

## DLP 및

## 암호화 구축

금융, 정부/공공, 의료, 보험 시장

## 은행 업계에서 검증된 DLP 성과

1

### 상황

2백 개의 분산형 지점을 보유하고 소규모 지역 은행에 IT 서비스를 제공하는 한 기업에서 수신 이메일에서 스팸과 바이러스를 필터링하고 아웃바운드 이메일에서 중요 데이터를 보호하는 경제적인 솔루션을 제공해야 했습니다. 금융 정보는 특히 민감한 정보이므로 DLP 솔루션은 금융 관련 규정을 철저히 준수해야 했습니다. 이 기업은 SOX, PCI, PII, 여러 정부에서 제정한 규정을 준수해야 합니다

### 기술적 과제

이 기업은 확장성, 안정성, 경제성을 갖춘 시스템을 고객에게 제공할 수 있어야 합니다. 지원하는 은행에 강력한 DLP 솔루션을 제공하는 것이 무엇보다 중요했습니다. 또한 다양한 은행을 지원하므로 각 은행에 따라 솔루션을 맞춤 구성할 수 있어야 했습니다. 그러나 은행에서 엄격한 규정의 준수를 입증하기 위해 보고서를 실행하도록 지원하는 것도 중요했습니다. SOX, PCI, PII, 정부에서 제정한 몇몇 규정을 준수해야 합니다.

### Cisco의 강점

Cisco IronPort는 경제성과 확장성까지 갖춘 종합 이메일 보안 솔루션을 제공할 수 있었습니다.

Cisco IronPort는 DLP의 선두 주자인 RSA와 손잡고 Cisco IronPort 이메일 어플라이언스에서 통합 DLP 솔루션을 제공했습니다. 이 RSA DLP 솔루션에는 미리 정의된 100여 개의 정책이 포함되어 미국 및 전 세계 규정의 준수를 지원합니다. 따라서 기업에 따라 맞춤형 솔루션을 간단하게 구성할 수 있습니다.

이 솔루션은 Cisco IronPort 솔루션과의 통합을 지원하므로 간편하게 클라우드 또는 어플라이언스에서 DLP 정책에 대한 보고서를 실행하여 은행의 규정 준수를 입증할 수 있습니다. 관리자는 실시간 및 예약 보고서에 액세스하면서 정책, 심각도, 발신자를 기준으로 대표적인 DLP 이메일 위반 사례를 검토할 수 있습니다. 또한 메시지 추적 기능으로 특정 DLP 위반에 해당하는 메시지를 검색할 수 있습니다. 은행은 이 두 가지 추적 시스템으로 DLP 솔루션의 유효성을 입증할 수 있습니다.

## 신뢰 관계 구축

### 2

#### 상황

워싱턴 DC와 웨스트버지니아 찰스턴에 각각 본사를 둔 이 고객은 75억 달러 규모의 지주 회사로 웨스트버지니아, 버지니아, 워싱턴 DC, 메릴랜드, 오하이오에 130여 개의 종합 서비스 지점을 두고 있습니다. 이 기업은 은행 규정을 준수하기 위한 DLP 및 암호화 솔루션을 필요로 했습니다

#### 기술적 과제

이 고객은 기존 Cisco IronPort Email Security Appliance가 있지만, 암호화 및 DLP 솔루션의 모든 대표적인 벤더 제품을 검토하고자 했습니다. 구체적인 인프라, 기능, 예산 요구 사항에 부합하는 최상의 제품을 찾았습니다.

#### Cisco의 강점

다양한 솔루션을 검토하는 과정에서 Cisco IronPort가 기존 인프라를 기반으로 하고 만일의 지장을 최소화하면서 최상의 솔루션을 제공할 수 있음이 분명해졌습니다. 고객은 네트워크에 Cisco IronPort ESA를 사용하고 있으므로 암호화 및 DLP 솔루션을 추가하는 것은 기능 업그레이드 및 활성화의 차원이었습니다. RSA DLP 전략은 100여

개의 사전 정의된 정책으로 구현되므로 알맞은 정책을 선택하여 적용하면 해결됩니다. 이 고객은 이미 인바운드 이메일 보안 솔루션에 만족한 상태이므로 동일한 신뢰 받는 브랜드로 아웃바운드 보안을 구현하는 것도 희소식이었습니다. 또한 고객은 Cisco IronPort가 고객과 긴밀하게 공조하면서 향후 DLP 요구 사항에 부합하는 전략을 제공하는 것에도 만족했습니다. Cisco IronPort는 가장 뛰어나고 편리한 솔루션일 뿐 아니라 헌신적인 파트너였기 때문에 이 고객은 Cisco IronPort의 이메일 DLP 솔루션 구축을 선택했습니다.

## 적용 범위를 확장하면서 비용 절감

### 3

#### 상황

이 고객은 카운티 경찰국을 비롯하여 카운티 정부를 위한 이메일 서비스를 지원합니다. 모든 직원이 기밀 정부 데이터를 보호할 수 있도록 암호화 및 DLP 솔루션을 구축해야 했습니다.

#### 기술적 과제

이 고객은 암호화 및 DLP 요구 사항을 모두 해결할 경제적인 솔루션을 찾았고, 또한 모든 직원까지 포함하도록 서비스 범위를 확장하고자 했습니다. Zix 기반의 암호화 솔루션이 있었지만, 엄청난 비용과 제한적인 구축 때문에 대체 하길 원했습니다. 기존의 속도로는 직원의 일부에게만 암호화를 지원할 수 있었고, DLP 솔루션은 없었습니다.

#### Cisco의 강점

고객은 Cisco IronPort가 DLP와 암호화의 복합 솔루션을 제공할 수 있다는 데 기뻐했습니다. 다른 Cisco 솔루션을 성공적으로 구축하여 매우 만족스럽게 사용한 적이 있기 때문입니다. 현장 평가를 실시하고 DLP의 적중률과 보고 기능에 감명 받았습니다.

Cisco IronPort가 손잡은 RSA는 뛰어난 적중률과 낮은 오탐지율을 자랑하는 DLP 솔루션을 제공합니다. 또한 Cisco IronPort는 DLP 위반 보고서를 구현하여 간단하게 DLP 활동을 추적하고 관리할 수 있게 했습니다. 관리자는 실시간 및 예약 보고서에 액세스하면서 정책, 심각도, 발신자를 기준으로 대표적인 DLP 이메일 위반 사례를 검토할 수 있습니다.

고객은 적중률과 성능뿐 아니라 비용 구조에도 만족했습니다. Cisco IronPort의 암호화 및 DLP 솔루션으로 경쟁 제품보다 상당한 비용을 절감할 수 있었습니다. 이 고객은 Cisco IronPort 솔루션으로 경쟁 제품보다 훨씬 저렴한 비용으로 모든 사용자에게 DLP 및 암호화 솔루션을 구축할 수 있었습니다.

## 의료 업계에서 커뮤니케이션 개선

### 4

#### 상황

한 대형 지방 의료 기관은 통합 의료 서비스 시스템을 운영하면서 응급실, 입원, 첨단 수술, 재활 및 홈케어까지 다양한 의료 분야에서 우수한 품질의 서비스를 제공합니다. 이 고객은 중요한 개인 의료 정보(PHI)를 식별하고 보호하기 위한 암호화 및 DLP 솔루션을 모두 구현해야 했습니다.

#### 기술적 과제

몇 년 전부터 Cisco IronPort Email Security Appliance를 네트워크에 구축하여 사용하던 이 고객은 인바운드 이메일 보안에 매우 만족했습니다. 규정 준수 및 환자 의료 정보의 이메일 전송에 대한 우려 때문에 추가적인 요구 사항에 따라 이메일 암호화 및 DLP 솔루션의 형태로 아웃바운드 보안을 구현해야 했습니다. 의사가 다른 의료진, 보험사, 환자와 안전하게 통신할 수 있는 새로운 기술이 필요했습니다.

#### Cisco의 강점

Cisco IronPort ESA가 구현된 인바운드 보호에 대단히 만족했던 이 고객은 Cisco 브랜드에 대한 신뢰와 확신으로 Cisco DLP 및 암호화 솔루션에도 관심을 나타냈습니다.

이 고객은 여러 솔루션을 조사한 후 Cisco가 자신의 요구 사항에 부합하는 완전한 통합 이메일 보안을 제공할 수 있다는 데 이내 감명 받았습니다. Cisco IronPort의 아웃바운드 이메일 암호화 및 DLP가 높은 지지를 받으면서 이 고객에게 적절한 최상의 솔루션으로서 더 확실하게 검증되었습니다.

이 기업은 특히 Cisco IronPort가 RSA와 손잡았다는 사실에 만족했습니다. DLP 분야에서 리더십과 전문성을 갖춘 업체였기 때문입니다. 사전 정의된 템플릿과 낮은 오답지율 덕분에 경쟁 제품과 더욱 차별화되었습니다. 이제 Cisco IronPort DLP 솔루션을 기존 인프라에서 운영하고 있는 이 고객은 자신 있게 안전한 방식으로 외부 의료진, 보험사, 환자와 커뮤니케이션할 수 있게 되었습니다.

## 현재 및 미래에 손쉬운 통합

### 5

#### 상황

이 회사는 종합 금융 서비스 기관으로 개인, 기업, 법인 투자자를 대상으로 각종 금융 자문과 서비스를 제공합니다. Google Postini 이메일 보안 솔루션을 사용했지만, 규정 준수 요건에 부합하는 DLP 솔루션을 찾았습니다.

#### 기술적 과제

이 고객은 펜실베이니아 및 매사추세츠에 시행되는 규정에 부합하는 최상의 DLP 솔루션을 찾았습니다. 또한 GLBA, Sarbanes-Oxley, PCI, HIPAA 및 기타 일반적인 규정 요건도 해결해야 했습니다. 마지막으로, 이 고객은 기존 인프라와 완벽하게 통합되는 솔루션으로 향후 규정 준수 요건도 해결할 수 있기를 원했습니다.

#### Cisco의 강점

이 고객은 DLP 솔루션에 대해 조사하면서 RSA DLP와 Cisco IronPort ESA의 통합 솔루션이 제공하는 최고의 성능에 감명 받았습니다.

새로운 이메일 보안 솔루션을 찾진 않았지만, Cisco IronPort ESA를 도입하고 이메일 보안 및 DLP를 하나의 어플라이언스에서 번들 구성하는 것이 훨씬 더 경제적이라는 사실을 깨달았습니다. 이 통합 솔루션으로 이메일 보안을 강화할 뿐 아니라 구축 과정에서 상당한 비용을 절약할 수 있다는 점도 알게 되었습니다. Cisco IronPort ESA는 기존 인프라에 손쉽게 통합될 수 있으며, 번들로 구성된 RSA DLP는 이 고객이 찾던 최상의 DLP 솔루션이었습니다.

고객은 특히 Cisco IronPort Email DLP 솔루션이 100여 개의 사전 정의된 정책을 기본적으로 제공한다는 데 기뻐했습니다. 즉 규정 요건이 바뀌더라도 다양한 정책을 수월하게 구현할 수 있음을 의미했습니다.

## 단일 플랫폼 찾기

### 6

#### 상황

500여 명의 가입자를 보유한 한 대형 생명보험사가 이메일 보안 솔루션을 통합해야 했습니다. 이 회사는 인바운드 이메일 보안과 아웃바운드 검사, DLP, 암호화를 모두 제공할 수 있는 단일 벤더를 원했습니다.

#### 기술적 과제

이 회사는 암호화, DLP, 인바운드 이메일 보안을 위한 단일 솔루션을 찾았고 단일 벤더와 함께 일하기를 강력히 희망했습니다. 규정 요건 준수를 지원할 수 있는 DLP 솔루션이 필요하다는 점을 특히 강조했습니다.

#### Cisco의 강점

고객이 여러 솔루션의 환경을 검토하면서 많은 벤더가 자신의 문제점 중 하나에는 적합한 솔루션을 제공하지만 이 3가지 영역 모두에서 최상의 성능을 제공할 수 있는 업체는 드물다는 사실을 알게 되었습니다. 이 고객은 결국 Cisco IronPort ESA를 선택했습니다. 이메일 보안, 암호화, DLP에서 최고의 성능을 제공했기 때문입니다.

Cisco IronPort는 이 회사의 이메일 게이트웨이를 통합하여 고객이 간단하게 구축하고 편리하게 사용할 수 있게 했습니다. DLP가 핵심 요건이었으므로 고객은 Cisco IronPort ESA와 통합형 RSA 이메일 DLP 솔루션을 함께 구축했습니다. 이 DLP 솔루션의 간소화 및 정확성은 인상적이었습니다. 버튼만 누르면 관리자가 사전 정의된 RSA 이메일 DLP 정책을 실행할 수 있습니다. 이는 미국 중심의 HIPAA, 영국 중심의 Data Protection Act뿐 아니라 PCI DSS(Payment Card Industry Data Security Standards)와 같은 비정부 규정도 지원하도록 설계되었습니다.

이 고객은 오탐지율이 낮다는 데에도 만족했습니다. DLP 솔루션에서 자주 발생하는 문제이기 때문입니다. RSA Email DLP의 사전 정의된 정책은 RSA의 정보 정책 및 분류 연구 팀에서 개발한 것으로 고급 콘텐츠 분석 기법을 적용하여 오탐지를 줄이고 적중률을 극대화합니다.