는 Rackspace를 통해 온사이트 또는 호스팅 환경에서 유연하게 구축할 수 있도록 지원합니다.

주요 특징

- 정규식 및 키워드, DB와 문서의 지문 인식, 학습과 같은 고급 컨텐트 인식 탐지 기술을 활용하여 클라우드 이메일의 사용을 정밀하게 제어
- 최종 이메일 전달을 위해 Symantec Email Security.cloud 서비스와의 원활한 통합 지원
- 직관적인 관리 콘솔(Symantec DLP Enforce Platform)에서 간편하게 클라우드 데이터 유출 정책을 관리하고 자동으로 인시던트 재조정

통합 관리 및 리포팅

데이터가 점차 다양한 디바이스 및 스토리지 환경으로 확산됨에 따라 정책을 일관성 있게 정의하고 적용하는 기능이 더욱 중요해졌습니다. Symantec DLP는 통합 관리 콘솔인 DLP Enforce Platform과 비즈니스 인텔리전스 리포팅 툴인 IT Analytics for DLP를 제공하므로 한 번만 정책을 작성한 다음 어디서나 적용하고 측정 가능한 방식으로 정보 리스크를 줄일 수 있습니다. **DLP Enforce 및 IT Analytics**는 아래와 같은 혜택을 제공합니다.

- **단일 웹 기반 콘솔**을 통해 엔드포인트, 모바일 디바이스, 클라우드 기반 서비스, 온사이트 네트워크 및 스토리지 시스템의 전 범위를 대상으로 데이터 유출 정책을 정의하고 인시던트를 검토, 재조정하며 시스템 관리를 수행할 수 있습니다.
- **사전 구현된 60여 개의 정책 템플릿** 및 편리한 **정책 작성기**를 활용하여 신속하게 DLP 솔루션을 가동하고 실행할 수 있습니다.
- 강력한 **워크플로우 및 재조정 기능**을 활용하여 인시던트 대응 프로세스를 간소화하고 자동화할 수 있습니다.
- DLP 활동에 **비즈니스 인텔리전스**를 접목시키는 **고급 분석 툴**을 통해 차원 높은 리포팅 및 임시 분석 작업을 수행할 수 있습니다. 여기에는 시스템 데이터를 추출하여 다차원 큐브로 요약한 다음 기업의 다양한 이해 관계자를 위해 유용한 리포트, 대시보드, 성과표(scorecard)를 생성하는 기능도 포함됩니다.

DLP Enforce를 통해 일관성 있는 정책을 적용하고 적절한 조치를 취함으로써 정보의 안전을 보장할 수 있습니다.

지금 바로 정보 보호를 시작하십시오.

시만텍은 고객의 보안 및 컴플라이언스 정책을 방화벽 외부로 확장함으로써 더 완벽하고 효과적인 정보 검색, 모니터링, 보호를 지원할 만반의 준비를 갖추었습니다. 검증된 구축 방법론, 직관적인 정책 및 인시던트 관리 툴, 고위험 채널 전반에 적용되는 포괄적인 지원을 통해 총소유비용을 낮춥니다.

go.symantec.com/dlp에서 자세히 알아보고 오늘날 클라우드 중심 모바일 환경을 위해 개발된 통합적인 정보 보호 솔루션의 이점을 확인하십시오.

시스템 요구 사항

Symantec DLP for Cloud Storage 및 Cloud Prevent for Office 365는 통합 관리 플랫폼과 컨텐트 인식 탐지 서버로 구성됩니다. 유연한 구축 옵션: 온사이트, 하이브리드 클라우드, (시만텍 DLP 전문화 파트너가 제공하는) 관제 서비스 중에서 선택할 수 있습니다. Symantec DLP는 다른 솔루션과 달리 분산된 환경에서 뛰어난 성능을 제공할 뿐 아니라 수십만 명 규모의 사용자 및 장치로까지 확장될 수 있습니다.

운영 체제	Microsoft Windows Server 2008, 2012 Red Hat Enterprise Linux VMware ESX 및 ESXi
프로세서	3.0GHz CPU 2개
메모리	6GB - 8GB
스토리지	140GB
네트워크	동선 또는 광섬유 1GB/100MB 이더넷 NIC 1개
데이터베이스	Oracle 11g Standard Edition

추가 정보

시만텍 웹 사이트

http://go.symantec.com/kr/dlp

21350066 06/15