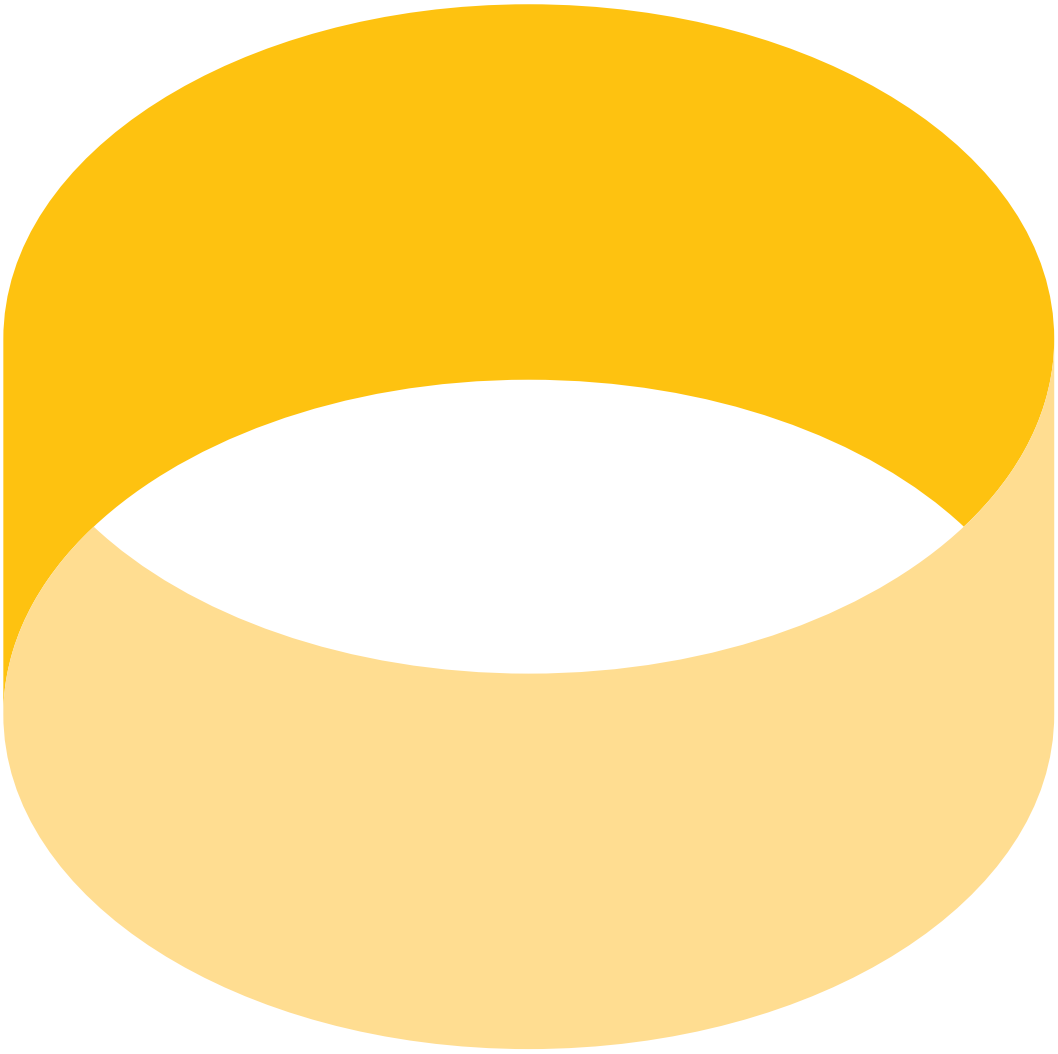

Office 365 구현 계획 시작

백서

작성자
Deena Thomchick
시만텍 클라우드 담당 상임 이사

Symantec™

준비 완료

귀사는 Office 365를 도입하려 합니다. 귀사는 부분적으로 Exchange Online을 구축하든지 직접 100% 클라우드로 전환하든지에 관계없이 Office 365를 도입하기로 결정했으며 최대한 신속하게 진행할 계획입니다. SaaS 도입을 본격적으로 시작하기 전에 Exchange Online 및 기타 Office 365 요소를 구현할 때 결정해야 하는 핵심 사항을 고려해야 합니다. 잠시 시간을 내어 아래와 같이 귀사가 본 백서에서 다루는 항목에 어떻게 접근할지 생각해 보십시오. 이러한 사항은 Office 365 구축에서 "해야 할 일" 목록에 영향을 줄 수 있는 요인입니다.

성능 계획

Office 365로 이전하면 Microsoft 라이센싱 비용이 감소되지만 대역폭 요구 사항 및 활성 상태의 인터넷 연결 수가 증가하면서 새로운 보안 요구 사항이 발생하게 됩니다. 따라서 Office 365 보안 요구 사항을 해결하기 위한 예산을 배정해야 합니다. 많은 기업이 이러한 요구 사항을 간과했습니다.

일반적인 Exchange Online 사용자 1명이 애플리케이션을 운영할 때 6개 이상의 인터넷 연결이 활성 상태여야 하며 그에 따라 인터넷 트래픽이 200MB 가량 증가합니다. 귀사는 이렇듯 증가하는 인터넷 트래픽과 동시 연결 수를 수용할 수 있습니까?

이러한 증가에 준비된 상태인지 확인하기 위해 인터넷 대역폭 및 네트워크 인프라스트럭처를 평가했습니까?

사용 중인 보안 솔루션은 이러한 트래픽 증가를 처리할 수 있습니까? Office 365 연결을 수용하기 위해 보안을 축소하는 경우가 있지만 현재의 보안 위협 환경을 고려하면 매우 위험한 전략입니다. 당장 예산을 절약했다가 추후 훨씬 더 큰 비용을 치르게 될 수도 있습니다.

Office 365를 위한 보안 대비

클라우드 애플리케이션, 특히 Office 365와 같이 비즈니스에 핵심적인 애플리케이션의 도입을 계획할 때 여러 보안 문제를 해결해야 합니다. 비즈니스의 상당 부분이 Office 365 클라우드로 이전하는 경우 귀사를 보호하고 컴플라이언스를 유지하기 위해 보안을 추가하고 강화할 준비가 되셨습니까?

Elastica는 클라우드 애플리케이션의 비즈니스 대비 상태 평가(Business Readiness Rating)를 위해 7가지 카테고리에서 85가지 이상의 특성을 분석합니다. 시만텍은 Office 365 특성에 대한 분석 및 대규모 클라우드 애플리케이션 도입 프로젝트를 수행한 경험을 바탕으로 아래와 같이 고객이 검토할 수 있도록 계획 카테고리를 분류했습니다.

- 액세스 제어
- 서비스 특성
- 관리 제어
- 컴플라이언스 및 책임
- 데이터 보호 및 거버넌스

Office 365를 위한 액세스 제어

Office 365 구현을 위해 설정할 암호 제어, 인증, 신원 정보 관리 시스템은 무엇입니까? Office 365는 비즈니스 환경을 지원하는 클라우드 플랫폼으로 다양한 액세스 제어 옵션을 활용할 수 있습니다. 공격자는 계정 인증 정보를 표적으로 삼기 때문에 보안 사용자 인증 및 사용자 액세스 전략을 구현하는 것이 중요합니다.

통합 신원 정보 관리(Federated Identity Management)를 위해 사용하는 것은 무엇입니까? OAuth 또는 SAML입니까? Office 365는 OpenID를 지원하지 않습니다.

무차별 공격으로부터 계정을 보호하려면 어떻게 해야 합니까? CAPTCHA를 활용하거나 로그인 실패 반복 시 점진적 응답(progressive response)을 설정할 수 있습니다.

다중 인증(Multi-factor Authentication, MFA)을 구현해야 합니다. 암호만으로는 충분한 보안이 되지 않습니다. Office 365와 같이 비즈니스에 핵심적인 시스템의 경우 더욱 그렇습니다. Office 365에서는 SMS 또는 모바일 앱을 통해 MFA를 제공할 수 있습니다. 현재 Office 365는 USB 토큰, 스마트 카드, 보조 이메일, 보안 질문, 생체 인식 기술을 통한 MFA를 기본적으로 지원하지 않습니다. 이러한 옵션을 사용하려면 해당 서비스를 제공하는 SSO(Single Sign On) 솔루션을 찾아야 합니다.

필요한 암호 품질 요구 사항을 결정하십시오. Office 365는 최소 암호 길이 및 강력한 암호 형식을 필요로 합니다. 사용자는 정기적으로 암호를 변경해야 합니다. 사용자가 암호를 잊어버린 경우 암호를 재설정하고 복구하는 기능이 기본적으로 제공됩니다.

Office 365에 사용 가능한 디바이스를 제한하는 액세스 제어를 설정하고 싶으십니까? 가능합니다. 단, IP 주소 범위에 따라 로그인을 제한할 수는 없습니다. 디바이스에서 Office 365로 수행할 수 있는 작업을 제어하고 싶으십니까? 예를 들어 BYOD 디바이스는 Office 365에 액세스할 수 있지만 관리되지 않는 디바이스에 파일을 다운로드할 수는 없습니다.

Active Directory(AD)와의 통합 기능을 활용하고 싶어할 수도 있습니다. 대다수 기업처럼 귀사도 AD를 사용하는 경우 바람직합니다. Office 365는 LDAP 통합을 지원하지 않기 때문입니다.

이미 SSO(Single Sign On) 솔루션이 있고, Office 365에 사용할 예정이십니까? 아직 없다면 각종 클라우드 애플리케이션뿐 아니라 내부 또는 프라이빗 클라우드 시스템도 다룰 수 있는 솔루션으로 도입하는 것도 가능합니다.

Office 365 서비스 특성

Office 365는 프라이빗 Microsoft 호스팅 플랫폼에서 호스팅됩니다. 멀티테넌트 환경으로, 고객 데이터는 데이터 레벨에서 분리됩니다.

웹 기반 서비스 형태로 이용할 수 있으며 데스크탑 클라이언트 및 기본 모바일 앱을 모두 지원합니다. Office 365를 사용하기 위해 이 모든 방식을 활성화할 경우 사용 방식에 따라 추가 보안 제어를 설정할 필요성을 고려해야 합니다. 사용자가 모바일 앱 또는 웹 인터페이스를 통해 계정에 액세스할 경우 다중 인증이 필요할 수도 있습니다.

다른 애플리케이션 또는 귀사의 웹 사이트를 Office 365에 연결하는 것을 고려한 적이 있으십니까? 귀사가 선택할 수 있는 옵션 중 하나입니다. Office 365는 Office Dev Center 온라인에서 API 카탈로그를 제공하며 모든 API가 REST 서비스입니다.

관리 제어

어떤 관리 액세스 제어가 필요하십니까? Office 365에서 제공하는 역할 기반 액세스 제어를 활용할 예정입니까? 이미 역할을 정의하셨습니까, 아니면 역할을 생성해야 합니까?

감사 추적은 컴플라이언스 및 침해 사고 대응에 매우 중요합니다. Office 365에서 기본 제공하는 제어 기능으로 관리자 및 엔드유저의 활동을 추적할 수 있지만, Office 365 기업 계정에서 발생하는 상황에 한해 모니터링이 가능합니다. 타사 CASB(Cloud Access Security Broker)를 구축하지 않는 한 이러한 범위를 초과하여 온프레미스 환경 또는 기타 클라우드 서비스에서 전개되는 활동에 대한 감사 추적은 불가능합니다.

어떤 정책 제어를 설정하고 싶으십니까? Office 365에서 몇 가지 옵션을 제공하지만, 정책 제어를 위한 컨텐트 분류 기능은 기본 제공하지 않으며 관련 범위도 Office 365 환경 및 Microsoft 플랫폼으로 제한됩니다. Office 365 이외의 영역까지 포괄하는 컨텐트 식별 및 분류, 정책 제어, 감사 기능을 설정하려면 CASB, 클라우드 DLP 솔루션 등 추가 클라우드 보안 옵션을 찾아야 합니다.

컴플라이언스 및 책임

귀사의 중요한 컴플라이언스 관련 데이터를 Office 365에 보관하려 합니다. Microsoft는 CSA STAR Self-Assessment, PCI, HIPAA, ISO 27001, SSAE 16 SOC2 Type II, ISO 27018, SOC I type 2, GAAP, FISMA, ISAE-3402, NIST SP 800-53, FedRAMP 등 대부분의 컴플라이언스 요건을 충족합니다. 현재 Truste, Safe Harbor, SOC III, ITAR, COBIT는 지원하지 않습니다.

반드시 Office 365 공용 SLA(Service Level Agreement)를 읽고 Office 365와 관련하여 Microsoft의 책임에 해당하는 보안 활동과 해당하지 않는 보안 활동을 숙지해야 합니다. 특히 중요한 점은 귀사의 사용자가 Office 365에 업로드하고 공유하는 데이터에 대해 Microsoft가 책임지지 않는다는 것입니다. 또한 귀사 직원의 계정 인증 정보가 유출되어 무단 계정 액세스가 발생하는 경우에도 Microsoft는 책임을 지지 않습니다.

데이터 보호

Office 365는 귀사의 데이터를 위해 몇 가지 기본적인 보호 기능을 제공합니다. Office 365 클라우드에 저장된 데이터를 암호화합니다. Office 365 데이터가 Office 365 클라우드 이외의 지점, 즉 오프라인 엔드포인트 또는 다른 클라우드에 저장된 경우에는 암호화하지 않습니다.

Office 365는 전송 중인 데이터를 보호하기 위해 2048비트 이상의 SSL을 제공하며 OpenSSL, Heartbleed, Logjam, FREAK, CRIME, DROWN 취약점으로부터 보호됩니다. 하지만 Office 365는 POODLE 공격에 대한 대응책으로 잘 알려진 TLS_FALLBACK_SCSV를 지원하지 않습니다. 게다가 HTTP STS, X-SXX, X-Content, X-Frame과 같은 HTTP 보안 헤더도 지원하지 않습니다.

Office 365에서는 내부 및 외부 사용자 모두를 위해 공유 제어 기능을 제공합니다. 귀사의 사용자가 외부 사용자와 공유하는 것을 허용할지 여부를 결정해야 합니다. Office 365와 같은 협업 플랫폼이 매우 효과적인 비즈니스 지원 도구가 되지만, 부주의에 의한 과잉 공유는 기업의 중요 데이터가 유출되는 가장 큰 원인입니다. 따라서 귀사의 사용자에게 책임 있는 데이터 공유 프랙티스에 관한 교육을 실시하는 방안을 마련해야 함을 인식하고 관련 결정을 내려야 합니다. 그 밖에 우발적인 데이터 유출 사고를 방지하는 데이터 거버넌스 및 클라우드 DLP 제어 기능을 도입하는 것도 고려하십시오. 이것은 Gartner가 Office 365와 같은 플랫폼을 구축하려는 기업에게 CASB 도입을 적극 권장하는 이유 중 하나입니다. DLP 솔루션이 있다면 CASB 기능과 함께 Office 365로 확장할 수 있습니까?

보안 위협 차단

사용자 계정이 유출되면 귀사에 심각한 위협이 됩니다. 게다가 수천 개의 사용자 인증 정보가 활성화되고 사용자 인증 정보를 노리는 악성 코드가 만연하며 인터넷에서 직접 Office 365 계정에 액세스하는 것이 가능하므로 귀사의 사용자 계정이 유출될 확률이 높습니다. 유출된 계정을 알아내는 가장 좋은 방법은 사용자 행위 분석(UBA)입니다. Office 365는 기본 UBA 기능으로 데이터를 분석하지만, 다른 시스템과 같은 수준의 UBA 인텔리전스를 제공하지 못할 수도 있습니다. Office 365 계정에 국한되며, 여러 클라우드 애플리케이션의 전 범위에서 사용자 행위를 분석하지 못합니다. 광고 타깃 지정을 위해 데이터를 분석하지 않습니다.

계획 시작

Office 365 도입 시 내려야 할 보안 결정을 알게 되었으므로 이제 구축 계획을 시작할 수 있습니다. 진행 상황을 문서화하고 추적하는 데 활용할 수 있는 계획 샘플은 아래와 같습니다.

Office 365 도입 보안 계획

데이터 거버넌스 및 보호

1. 데이터 분류 계획 수립: 기존 DLP 솔루션을 사용할 수 있습니까? 여기에 CASB를 사용할 수 있습니까? 자체적으로 분류 시스템을 개발하고 유지 보수하려면 많은 노력이 필요합니다.
2. Office 365에서 위험한 데이터 탐지: 현재 Office 365를 사용 중이라면 현재 어디에 리스크가 있는지 파악하십시오. 더 나아가 CASB를 활용하여 Office 365에 있는 중요 데이터를 지속적으로 모니터링하십시오.
3. 위험한 데이터의 공유를 차단하기 위한 정책 구현: CASB API 통합을 활용하여 신속하게 해결하고 CASB 게이트웨이 제어로 과잉 공유를 미연에 방지할 수 있습니다.
4. 관리되지 않는 디바이스에 대한 다운로드를 금지하는 정책 등 관리되지 않는 디바이스의 기능을 제한하는 정책 이행.
5. 위험한 데이터를 공유하고 있는 사용자를 찾아 교육: 정확히 대상을 지정한 알림 기능이 위험한 사용자 행위를 바로잡는 데 효과적일 수 있습니다.
6. 컴플라이언스 요건에 따라 데이터 암호화: CASB에 있거나 Office 365에서 기본 제공하는 암호화 기능이 요건에 부합하는지 확인합니다. 귀사가 암호화 키를 철저히 제어하도록 규정한 까다로운 요건을 이행해야 한다면 그 기능만으로는 부족할 수 있습니다.
7. 월별 데이터 리스크 리포트를 생성하는 프로세스: 현재 상황을 파악하고 정기적으로 경영진에 리포팅하여 향후 계획 및 프로비저닝이 원활하게 진행될 수 있습니다.

컴플라이언스 및 개인 정보 보호

8. Office 365에 저장되는 규제 대상 데이터 식별: 중요 데이터를 식별하는 DLP 또는 CASB 솔루션에서 주요 컴플라이언스 관련 분류 기능에 중점을 두면서 관련 요구 사항도 해결해야 합니다.
9. Office 365에 저장되는 규제 대상 데이터에 대한 합당한 비즈니스 사유 확인: Office 365에 저장할 수 없는 데이터가 있습니까? 즉 클라우드에서 해당 데이터를 보호할 수 없는 경우가 있습니까?
10. 합당한 비즈니스 사유가 없을 경우 Office 365에서 규제 대상 데이터 배제: 규제 대상 데이터를 Office 365에 저장할 필요가 없다면 Office 365에 업로드하는 것 자체를 금지하는 자동화된 정책 제어 및 보안 기능을 구현하십시오. 게이트웨이 제어를 통해 이러한 데이터가 클라우드에 업로드되지 않도록 할 수 있습니다.
11. 규제 대상 데이터가 클라우드에서 공유되지 않도록 하는 정책 구현: 자동화된 정책 제어를 생성합니다. API 기반 CASB는 안전하지 않은 공유 문제를 신속하게 해결할 수 있습니다. 실시간 트래픽에서 인라인 방식으로 공유 트랜잭션을 읽는 게이트웨이 기반 CASB는 안전하지 않은 공유를 차단할 수 있습니다. 모든 CASB에서 가능한 것은 아닙니다.

성능 및 보안

12. 사용자 수 및 제안된 도입 일정 파악: Office 365를 언제 구축할지 결정합니다. 대부분의 기업은 완전히 이전하기 전에 한동안 하이브리드 방식을 선택할 것입니다.

13. 필요한 사용자당 평균 대역폭 및 연결 수 결정: 블루코트의 조사에 따르면, Microsoft Exchange 구축 시 평균 사용자 1인당 200Mbps 대역폭 및 7개의 동시 연결이 추가로 필요합니다. Office 365 애플리케이션이 추가되면서 100Mbps가 늘어나고 40개 이상의 동시 연결이 필요하게 될 수 있습니다.

14. 기존 보안 시스템을 프로비저닝하여 증가한 대역폭 및 연결 요구 사항 처리: 인터넷 트래픽 증가를 수용하기 위해 리소스를 추가해야 하는 상황이 실현될 수 있습니다.

15. 성능 최적화를 위해 게이트웨이 튜닝: 게이트웨이 및 방화벽에서 Office 365 성능 튜닝 및 트래픽 조절 기능을 활용하십시오.

보안 위협 탐지

16. 허가받은 모든 클라우드 애플리케이션에 단일 로그온 및 다중 인증 구현: 인터넷에서 직접 클라우드 애플리케이션에 액세스할 수 있으므로 보안에서 액세스 제어가 매우 중요합니다.

17. DLP 구현: CASB 통합을 활용하여 기존 DLP를 확장하거나 추가 DLP 기능의 도입을 검토하십시오. 데이터 분류 기능을 제공할 수 있는 솔루션을 활용하십시오.

18. CASB로 클라우드 애플리케이션에서 사용자 행위 분석: 사용자 행위 분석 및 클라우드 가시성을 통해 Office 365 계정 유출을 찾아 처리하고, 자동화된 정책 제어를 통해 보호를 강화하십시오.

19. 이메일 보호 구현: 이메일은 일차적인 공격 경로이므로 효과적인 이메일 보호 기능을 갖춰야 합니다. 현재 이메일 보호 솔루션을 Exchange Online으로 확장할 수 있는지 아니면 새로운 보호 기능을 추가해야 하는지 평가하십시오. 이메일 DLP가 없으면 추가할 방법을 알아보십시오.

20. ATP 보호 구현: 계정을 유출하고 조직을 감염시키는 악성 코드를 차단하십시오. 악성 코드 차단 및 ATP(Advanced Threat Protection)는 핵심 보안 프랙티스이므로 클라우드 계정으로 확장해야 합니다.

결론

Office 365로의 마이그레이션을 축하합니다. 협업 클라우드 솔루션으로 이전하면서 다양한 혜택을 누릴 수 있습니다. 하지만 성공적으로 안전하게 Office 365를 도입하기 위해서는 결정하고 행동해야 할 것이 많습니다.

각종 리스크, 특히 핵심 비즈니스를 클라우드로 이전하는 것과 관련된 리스크로부터 귀사를 보호하기 위한 여러 옵션을 분석하고 검토하십시오. 다른 기업이 도입 과정에서 얻은 교훈을 활용하고 초기 단계에서 구현 계획 프로세스에 보안을 구현하십시오. 귀사를 확실하게 보호할 수 있도록 새로운 클라우드 보안 방어 체계를 추가하고 기존 보안 방어 체계도 조정해야 합니다.

시만텍과 블루코트는 Office 365를 도입하는 기업을 위해 업계 최고의 DLP, 데이터 과학 기반의 CASB, SWG, ATP, 엔드포인트 보호, 이메일 보안 솔루션을 제공합니다.

저자 소개

Deena Thomchick는 시만텍에서 클라우드 담당 수석 이사를 맡고 있습니다. Deena는 기술 업계에서 주로 보안 전문가로 25년 넘게 종사한 베테랑입니다. 그녀는 암호화, 지능형 보안 위협 차단, 네트워크 보안, 엔드포인트 보안 등 여러 분야에서 활동했습니다.

참고: 이 리포트에서 언급한 Office 365의 특성은 2016년 6월의 Office 365 분석을 토대로 하며 변경될 수 있습니다. Office 365에 대한 최신 Elastica Business Readiness를 확인하려면 시만텍에 연락하여 Elastica Shadow Data Risk Assessment 무료 리포트를 요청하십시오. 본 리포트의 내용은 일반적인 지침으로만 활용해야 합니다. 최신 Office 365 기능에 대한 구체적인 사항은 Microsoft에 문의하십시오.

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.com/ko/kr)와 페이스북, 트위터, 링크드인을 통해 확인할 수 있다.

Symantec™ 서울시 강남구 테헤란로 152강남파이낸스센터 28층 | TEL: 02-3468-2000 | FAX: 02-3468-2001 | www.symantec.com/ko/kr

SYMC_WP_Start_Planning_Office365_KR_v1a