

보안 관리에 대한 특강:
강력한 보안 태세를
구축하는 열쇠에
관한 교육

**진화하는 사이버 위협 환경과
변화하는 보안 과제는 귀사에
실제로 영향을 줄 수 있습니다.**

**보안 솔루션의 지능형 관리 시스템을
구축하여 귀사의 보안 상태, 정책 관리
및 보안 태세 강화 지침을 좀 더
잘 파악하는 것이 중요합니다.**

소개

위협은 더욱 정교해지고 공격 영역도 확대되는데, 기업들은 이를 어떻게 막을 수 있을까요? 조직들은 여러 환경에 분산되어 있는 리소스를 직접 관리하고 있기 때문에 복잡성 증가, 가시성 부재, 효과 없는 대응 방법 등 여러 보안 문제에 처해 있습니다.

많은 조직들이 뒤쳐지지 않기 위해 솔루션을 더 많이 배포하고 있지만, 단일 워크로드에 있는 특정 보안 문제를 다중 지점 솔루션으로 처리하는 경우가 많습니다. 이로 인해 전체 보안 상태를 파악하지 못하게 되면서 조직의 전반적인 보안이 영향을 받게 될 수 있습니다.

너무도 많은 개별 제어, 포인트 솔루션 및 보안 공급업체를 관리하고 있는 데다가, 대개 서로 격리된 다양한 데이터 세트로 인해 발생하는 "노이즈"까지 증가하면서 관리 업무가 부담이 되어 보안을 취약하게 만들 수 있습니다. 또한 이종 포인트 솔루션은 서로 통합하기가 어려운 경우가 많아 위협에 효과적으로 대응하지 못하는 것은 물론 귀사의 보안 태세를 파악하기도 어렵습니다.

이 eBook에서는



리소스 전반의 보안 상태와 위험을 파악하는 데 도움이 되는 완벽한 **가시성**



일관된 보안 정책을 정의하는 데 도움이 되는 내장 보안 **제어**



실행 가능한 정보와 조언을 통해 보안 수준을 높이는 데 도움이 되는 효과적인 **지침** 등

세 가지 기본 원칙을 사용하여 지능형 보안 관리를 구현하는 방법을 설명합니다.

01.

가시성



02.

제어



03.

지침



01.

가시성

보안 상태 파악



 메뉴 사용자 장치 앱 및 데이터

가시성은 지능형 보안 관리를 구현하는 첫 단계입니다. 조직 내 리소스 전반의 위험을 알아내기 위해서는 보안 상태에 대한 통찰이 필요합니다. 그래야만 위협을 효과적으로 감지하고 이에 대응할 수 있습니다.

Microsoft 365 보안 관리 솔루션으로 귀사의 사용자, 장치, 앱 및 데이터의 보안 상태를 어떻게 파악할 수 있는지 확인해 보세요.

 메뉴 사용자 장치 앱 및 데이터

요즘은 사용자들이 언제 어디서든 장치와 상관없이 접속하여 액세스를 요구함에 따라 ID가 새로운 보안 경계가 되었습니다. 이에 따라 (사용자 환경에 지장을 주지 않고) 사용자 ID를 보호하는 일이 최신 사이버 보안에서 가장 중요한 측면 중 하나가 되었습니다.

Microsoft의 ID 및 액세스 관리 서비스인 Azure Active

Directory(Azure AD)는 조직 디렉터리의 무결성과 보안을 파악할 수 있도록 액세스, 사용 및 보안 보고서를 제공합니다. 이 정보를 보고 디렉터리 관리자는 가능한 보안 위험을 더 잘 확인하고 마이그레이션할 수 있습니다.

Azure AD를 사용하여



특정 사용자의 장치와 로그인 활동 데이터를 보여주는 사용자별 보고서



지난 24시간, 7일 또는 30일 이내에 감사한 모든 이벤트 기록이 담긴 활동 로그와 그룹 활동 변경 사항과 비밀번호 재설정 및 등록 활동

을 보고 분석할 수 있습니다. 이 외에도 Azure AD는 권한이 있는 ID를 심도 있게 파악하여(그 오용과 관련된 위험이 크기 때문에) 권한이 있는 계정을 관리하고, 그 활동을 모니터링하는 일을 돕습니다. Azure AD Privileged Identity Management를 통해 오용되고 있는 관리자 역할을 쉽게 식별할 수 있어, 관리자와 관리자의 리소스 액세스를 발견하고, 제한하고, 모니터링할 수 있습니다. 관리 액세스가 필요한 사용자는 다단계 인증으로 그 ID를 입증한 후에 사전에 구성된 제한 시간 동안 액세스 권한을 행사할 수 있습니다(적시 액세스 권한으로).

 메뉴

 사용자

 장치

 앱 및 데이터

사용자들이 상시 연결되어 있는 상태에서는 장치 보안이 매우 중요합니다. 따라서 보안 팀도 엔드포인트 보안을 파악할 수 있고, 사건의 범위와 근본 원인을 신속하게 평가할 수 있는 기능, 조사 및 시정 조치를 위한 다양한 툴셋을 갖춘 솔루션이 필요합니다.

Windows Defender Advanced Threat Protection(ATP)에는 Windows Secure Score가 포함되어 있습니다. 보안 관리 팀과 보안 운영 팀 모두 Windows Secure Score를 통해 그 엔드포인트의 보안 상태와 최신 위협으로부터 얼마나 잘 보호되고 있는지를 실시간으로 파악할 수 있으며, 구성 문제를 사전에 해결하여 조직의 공격 영역을 줄일 수 있습니다. Windows Secure Score는 전반적인 보안 태세를 강화하는 조치를 제시해 주기 때문에 IT 팀마다 서로 다른 보고서를 수동으로 수집할 필요가 없습니다.

Windows Secure Score 대시보드를 통해서는, 상세한 보안 제어 구성과 함께 다음을 확인할 수 있습니다.



귀사의 현재
Microsoft Secure Score.



시간 경과에 따른 귀사의
Windows Secure Score



Windows Defender
보안 제어



각 보안 제어의 권장 조치를
포함하는 개선 기회

← 메뉴

사용자

장치

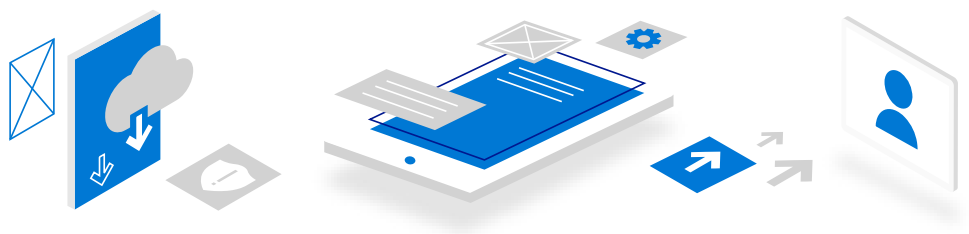
 앱 및 데이터

현재 기업들이 직면하고 있는 사이버 위협의 정교함과 범위를 고려할 때 그 앱과 데이터의 보안이 항상(저장할 때, 전송할 때, 처리할 때) 필요합니다. 또한 GDPR 같은 규정이 도입되면서 데이터 보안과 사용 투명성이 그 어느 때보다도 중요해졌습니다.

Microsoft 365에서 앱과 데이터를 파악할 수 있는 주요 경로 중 하나는 사용자의 활동을 파악할 수 있는 감사 로그와 보고서입니다. Office 365 보안 및 규정 준수 센터를 통해 로그를 검색하여 쉽게 액세스할 수 있습니다. 내장 보고서를 이용해 로그 데이터를 시각적으로 표시할 수 있습니다. 예를 들어, SharePoint Online, One Drive for Business 및 Exchange Online에서 데이터 손실 방지(DLP) 정책을 위반하고 있는 사람이 몇 명인지, 또는 Office 365 Advanced Threat Protection 기능으로 차단된 악성 첨부 파일이 몇 개인지 볼 수 있습니다.

Microsoft Cloud App Security를 이용해 Shadow IT 보고와 관리 및 위험 평가를 포함해 조직 내에서 이루어지는 전체 클라우드 사용도 추가로 파악할 수 있습니다. 뿐만 아니라 Office 365 Management Activity API의 데이터 구문을 분석하여 새로운 위치에서 로그인, 특이한 간격으로 로그인 또는 통상적으로 사용하지 않는 ISP 사용하는 것과 같은 비정상적인 활동에 대한 경고를 생성합니다.

이러한 경고는 알려진 랜섬 확장자가 있는 파일을 OneDrive로 업로드 또는 동기화하거나 민감한 인사 자료가 있는 SharePoint 사이트에서 대량의 콘텐츠를 다운로드하는 특이한 활동에 대해서도 생성할 수 있습니다.



02.

제어

조직에 필요한 데이터 보호 정의



 메뉴 사용자 장치 앱 및 데이터

보안 상태를 파악한 후 다음 단계는 보안 태세에 대한 지속적인 제어입니다. 일관된 보안 정책을 생성하여 사용자에게 맞게 지정하고, 지능형 보안 관리에 반드시 필요한 제어를 활성화해야 합니다.

Microsoft 365 보안 관리 솔루션을 이용해 정책을 정의하고 사용자, 장치, 앱 및 데이터용 제어를 활성화하는 방법을 살펴봅니다.

 메뉴 사용자 장치 앱 및 데이터

Microsoft 365는 조건부 액세스를 사용하고, 권한이 있는 ID를 제어 및 보호하여 출입구부터 조직을 지켜줍니다.

Azure AD는 Microsoft의 ID 및 액세스 관리 솔루션으로서, 조직에서 사용자 ID 및 관련 액세스 권한을 쉽게 관리할 수 있도록 설계되었습니다. Azure AD는 조건부 액세스, 사용자 및 로그인 위험 계산, 다단계 인증, 권한이 있는 ID 관리 같은 기능을 사용하여 데이터 액세스를 안전하게 제안할 수 있게 도와줍니다.

Azure AD Conditional Access는 지배 구조, 위험 및 규정 준수 시나리오에서 액세스를 관리하기 위한 효과적인 토대를 제공합니다. 조건부 액세스 정책은 장치 상태, 애플리케이션 민감성, 위치 및 사용자 규칙에 따라 적용할 수 있습니다.

또한 **Microsoft Enterprise Mobility + Security**는 각 액세스 요청과 사용자의 위험을 계산한 다음 필요한 시정 조치를 자동으로 적용하는 ID 보호 기능을 사용하여 가장 앞선 위협으로부터 데이터를 실시간으로 지킬 수 있습니다.

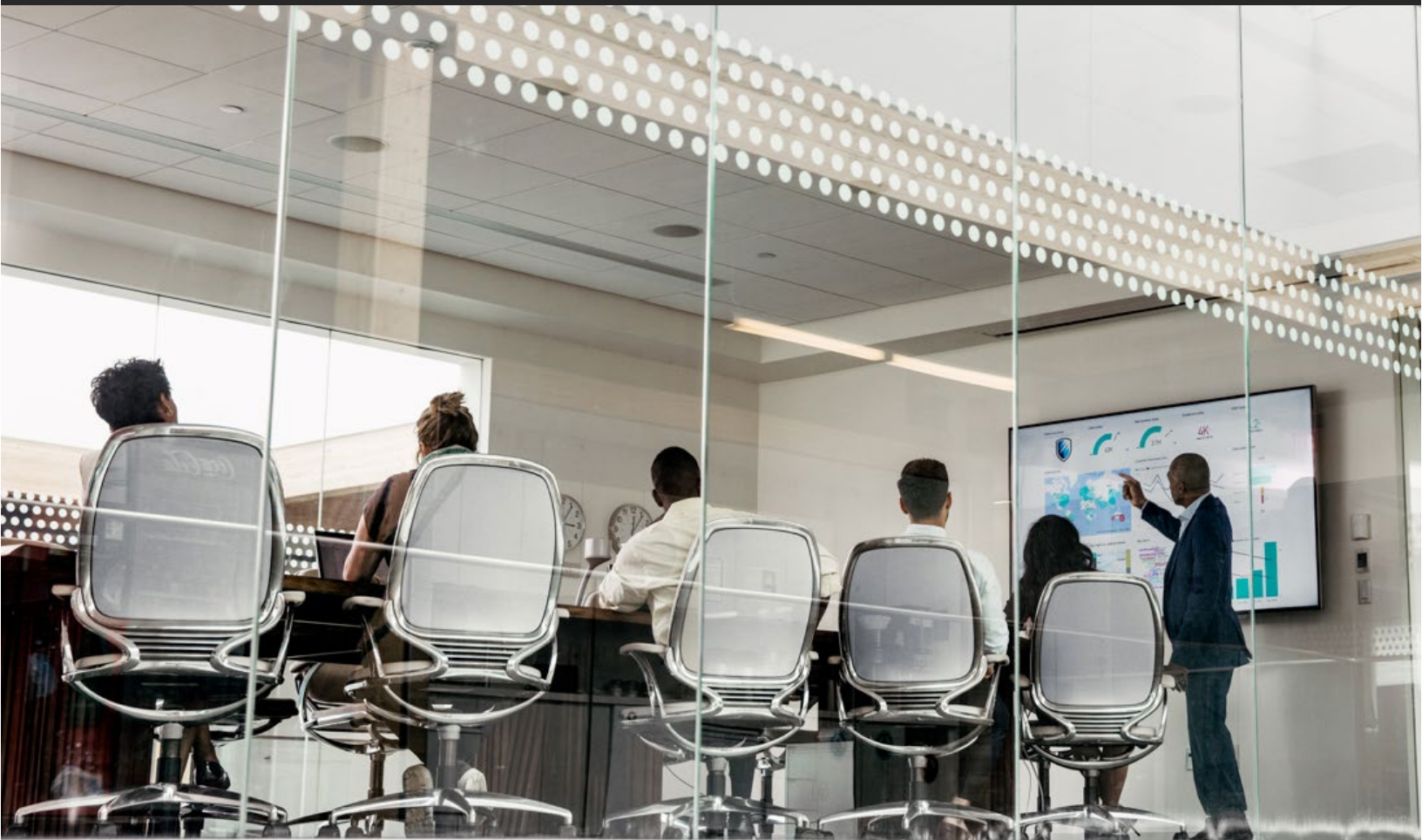
관리자 계정 손상에 비하면 계정 손상은 약과에 불과합니다. 따라서 관리자 권한이 있는 계정의 수와 확률을 최소화하는 것이 매우 중요합니다. Azure AD Privileged Identity Management를 사용하면 필요할 때만, 필요한 기간 동안만, 그리고 권한 상승 정책을 준수할 때만 관리자 액세스 권한을 부여하는 정책을 설정하여 관리자 권한이 있는 사용자의 수를 최소로 줄일 수 있습니다.



 메뉴 사용자 장치 앱 및 데이터

가장 중요한 보안 관리 방법 중 하나는 전체 Windows Security 스택을 신속하게 활성화하고 보안 정책에 부합되는 방식으로 구성할 수 있는 기능입니다. Microsoft는 모든 Windows Defender ATP 구성요소를 중앙에서 관리하는 도구를 제공합니다.

귀사의 보안 관리자가 System Center Configuration Manager 또는 Microsoft Intune을 하나로 통합된 IT로 사용하여, 한곳에서 Windows Security 제어 전체를 활성화 및 구성할 수 있습니다. 이 기능은 역할 기반 보안을 사용하여 해당 인력의 액세스와 제어를 제한하는 조직에서 매우 효과적입니다.



← 메뉴

사용자

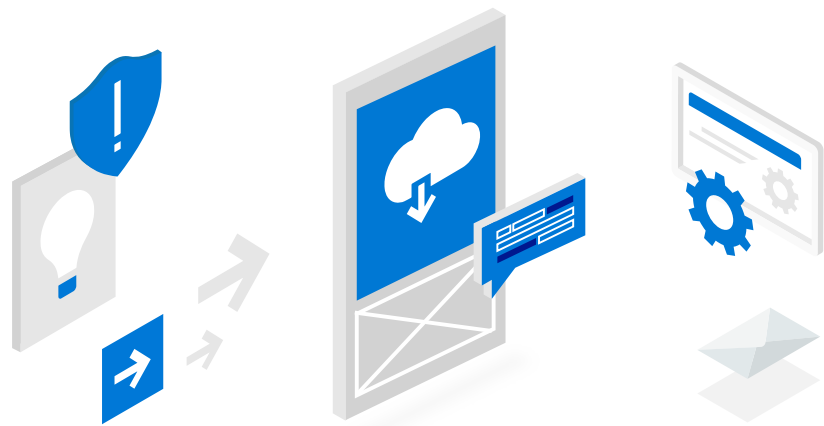
장치

앱 및 데이터

중요한 보안 및 규정 준수 기능을 위한 맞춤형 중앙 집중식 포털인 Office 365 보안 및 규정 준수 센터를 통해 앱과 데이터의 보안을 더욱 잘 제어할 수 있습니다. 예를 들어, DLP 및 데이터 보존 정책을 설정하고, 맬웨어와 스팸 처리 방법을 구성하고, 위협 인텔리전스 데이터를 볼 수 있습니다.

보안 및 규정 준수 센터를 이용해 역할 기반 보안 그룹을 간단하게 구성하여 글로벌 관리 권한 외에 필요한 보안 및 규정 준수 기능에만 액세스할 수 있게 할 수 있습니다. 이렇게 하면 청구, 라이선스 할당, 새로운 사용자 생성 같은 관리 기능에 대한 액세스를 쉽게 제한할 수 있습니다.

새로운 주요 보안 분석 도구를 하나 더 소개하면 Microsoft Secure Score가 있습니다. 이 도구는 보안 모범 사례와 비교하여 귀사의 구성 점수를 하나의 숫자로 나타냅니다. Secure Score는 다양한 Microsoft 워크로드의 다단계 인증, 감사, 보안 기능을 활성화하는 것을 포함해 핵심 보안 제어를 찾아 활성화합니다. 또한 귀사에서 활성화한 제어의 이력 데이터를 기록하기 때문에 진행 상황 및 점수를 추적하여 조직 내 다른 구성원과 이를 공유할 수 있습니다.



03.

지침

최신 상태의 보안 인텔리전스 유지



 메뉴 사용자 장치 앱 및 데이터

**최적의 보안 정책을 정의하는
제어를 갖춘 후에는 보안 태세를
강화하는 데 사용할 수 있는
지속적인 인텔리전스 및 권장안이
필요합니다.**

Microsoft 365 보안 관리 솔루션이
사용자, 장치, 앱 및 데이터를 위한
내장된 인텔리전스 및 권장안을
어떻게 제공하는지 살펴봅니다.

 메뉴

 사용자

 장치

 앱 및 데이터

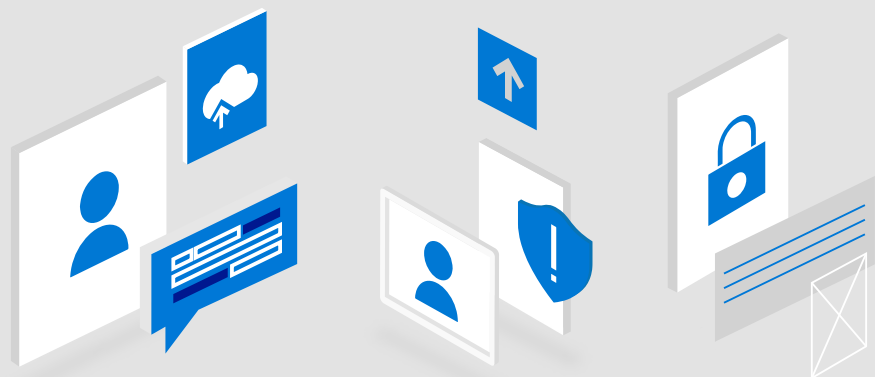
Azure AD는 위험 기반 조건부 액세스로 방어의 최전선 역할을 합니다. Azure AD는 크게 세 가지 범주의 보안 보고서를 제공합니다. 즉,

 로그인 이 이상하고 로그인이 무단 액세스 시도인 위험 수준과 관련되는 경우

 사용자 자격증명이 위험한 로그인에서 자주 등장하거나 무단 활동에서 발견되어 손상되었음을 알 수 있는 경우

 보안 태세를 강화해야 하는 경우, 즉 구성 변경을 마이그레이션할 수 있는 방어 기능에 취약점이 있는 경우

Azure AD Identity Protection Security Reports에는 이 정보가 Azure AD Portal에, 또는 프로그램으로 표시되기 때문에 SIEM 또는 발권 시스템에 통합할 수 있습니다.



← 메뉴

사용자

장치

앱 및 데이터

Windows Secure Score 를 통해 보안 팀은 사용할 수 있는 보안 제어가 무엇인지, 그리고 조직의 보안 태세를 강화하는 데 도움이 될 수 있는 구성이 어떤 것인지 더욱 잘 파악할 수 있습니다.

Windows Secure Score 대시보드는 각 Windows Defender 보안 제어에 필요한 조치를 제안합니다. 각 제어에 사용할 수 있는 모든 구성 옵션을 표시하고, 어느 기기에 어떤 것을 적용할지를 보여주며, 각 구성 옆에 있는 숫자는 이 추가 구성이 귀사의 전체 점수에 얼마나 기여할지를 나타냅니다. 위협이 감지되면 관련 경고와 함께 차단 및 마이그레이션 권고가 표시됩니다.





메뉴



사용자



장치

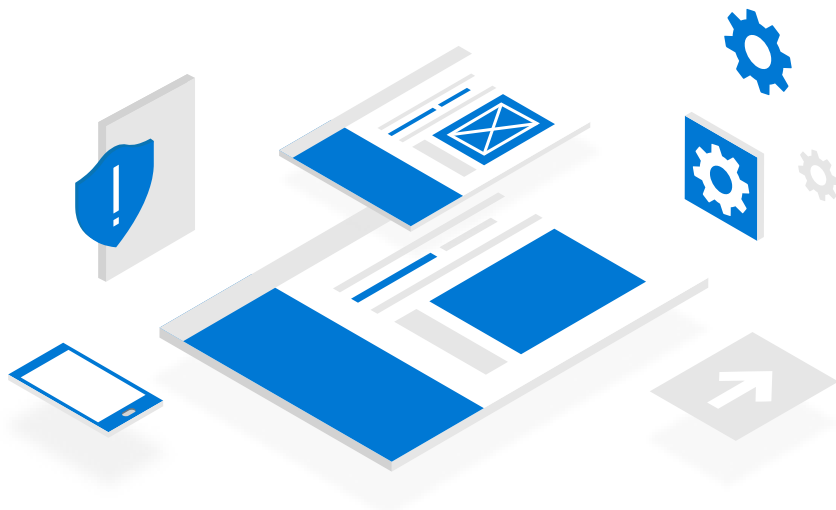


앱 및 데이터

Microsoft 365는 Office 365 보안 및 규정 준수 센터와 Microsoft Secure Score를 통해 귀사 보안 태세를 강화하는 데 도움이 되는 권고안을 제시합니다.

보안 및 규정 센터는 귀사 조직에 제공할 수 있는 권고안을 보여줍니다. Office 365는 머신 러닝으로 사용 신호를 해석하여 데이터 보호에 관해 권고합니다. 예를 들어, 세무 서류를 보호하고 있지 않을 경우 7년 동안 그 내용을 보유하는 데이터 보존 정책을 만들 것을 권고할 수 있습니다. 개인 식별 정보(PII)에 관한 데이터 손실 방지 정책이 없는 경우 간단하게 정책을 만들도록 도와줄 수 있습니다. 이 서비스는 귀사 업종에 해당하는 정보를 활용하여 사용자에게 좀 더 맞는 권고안을 제안할 수도 있습니다.

Microsoft Secure Score를 통해 생산성과 보안의 균형을 쉽게 맞출 수 있습니다. 고객 지원에서 얻은 당사의 모범 사례와 데이터를 토대로 데이터 유출, 계정 침해 및 권한 상승 같은 위협을 좀 더 잘 막을 수 있는 보안 제어를 제안할 수 있습니다.





Microsoft Intelligent Security Graph를 기반으로 활용

Microsoft의 보안 관리 솔루션(본 eBook에 언급된 것 포함)은 **Microsoft Intelligent Security Graph**에서 제공합니다. Intelligent Security Graph에서 제공하는 정보는 광범위한 Microsoft 제품과 파트너의 기기와 클라우드 서비스에 있는 방대한 양의 위협 정보와 보안 데이터로 생성됩니다.

빠르고 복잡한 공격을 막아내기 위해 **Intelligent Security Graph**는 머신 러닝과 인공지능을 활용하여 위협을 감지하고 빠르게 대응합니다. 이 시스템은 지속적인 데이터 흐름에서 수집하고 상호 연결하고 학습하며 최신 위협 정보를 지속적으로 업데이트합니다. 당사에서 운영하는 전 세계 수백 개 클라우드 서비스와 당사에서 매일 업데이트하는 전 세계 10억 대 이상의 PC에서 이 익명 데이터가 나옵니다. 위협 사냥꾼, 연구자, 분석가, 엔지니어들이 모델을 정교하게 조정하며, 더 많은 통찰과 컨텍스트를 추가합니다. 또한 당사 디지털 범죄반(Digital Crimes Unit)과 사이버 방어 운영 센터(Cyber Defense Operations Center)가 기업 및 사법 기관과의 협력, 광범위한 연구를 통해 외부 데이터 포인트와 데이터를 집계합니다.



지능형 보안 관리 시작

Microsoft 365는 귀사 조직의 사용자, 장치, 앱 및 데이터의 보안 관리를 최적화하여 다중 지점 보안 솔루션 및 관리 콘솔을 최소화합니다. Microsoft 365 보안 관리 솔루션은 포괄적 파악과 제어가 가능하며, 내장된 지침과 권고안을 제시합니다.

다음과 같이 시작합니다.

1. Azure AD를 사용하여 환경에 있는 ID 보호합니다.
2. Windows Defender Security Center를 통해 장치의 위협 관리를 활성화합니다.
3. Office 365 보안 및 규정 준수 센터, Microsoft Secure Score 및 Microsoft Cloud App Security를 사용하여 SaaS 애플리케이션 데이터와 앱을 관리하고 제어합니다.

조직의 보안 태세를 강화할 준비가 되셨나요?

지능형 보안 관리에 대해 자세히 알아보기

추가 리소스

ID 및 액세스 관리

➤ [Azure Active Directory에 대해 알아보기](#)

장치용 보안 관리

➤ [Windows Defender Security Center에 대해 자세히 알아보기](#)

앱 및 데이터용 보안 관리

➤ [Office 365 보안 및 규정 준수 센터에 대해 자세히 알아보기](#)

➤ [클라우드 앱 보안 개요 보기](#)

© 2018 Microsoft Corporation. All rights reserved. 이 문서는 "있는 그대로" 제공됩니다. URL 및 기타 인터넷 웹 사이트 참조를 비롯하여 이 문서에 기술된 정보 및 관점은 예고 없이 변경될 수 있습니다. 이를 사용함으로써 발생하는 위험은 사용자가 부담합니다. 이 문서는 Microsoft 제품의 지적 재산권에 어떠한 법적 권리도 제공하지 않습니다. 이 문서를 복사하여 내부 참조용으로 사용할 수 있습니다.