SHAREPOINT 콘텐츠에 대한 제어 자동화

보안 위협으로부터 민감한 비즈니스 콘텐츠 보호

Quest

콘텐츠 보안의 과제

최근 몇 년 사이에 일어난 Edward Snowden의 NSA 보안 침해(대부분 SharePoint 서버에서 유출) 및 다수의 기타 심각한 시스템 침해 사례는 여러 기업에게 SharePoint 보안 전략을 검토하도록 경종을 울려왔습니다. 이러한 공격은 특권 계정 자격 증명이 위험에 노출되고 악용되었기 때문에 성공할 수 있었습니다. 그리고 그 규모도 커지고 있습니다. 이제 공격의 주체는 단독으로 행동하는 해커가 아니라 조직화된 단체가 되었으며, 일부는 국가에서 후원하는 것으로 추정됩니다.

데이터 및 네트워크 취약성 면에서 대체로 가장 약한 고리는 직원입니다. 엉뚱한 사람에게 정보를 전송하거나 대규모 이메일에 부주의로 파일을 첨부하기도 합니다. 특히 액세스 권한이 취약합니다. 해커는 대부분 공유하거나 자주 변경하지 않는 사용자 이름과 암호(놀랍게도 관리자 자격 증명인 경우가 있음)에 대한 액세스 권한을 획득하여 조직 전체의 다수의 시스템에 액세스할 수 있습니다. 또한 데이터가 보안 수준이 낮은 시스템의 잘못된 위치에 저장되거나 안전하다고 추정되는 시스템에 잘못 분류되어 태그가 지정되는 경우도 흔히 발생합니다.

클라우드 기반 애플리케이션은 보통 관리 및 유지 보수를 중앙 IT에서 이행하므로 특히 더 취약합니다. 클라우드에서는 또한 지원 및 유지 보수에 대한 타사 공급업체 의존도가 높기에 이러한 액세스도 모니터링해야 합니다. 물리적 디바이스도 취약하긴 마찬가지입니다. 암호화되지 않은 휴대용 드라이브를 분실하거나 문서 기록을 부적절하게 폐기 처분할 수도 있고, 노트북은 도난당하기 쉽습니다.

사용자는 사무실이나 집에서, 그리고 이동 중에 엔터프라이즈 시스템 내부 콘텐츠에 대한 더 많은 액세스를 요구하므로, IT 팀은 계속해서 신속하고 비용 효율적으로 서비스를 제공하는 동시에 데이터를 안전하게 유지해야 합니다. 이를 위해서는 생산성과 비용, 정보의 가치가 균형을 이루는 접근 방법이 필요합니다.

취약성 감소 또는 제거에 대한 SharePoint 정보 거버넌스의 중요성, SharePoint 기본 제공 데이터 보호 툴의 한계 및 더 나은 SharePoint 보안 구현 방식을 살펴보겠습니다.

SharePoint 보안

SharePoint는 다음 세 가지 방법으로 중요한 비즈니스 데이터를 보호합니다.

- 사용자 인증
- 콘텐츠 사용 권한
- 사용자 관리

사용자 인증

제공된 SharePoint 시스템에 대한 사용자의 액세스를 결정합니다. 대부분의 SharePoint 솔루션은 Microsoft Active Directory를 사용하여 권한이 부여된 사용자 목록을 유지 보수합니다. 이는 Windows와 같은 핵심 시스템, SharePoint와 같은 비즈니스 엔터프라이즈 툴, SAP 또는 Salesforce와 같은 기타 HR 또는 재무 툴에 대한 사용자 액세스를 제어하는 중앙 데이터베이스입니다.

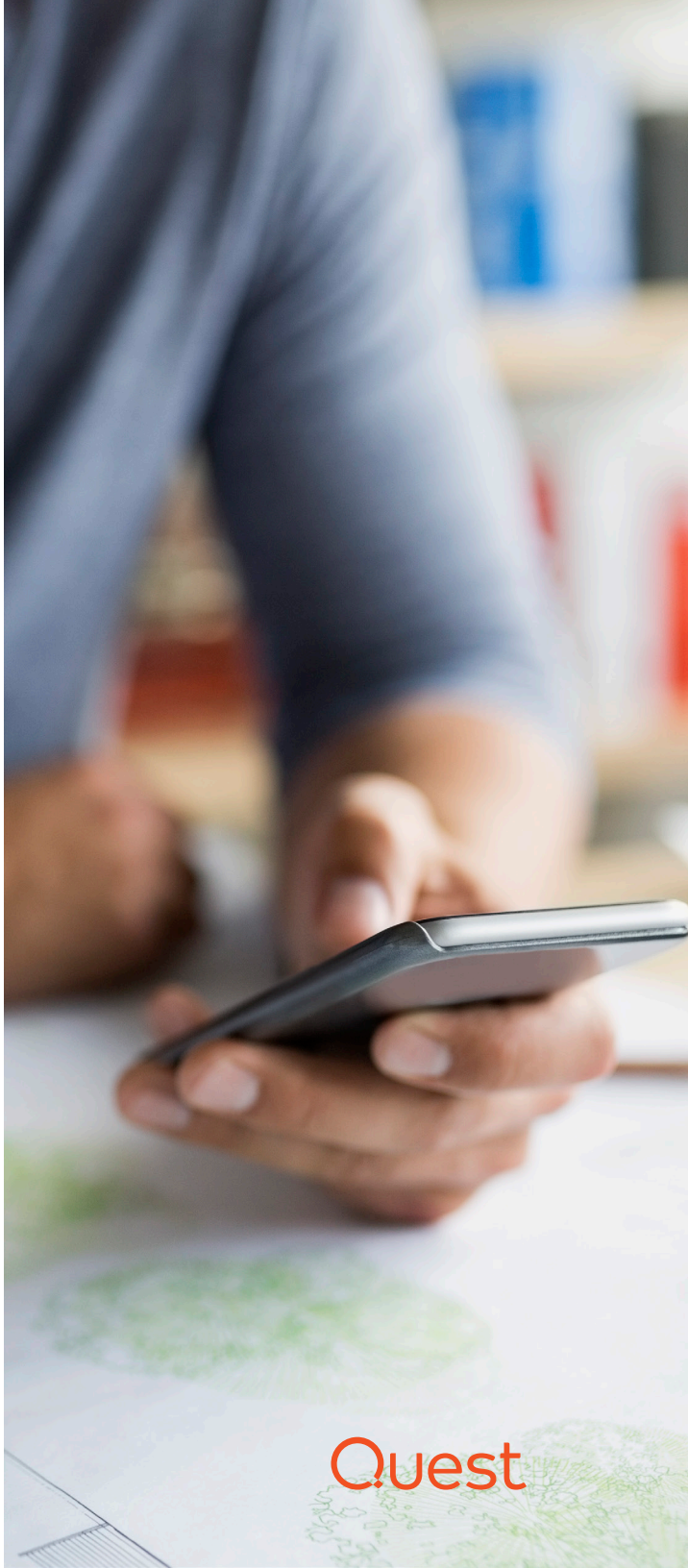
SharePoint Online이나 Office 365에서 사용하기 위해 Active Directory 인증이 클라우드로 확장될 수도 있습니다. 이러한 클라우드 기반 플랫폼은 자체적인 Microsoft 승인 계정을 사용하여 사용자에게 Active Directory 외부 인증을 제공하는 "공유" 기능도 제공합니다

외부 사용자에게 콘텐츠를 노출하는 경우 관리자는 SharePoint 데이터 보호의 두 번째 계층인 콘텐츠 사용 권한을 주의 깊게 감시해야 합니다.

콘텐츠 사용 권한

SharePoint에 대한 액세스 권한이 부여되면 사용자에게 특정 작업을 수행할 수 있는 권한이 부여되어야 합니다. SharePoint 권한이나 보안 모델을 사용하면 웹 애플리케이션, 사이트 컬렉션, 사이트, 목록, 폴더 및 항목과 같은 SharePoint 팜의 모든 범위에 걸쳐 액세스 권한을 부여할 수 있습니다.

기본 권한 수준은 사용자의 기능 요구 사항과 보안 고려 사항에 따라 개별 사용자, 사용자 그룹 또는 보안 그룹에 할당할 수 있는 사전 정의된 사용 권한 집합입니다. 기본적으로 SharePoint 권한 수준은 사이트 컬렉션 수준에서 정의되며 상위 개체에서 상속됩니다. 필요한 경우 개체에 고유한 권한을 적용하기 위해 상속이 중단될 수 있습니다.



이러한 사용 권한 수준은 각기 사용자가 다음을 포함하는 일련의 관련 작업을 수행할 수 있는 특정 사용 권한 집합으로 구성됩니다.

- 항목만 보기
- 항목 보기, 추가, 업데이트 및 삭제
- 목록 추가, 편집 및 삭제
- 사이트 및 페이지 생성
- 사용자 정보 탐색
- 권한 관리

사이트 컬렉션 관리자는 위와 같은 1개 이상의 특정 권한으로 구성된 사용자 정의 권한 수준을 정의할 수 있습니다. 이러한 새 수준은 사용자와 개체에 적용될 수 있습니다.

SHAREPOINT의 팀 사이트에 사용할 수 있는 기본 사용 권한 수준

- **보기만 가능** - 사용자가 애플리케이션 페이지를 볼 수만 있습니다.
- **제한된 액세스** - 적용할 수 없는 사용 권한 수준입니다. 대신에 사용자에게 상위 내부의 SharePoint 개체에 대한 세분화된 액세스 권한이 제공되면 상위 개체에 자동으로 제공됩니다. 그러면 전체 사이트에 대한 액세스 권한을 부여하지 않아도 사용자가 특정 목록, 문서 라이브러리, 폴더, 목록 항목 또는 문서에 액세스할 수 있습니다.
- **읽기** - 사용자가 페이지와 목록 항목을 보고 문서를 다운로드할 수 있습니다.
- **참가** - 사용자가 개인 보기를 관리하고 항목과 사용자 정보를 편집할 수 있습니다. 기존 목록에서 버전을 삭제하고 개인 웹 파트를 추가, 제거 및 업데이트할 수도 있습니다.
- **편집** - 사용자가 목록을 관리할 수 있습니다.
- **디자인** - 사용자가 웹사이트에서 항목 또는 페이지 보기, 업데이트, 삭제, 승인 및 맞춤 구성을 수행할 수 있습니다.
- **모든 권한** - 사용자가 웹사이트에 대한 모든 권한을 갖습니다.

Quest

사용자 관리

SharePoint 데이터 보호의 세 번째 계층을 사용하면 관리자가 직접 또는 그룹을 통해 사용자를 관리할 수 있습니다. 사용자 직접 관리란 정확하게는 관리자가 특정 사용자에게 사이트 또는 목록과 같은 특정 SharePoint 개체에 액세스하는 권한을 부여할 수 있음을 의미합니다. SharePoint에서는 이를 쉽게 수행할 수 있지만, 사용자의 수가 많은 경우 관리 및 유지 보수가 어려울 수 있습니다.

그러나 그룹을 통해 사용자를 관리하려면 개별 사용자가 아닌 그룹에 권한을 적용해야 합니다. 손쉽게 그룹에서 사용자를 추가하거나 제거하여 해당 권한의 적용 여부를 제어할 수 있습니다. 권한을 수정해야 하는 경우 특정 그룹에 대해 권한을 수정하면 해당 그룹의 모든 사용자에게 적용됩니다.

MICROSOFT에서 제안하는 SHAREPOINT 그룹

- 읽기 권한이 있는 사이트 방문자
- 참가 권한이 있는 사이트 구성원
- 모든 권한이 있는 사이트 소유자

SharePoint가 민감한 비즈니스 콘텐츠를 보호하는 데 실패하는 경위

내부자 위협으로 인한 데이터 침해가 더 흔해지고 그 결과가 더욱 심각해짐에 따라 시스템 관리자를 투명하게 유지하거나 실수로 조직을 위험에 노출시키는 것을 막고자 하는 보안 제어력이 점점 더 중요해지고 있습니다. 하지만 SharePoint 기본 제공 툴은 다음 네 가지 주요 영역에서 한계가 있습니다.

- 사이트 프로비저닝 제어력 부족
- 확장할 수 없는 권한 모델
- 중앙 집중식 보안 및 거버넌스 제어
- 위치 대 콘텐츠 보안 및 제어

사이트 프로비저닝 제어력 부족

사이트와 페이지를 생성하기 위해 사용자나 사용자 그룹에 관련 권한이 할당될 수 있지만, SharePoint는 사이트 생성 프로세스에 대한 제어력이 거의 없습니다. 예를 들면 다음과 같습니다.

- 새 사이트 요청을 승인하거나 거부하기 위해 추가 워크플로우 프로세스를 즉시 호출할 수 없습니다. 사이트 소유자는 원하는 대로 거의 무제한에 가까운 하위 사이트 계층을 생성할 수 있기 때문에 상황이 더욱 복잡합니다.
- 생성된 사이트의 특성을 정의하는 데 필요한 지원이 제한적입니다. 사전 정의된 템플릿 목록에서 손쉽게 사이트를 생성할 수 있지만, 이 프로세스는 미묘한 제어 기능이 부족합니다. 마찬가지로 사이트 메타데이터, 콘텐츠 유형 및 기본 권한을 기본 사용자 모델 내부에서 관리 및 제어하기 어렵습니다.

이러한 한계로 인해 많은 SharePoint 시스템은 적절한 제어 기능 없이 사이트와 목록이 끊임없이 생성되고 증가하여 내부 콘텐츠 보안에 영향을 미칠 수 있는 "사이트 및 콘텐츠 스프롤" 현상을 급속히 겪게 됩니다. 이러한 사이트는 기업 거버넌스 규칙을 준수하지 않고 생성될 뿐 아니라 대개 활용도가 낮고 시스템 리소스만 소모하는 상태로 남습니다.

본질적으로 확장할 수 없는 표준 권한 모델

앞서 언급한 바와 같이 SharePoint 권한은 개체를 기반으로 합니다. 즉, 권한이 사용자나 그룹에 할당되고 사이트, 목록, 항목 또는 문서와 같은 개체에 적용됩니다. SharePoint는 한 번에 여러 개체(예: 10개의 사이트로 구성된 집합)의 권한을 확인하기 위해 바로 사용할 수 있는 간편한 방법을 지원하지 않습니다. 대신 각 개체를 개별적으로 검사해야 합니다.

여러 면에서 SharePoint의 기본 보안 모델은 팀 또는 공동 작업 사이트에 최적화되어 있습니다. 많은 사용자가 팜의 여러 부분에 광범위하게 액세스하는 엔터프라이즈 배포에는 잘 맞지 않습니다. 이 모델은 전적으로 개별 사용자 또는 사용자 그룹에 적용되어야 하는 정적 권한에 기반합니다. SharePoint 그룹은 도움이 되지만, 원하는 결과를 달성하려면 보통 Active Directory 그룹도 필요합니다. 이 그룹은 SharePoint 자체에서 유지 보수할 수 없으므로 최적의 솔루션이라 할 수 없습니다. 게다가 SharePoint 인터페이스는 각 Active Directory 그룹의 구성원 자격에 대한 가시성을 제공하지 않습니다.

표준 SharePoint 보안 모델의 일부 제한 사항은 다음과 같습니다.

- 사용자나 그룹을 수동으로 권한에 매핑할 경우 사이트 수가 증가함에 따라 시간과 비용이 많이 소모됩니다.
- 엔터프라이즈 전체에 SharePoint를 배포하는 경우 권한 수가 급격히 증가하는 경우가 종종 있습니다. 이러한 현상은 권한을 설정할 수 있는 세부적 수준(사이트 컬렉션, 사이트, 목록 및 항목)과 사용자 수 때문에 발생합니다.
- 분산된 SharePoint 사이트, 특히 개별 최종 사용자가 생성하고 관리하는 사이트에는 엔터프라이즈급 정책을 적용하기 어렵습니다. 예를 들어 외부 사용자가 "회사 기밀"로 표시된 리소스에 일관되고 추적 가능한 방식으로 액세스하지 못하도록 방지하는 것은 어려운 일입니다.
- 세부적 수준으로 권한을 지정하고 적용하는 것은 관리 및 유지 보수가 어렵고 많은 시간이 소요됩니다. 예를 들어 전체 문서 라이브러리가 아닌 개별 문서에 권한을 적용하는 일은 어렵습니다.
- 이전에 동의한 보안 정책을 변경하지 못하도록 방지할 수 없습니다. 필요한 제어 수준의 초기 구현과 시간이 지나도 유지되도록 이를 보장하는 것은 전혀 별개의 일입니다.

중앙 제어의 부족

사용자에게 다양한 권한 수준 조합을 할당하여 콘텐츠뿐 아니라 SharePoint 기능에 대한 액세스 권한을 부여할 수 있지만, 이로 인해 보안에 심각한 영향을 미칠 수 있습니다. 예를 들어 새로운 사용자가 참여하거나 기존 사용자가 조직 내 역할을 변경하면 해당 권한을 수동으로 구성하거나 변경해야 합니다. 이 추가적인 세분성 수준은 작업을 더 복잡하게 만듭니다.

마찬가지로 SharePoint는 새 사이트 요청을 승인하거나 이러한 사이트가 올바른 정책 및 거버넌스 규칙을 준수하도록 하는 중앙 집중식 옵션을 제공하지 않습니다. 대신에 SharePoint는 기본 제공 권한 관리 툴을 갖추고 있습니다. 이러한 툴은 직관적이지 않으며 원하는 결과를 달성하려면 함께 사용하거나 매우 특정한 방식으로 사용해야 합니다.

SharePoint의 기본 제공 권한 관리 툴에는 다음이 포함됩니다.

- **설정 페이지** - 대부분의 경우 SharePoint 보안은 특정 사이트 컬렉션 내부의 설정 페이지를 통해 관리됩니다. 각 SharePoint 사이트에는 사용자와 그룹을 관리할 수 있는 자체 설정 페이지가 있습니다. 라이브러리와 목록에도 자체적인 설정 페이지가 있습니다. 하지만 이러한 페이지에 대한 액세스 권한으로 다수의 다른 구성 옵션에도 액세스할 수 있으며, 이러한 옵션 중 일부는 활성화 시 되돌릴 수 없습니다.
- **중앙 관리** - 브라우저를 통해 액세스하는 별도 툴인 중앙 관리 콘솔은 설정 페이지보다 더 높은 수준의 구성 옵션을 제어할 수 있는 기능을 제공합니다. 여기에는 웹을 통해 익명으로 SharePoint 사이트에 액세스할 수 있도록 허용하는 등의 매우 강력한 설정이 포함됩니다. 중앙 관리에는 상태, 검색 및 타이머 작업에 대한 전반적인 관리자 보고서뿐만 아니라 여러 유용한 분석 보고서도 포함되어 있습니다. 이러한 툴은 사용자가 SharePoint와 상호 작용하는 방법과 시기를 강조 표시하고, 관리자는 이 툴을 통해 콘텐츠 수준에서 더욱 세부적 정보를 수집하기 위한 설정을 활성화할 수 있습니다.
- **Powershell** - 텍스트 중심 명령줄 언어인 PowerShell은 SharePoint에서 구성 및 보고하는 데 사용할 수 있는 매우 기술적인 툴입니다. 대량 관리 및 반복 가능 프로세스와 같은 스크립팅 툴의 모든 장점을 제공합니다. 하지만, 학습 곡선이 매우 가파릅니다. 기술적 역량이 탁월한 사용자를 제외하면 모두 “cmdlets”(PowerShell의 구성 요소 중 하나)를 완벽히 익히고 그래픽 사용자 인터페이스의 부족을 극복하는 데 어려움을 겪을 수 있습니다.

위치 대 콘텐츠 보안 및 제어

권한 관리 및 사이트 프로비저닝과 관련된 이전 문제가 해결되더라도 일반적으로 민감한 파일을 보호하는 방법과 관련된 다른 문제는 여전히 남아 있습니다. 우리는 보통 콘텐츠 그 자체가 아닌 위치에 대한 액세스를 확보하는 데 중점을 두고 많은 노력을 기울입니다. 그런데 의도적으로 또는 의도치 않게 문서를 보안 수준이 낮은 위치로 이동시키면 어떻겠습니까?

위치에 관계없이 콘텐츠 자체를 보호할 수 있는 기술이 있습니다. Microsoft는 SharePoint Online 내 통합 DLP(Data Loss Prevention) 기능과 권한 관리 기능을 개선했습니다.

이러한 기술은 문서와 함께 이동하거나 문서 내 콘텐츠의 특성을 탐지하는 액세스 및 사용 권한을 적용합니다(예: 생년월일이나 주민등록번호와 같은 PII(Personally Identifiable Information)가 포함된 경우). PII가 탐지되면 이 유형의 정보가 SharePoint Online 사이트에 추가되었다고 사용자에게 경고할 수 있습니다.

이 접근 방법은 Office 365에서 몇 가지 이점을 제공하지만, 특히 DLP(Data Loss Prevention)와 같은 온-프레미스 SharePoint에 대한 옵션은 매우 제한적입니다.

하지만 이는 많은 이들이 긴급하게 해결해야 할 부문입니다. 최근의 데이터 침해와 영향을 받은 조직의 후속 피해(작업, 매출, 평판 손실, 규제 벌금 등)가 이 문제를 급격히 대두시켰습니다.

Quest

Metalogix® ControlPoint로 보안 해결

SharePoint는 여러 기본 제공 툴을 통해 플랫폼 전반의 보안 문제를 관리할 수 있는 임시 수단을 제공합니다. 그러나 이러한 툴은 사실상 너무 기술적이거나 범위가 제한적입니다. 보안 시스템이 사이버 범죄자와 내부자의 위협에 맞춰 대응하기 어렵다는 이유만으로 사용자가 SharePoint의 사용을 중단하지는 않습니다. 하지만 올바른 수준의 보안, 규정 준수 및 관리 툴을 추가하면 조직은 성공을 이끄는 조합을 이룰 수 있습니다.

Metalogix® ControlPoint는 풍부한 기능과 직관적인 사용자 인터페이스를 통해 중요한 비즈니스 데이터를 자동으로 제어할 수 있는 방법을 제공합니다. 온-프레미스, 클라우드 혹은 하이브리드 SharePoint 배포든 단일 팜이든 아니면 다중 팜이든 ControlPoint는 한 위치에서 이 모두를 관리하는 데 이상적입니다. ControlPoint는 MSO-CAF 인증을 받았으며 Microsoft에서 Office 365 전용 환경으로 사전 승인 받았습니다.

SharePoint를 사용하고 있으며 보안 위협이 우려된다면 ControlPoint의 이점을 고려해보십시오.

Quest

CONTROLPOINT의 이점

SharePoint에서 사이트를 생성하는 기본적인 프로세스는 간단합니다. 하지만 체계적인 방식으로 사이트 생성을 제어하고 거버넌스 정책에 따라 사이트가 생성되도록 보장하며 확인하며 필요한 권한과 콘텐츠 설정을 확인하는 작업은 그리 간단하지가 않습니다. 실제로 기본 SharePoint에서는 사이트 프로비저닝을 적절히 제어할 수가 없습니다.

이로 인해 SharePoint 시스템은 일반적으로 사이트와 하위 사이트로 구성된 여러 계층으로 확장되며 복잡해집니다. 중앙 관리자는 새로 생성된 콘텐츠를 인식하더라도 이를 파악하기가 힘들어 보안 및 거버넌스에 대한 제어력을 상실하게 됩니다.

상대적으로 권한이 제한된 최종 사용자는 하위 사이트를 무수히 생성할 수 있으며, 이중 많은 사이트가 알 수 없는 상태로 방치됩니다. 이러한 각 사이트는 잠재적인 보안 위험을 야기합니다. 어떤 콘텐츠가 포함되어 있는가? 여전히 필요한 콘텐츠인가? 누가 액세스할 수 있는가? 사이트 소유자는 누구이며 이들이 아직도 동일한 팀이나 회사에서 근무하고 있는가?

Metalogix ControlPoint를 사용하면 사이트 컬렉션과 하위 사이트를 자동으로 프로비저닝할 수 있습니다. 모든 사이트와 사이트 컬렉션이 올바른 템플릿, 속성 및 거버넌스 정책(옵션)으로 설정되도록 프로비저닝 프로필을 설정할 수 있습니다. 그런 다음 사이트 승인, 거부 또는 편집 시 자동 이메일을 포함하는 승인 프로세스 워크플로우를 통해 사이트 요청이 전송됩니다.

사이트 프로비저닝은 새로 생성된 사이트가 생성된 시점부터 구조, 콘텐츠 및 메타데이터에 대한 조직의 표준 및 정책을 준수하도록 돕습니다. 예를 들어 사이트에서 생성된 모든 목록에서 버전 관리 기능이 활성화되어 있거나 감사 기능이 활성화되어 매일 비즈니스 관리자에게 감사 보고서를 보내는 경우 ControlPoint에서 생성한 거버넌스 정책에는 활성화 및 비활성화되는 사이트 및 사이트 컬렉션 기능을 지정하는 규칙이 포함될 수 있습니다. 기본 제공 사이트 정의 및 사이트 템플릿과 함께 사용하면 사용자가 특정 구조를 준수하는 사이트를 생성할 수 있고 특정 SharePoint 기능이 활성화되며 악의적 관리자가 이를 절대 변경할 수 없습니다.

ControlPoint의 사이트 프로비저닝 툴은 최종 사용자를 위한 SharePoint의 직관적인 사이트 생성 인터페이스를 유지 보수하는 데 도움을 주므로, 최종 사용자는 SharePoint 사이트에서 직접 새 사이트 및 사이트 컬렉션을 요청할 수 있습니다. 단, 시스템이 장기간에 걸쳐 확장되고 개발됨에 따라 엔터프라이즈에 필요한 제어 기능을 추가합니다.

자신 있게 권한 관리

SharePoint 권한 관리에서 가장 어려운 부분은 권한 정책 규정 준수를 보장하고 시간이 흘러도 보안 침해 및 민감한 콘텐츠에 대한 무단 액세스를 방지하는 것입니다. 이 문제는 최신 버전의 SharePoint 사용 시 외부에서 액세스할 수 있는 "공유" 기능과 깊은 관련이 있습니다.

SharePoint 환경이 성장함에 따라 권한의 복잡성도 기하급수적으로 커지는 추세입니다. SharePoint 그룹이 산발적으로 사용되고 직접 권한은 혼란스러운 상황을 초래하며 사용자는 부서를 옮기거나 다 같이 떠나 버립니다. SharePoint는 이러한 문제에 대한 전체적인 관점을 제공하지 않습니다. ControlPoint는 다릅니다.

ControlPoint에는 SharePoint 사용자, 그룹 및 권한 관리를 용이하게 하는 다양한 옵션이 포함되어 있습니다. 이러한 작업을 단일 사이트, 사이트 컬렉션, 다중 사이트 컬렉션 또는 전체 팜과 같은 다양한 계층 수준에서 수행할 수 있습니다.

ControlPoint는 장기적인 권한 정책 규정 준수를 지원할 수 있습니다. 단일 콘솔을 사용하여 모든 사이트, 사이트 컬렉션 및 팜에서 권한과 사용자를 감사, 정리 및 관리할 수 있습니다. 덕분에 Active Directory 또는 SharePoint 그룹을 통해 직접 할당되었든, 상속되었든, 또는 지정 부여되었든 관계없이 권한의 모든 측면을 분석하고 관리할 수 있습니다.

ControlPoint의 정책 적용 기능은 액세스 권한, 버전 관리 사용, 파일 업로드 제한 사항, 사이트 할당량 및 사이트 템플릿 사용도 자동으로 제어합니다. 사이트 관리자나 고급 사용자에게 제어 권한을 위임할 수도 있습니다.

이제 ControlPoint에서 정책 기능이 향상되고 SharePoint 내에서 권한 변경을 방지하기 위한 새로운 규칙이 포함되었습니다. 작업을 방지할 수 있을 뿐만 아니라 다음을 수행하려 시도하면 알림을 전송할 수도 있습니다.

- 권한 추가 또는 삭제
- 권한 수준 추가, 삭제 또는 업데이트
- SharePoint 그룹 추가, 삭제 또는 업데이트
- SharePoint 그룹 구성원 추가 또는 삭제
- 권한 상속 중단 또는 복원

사용자 감사 부담에서 해방

SharePoint 환경 배포, 업그레이드 계획 또는 유지 보수 검사 수행 시 누가 민감한 콘텐츠에 액세스 할 수 있는지 파악하는 것이 중요합니다. SharePoint의 표준 기능은 누가 SharePoint 구조 또는 데이터의 어떤 부분에 액세스할 수 있는지에 대한 정보를 제공하지 않습니다.

ControlPoint의 감사 기능은 이러한 성질의 모든 요청에 대한 신속한 응답을 보장합니다. ControlPoint는 특정 기간 동안 민감한 콘텐츠에 누가 액세스했는지에 대한 정보를 제공합니다. ControlPoint의 강력한 감사 기능은 복잡하고 시간이 많이 소요되는 규정 준수, 감사 및 보고 작업의 부담을 없애줍니다.

ControlPoint는 구성 변경부터 액세스되거나 삭제된 문서에 이르는 모든 내역이 기록된 보고서를 제공합니다. 각 보고서에는 이벤트 날짜와 시간, 책임 사용자와 같은 세부 정보가 포함되어 있습니다. 또한 사이트 컬렉션, 사이트, 목록 또는 문서에 관계없이 해당 범위를 제공합니다 (각각에 대한 URL 포함).

이 정보는 기존 사용자나 더는 액세스 권한이 없는 사용자가 거버넌스 계획 및 공식 정책을 준수하는지를 파악해야 하는 조직에 중요합니다. ControlPoint를 사용하여 필요에 따라 또는 특정

Quest

감사나 보안 프로젝트의 일환으로 이 데이터를 확인할 수 있습니다. ControlPoint는 장기적인 규정 준수를 위해 감사 데이터를 아카이브할 수도 있습니다.

PII(PERSONALLY IDENTIFIABLE INFORMATION) 식별 및 보안

PII와 같은 민감한 콘텐츠의 대형 데이터 유출 사고는 이러한 유형의 정보를 올바르게 보호해야 하는 필요성을 부각시킵니다. 특정 사이트나 문서 라이브러리에만 PII가 존재하도록 허용하는 등과 같이 위치 기반 보안에만 의존하는 것으로는 충분치가 않습니다. 콘텐츠를 손쉽게 복사하거나 다른 위치로 이동하거나 PII가 포함된 새 콘텐츠를 잘못된 위치에 업로드할 수 있기 때문입니다.

ControlPoint 및 Metalogix Sensitive Content Manager는 이 유형의 콘텐츠가 존재하는 위치를 식별하여 PII를 위한 새로운 보안 계층을 제공하고 이 콘텐츠를 보호하기 위한 조치에 필요한 툴을 SharePoint 관리자에게 제공합니다.

SharePoint 내 전체 팜 또는 독립 위치에서 PII가 있는지 스캔할 수 있으며 포함된 정보의 심각도 수준에 따라 콘텐츠를 분류합니다. PII 탐지 시 콘텐츠를 자동으로 격리 또는 삭제하거나 추가 작업을 위해 콘텐츠에 플래그를 지정할 수 있습니다.

Sensitive Content Manager를 배포하여 새로 추가된 SharePoint 콘텐츠 내의 PII를 거의 즉각적으로 자동 탐지할 수도 있습니다.

ControlPoint는 PII 탐지 시 SharePoint 관리자가 여러 작업을 수행하는 데 필요한 툴을 제공합니다. 누가 PII 포함 콘텐츠에 액세스할 수 있는지 확인하기 위해 Sensitive Content Manager 스캔에 대해 권한 보고서를 실행할 수 있으며 보안 위험이 식별되면 개선 권한 관리 단계를 수행할 수 있습니다. 또한, 관리자는 ControlPoint를 통해 최근에 민감한 콘텐츠에 액세스한 사람에 대한 보고서를 실행할 수 있습니다.

PII 포함 콘텐츠 탐지 시 지정된 콘텐츠 검토자가 승인할 때까지 업로드를 차단하거나 격리할 수 있습니다.

Quest는 온-프레미스 및 클라우드 모두에서 SharePoint의 PII와 같은 민감한 콘텐츠에 대한 DLP(Data Loss Prevention)를 재정의하고 있습니다. 고급 머신 러닝 기술을 기반으로 하는 Sensitive Content Manager는 기존의 데이터 보호 전략을 뛰어넘어 콘텐츠의 컨텍스트 인식 식별, 필터링 및 분류에 대해 훨씬 높은 정확도를 제공합니다. 게다가, 솔루션의 머신 러닝 특성 덕분에 즉시 사용할 수 있으며 다른 DLP 솔루션에서 일반적으로 요구되는 규칙 정의와 같이 오랜 시간과 비용이 소모되는 컨설팅 구성 연습이 필요하지 않습니다.

Quest

Metalogix ControlPoint가 데이터 손실 방지 문제를 해결하는 방식

- ControlPoint의 사이트 프로비저닝 기능으로 새 사이트 및 사이트 컬렉션에 대한 최종 사용자 요청 관리를 손쉽게 자동화할 수 있습니다.
- ControlPoint는 고급 사용자 권한 관리 기능을 지원합니다. 전체 팜에서, 또는 사이트마다 권한을 빠르게 수정할 수 있습니다. 사용자 간에 권한을 빠르게 복제하거나 자동으로 정리할 수 있습니다. 또한, ControlPoint는 부담 없는 마이그레이션 작업을 위해 사이트 권한 백업 및 복원을 지원합니다.
- ControlPoint를 사용하면 사용자가 문서 삭제 또는 하위 사이트 생성과 같은 특정 작업을 수행하지 못하도록 방지할 수 있습니다. 알림을 통해 모든 금지된 작업 시도를 관리자에게 알릴 수 있습니다. ControlPoint는 특정 수준 또는 그룹 업데이트와 같은 권한 변경을 방지하는 기능을 비롯하여 SharePoint 팜에 대한 추가 정책을 지원합니다.
- ControlPoint에는 기본 SharePoint와 비교할 수 없을 정도로 풍부한 정보를 제공하는 여러 감사 및 거버넌스 기능이 포함되어 있습니다. 여기에는 구성 변경과 문서 및 콘텐츠 액세스에 대한 보고서가 포함됩니다. 보고서에는 책임 사용자, 연관된 SharePoint 개체의 범위는 물론 관련 이벤트의 시간과 날짜가 포함됩니다.
- ControlPoint 및 Sensitive Content Manager는 클라이언트의 구체적인 요구 사항에 따라 맞춤 구성할 수 있으며 SharePoint 내 PII를 탐지하기 위해 바로 사용할 수 있는 매우 정확하고 유연한 솔루션을 제공합니다. 이렇게 조합된 솔루션은 고급 신경망 기반 머신 러닝을 사용하여 문서를 식별, 추적 및 보호하는 기능을 제공하며, 이를 통해 점점 더 복잡해지는 엔터프라이즈 환경 속에서 더욱 강력한 수준의 상황별 콘텐츠 인식이 가능합니다.

결론

SharePoint에서 민감한 비즈니스 콘텐츠를 보호하는 것은 쉬운 일이 아닙니다. 표준 인증 및 권한 모델은 장기적으로 관리하기 어려운 수준의 세분성을 허용할 뿐만 아니라 기본 SharePoint는 플랫폼 전반에 걸친 사용자 감사 수단을 거의 제공하지 않습니다. 동시에, 적절한 권한을 가진 최종 사용자가 프로비저닝 제어 기능이 거의 없는 상태로 사이트 및 하위 사이트를 너무 쉽게 생성할 수 있습니다. 이로 인해 대개 어떤 형태의 거버넌스도 따르지 않고 제멋대로 확장하는 계층 구조가 발생합니다.

SharePoint 콘텐츠 보호에 도움이 될 수 있는 전체 Metalogix 솔루션 제품군에 대한 자세한 정보는 quest.com/metalogix를 참조하십시오.

Quest

QUEST 소개

Quest는 급변하는 엔터프라이즈 IT 세계에 소프트웨어 솔루션을 제공합니다. 당사는 데이터 폭증, 클라우드 확장, 하이브리드 데이터 센터, 보안 위협 및 규정 요구 사항으로 인한 문제를 간소화하도록 도움을 드립니다. 당사는 Fortune 500의 95%와 Global 1000의 90%를 포함한, 100개국에 걸친 130,000개 회사의 글로벌 제공업체입니다. 1987년 이래로 당사는 현재 데이터베이스 관리, 데이터 보호, ID 및 액세스 관리 , Microsoft 플랫폼 관리 및 통합 엔드포인트 관리를 포함하는 솔루션의 포트폴리오를 구축해왔습니다. Quest를 통해 조직은 IT 관리에 소비되는 시간을 줄이고 비즈니스 혁신에 더 많은 시간을 할애할 수 있습니다. 자세한 내용은 https://www.quest.com/kr/을 참조하십시오.

이 제품의 향후 사용과 관련하여 문의 사항이 있다면 다음 연락처로 문의하십시오.
www.quest.com

Ebook-AutomatingControlSPContent-US-GM-KO-WL-41045