01 용어 정리

용어 정리

Data Loss Prevention(DLP)은 조직의 민감한 데이터가 허가 없이 밖으로 나가는 것을 탐지하고 막는 기능입니다. 이 가이드를 읽는 데 바탕이 되는 핵심 용어를 흐름에 따라 풀어 둡니다. 제품·기술 용어는 영어 그대로 두고, 일반 명사는 한국어로 적었습니다.

DLP의 뼈대 — Blade·Gateway·Data Type

가장 먼저 알아야 할 셋이 **DLP Software Blade**, **DLP Gateway**, **Data Type** 입니다. **Data Loss Prevention** 은 Security Gateway 위에서 도는 Software Blade 로, 기밀 정보가 조직 밖으로 새어 나가는 것을 탐지·차단합니다(약어 DLP). 이 블레이드를 켠 게이트웨이를 흔히 **DLP Gateway** 라 부릅니다. 그리고 **Data Type** 은 보호할 데이터를 분류해 정의한 것 으로, "신용카드 번호 패턴", "특정 키워드 목록", "사내 문서 템플릿" 같은 식으로 무엇을 지킬지를 규정합니다. DLP 정책의 규칙은 바로 이 Data Type을 두고 짜집니다.

> *Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.*
>
> — AdminGuide, "Glossary" (p.342)

흥미로운 점은 **Content Awareness** 도 같은 Data Type을 쓴다는 것입니다. Content Awareness는 데이터 가시성·집행을 제공하는 별도 Software Blade(약어 CTNT)인데, DLP와 Data Type 개념은 공유하되 기능과 동작은 서로 독립적 이라 게이트웨이가 각각 따로 집행합니다.

사람과 알림 — Data Owner·UserCheck

DLP를 사람 중심으로 돌아가게 하는 두 축이 **Data Owner** 와 **UserCheck** 입니다. **Data Owner** 는 조직 안에서 특정 영역의 정보와 파일을 책임지는 사람 으로, 자기 데이터가 어떻게 움직이는지 자동 알림과 리포트로 받아 봅니다. **UserCheck** 는 위반이 일어났을 때 사용자에게 실시간으로 알리고, 보낼지 말지를 사용자 스스로 결정하게 하는 방식입니다. 특히 **Ask User** 모드 는 전송을 잠시 붙들어 둔 채 사용자에게 사유를 묻고, 사용자가 결정할 때까지 기다립니다. 이 사용자 결정과 사유가 모두 로그로 남아 정책을 다듬는 밑거름이 됩니다.

인프라 용어

게이트웨이를 둘러싼 환경을 가리키는 용어도 익혀 둡니다. **Security Gateway** 는 트래픽을 검사하고 보안 정책을 집행하는 Check Point 서버 이고, **Security Management Server** 는 객체와 정책을 관리하는 서버 입니다. 관리자는 GUI 도구인 **SmartConsole** 로 작업하는데, DLP는 일부 설정을 **SmartDashboard**(R77.30 이하의 옛 GUI, 지금은 특정 레거시 설정용으로만 남음) 에서 하므로 두 화면을 오가게 됩니다. 둘 이상의 게이트웨이를 묶은 **Cluster**, 트래픽을 통과시키는 L2 다리로 동작하는 **Bridge Mode**, 인증서를 발급하는 내부 인증 기관 **ICA**, 서버 간 안전 통신 메커니즘 **SIC** 도 자주 나옵니다.

사용자·그룹은 보통 외부 **LDAP** 서버(예: Active Directory)로 관리하며, DLP는 이를 통해 누가 조직 내부 사람인지 파악합니다. **HTTPS Inspection** 은 SSL로 암호화된 트래픽을 풀어 검사 하는 기능으로, 암호화된 채널로 데이터가 새는 것을 잡으려면 함께 켜야 합니다.

동작과 식별 — Action·MultiSpect·CPcode

규칙에 걸렸을 때 DLP가 취하는 **Action** 은 네 가지입니다 — **Detect**(통과시키되 로그만), **Inform User**(통과시키되 위반 사실을 알림), **Ask User**(붙들어 두고 사용자에게 물음), **Prevent**(차단) . 데이터를 정확히 식별하기 위한 기술로는 여러 파라미터를 상관 분석하는 **MultiSpect** 와, 완전히 맞춤형 식별 로직을 짜는 **CPcode** 가 있습니다. 깊이 있는 설명은 DLP 소개와 Data Type 정의하기에서 이어집니다.

02 DLP 소개 — 왜 필요한가

DLP 소개 — 왜 필요한가

오늘날 데이터는 그 어느 때보다 쉽게 옮겨지고, 그 대부분이 어떤 수준으로든 민감 합니다. 이 장은 DLP가 왜 필요한지, Check Point가 이를 어떻게 푸는지, 그리고 관리자가 무슨 일을 하는지를 잡습니다.

데이터 유출이라는 위험

지식재산처럼 가치가 기밀 유지에 달린 데이터 도 있고, 법·규제 때문에 지켜야 하는 데이터도 있습니다. 유출되면 단순한 망신을 넘어 경쟁력 상실, 고객 이탈, 법적 책임 으로 이어질 수 있습니다. 문제를 키우는 것은 정작 유출 대부분이 악의가 아니라 실수에서 비롯된다는 점입니다 — 클라우드 서버, 공유 문서, 일을 집에 가져가는 직원처럼, 정보 공유를 편하게 만든 도구들이 동시에 돌이킬 수 없는 실수도 쉽게 만듭니다.

그래서 가장 좋은 해법은 보호 대상 데이터가 조직을 떠나기 전에 자동으로 붙잡는 정책 을 두는 것이고, 이것이 바로 Data Loss Prevention(DLP)입니다.

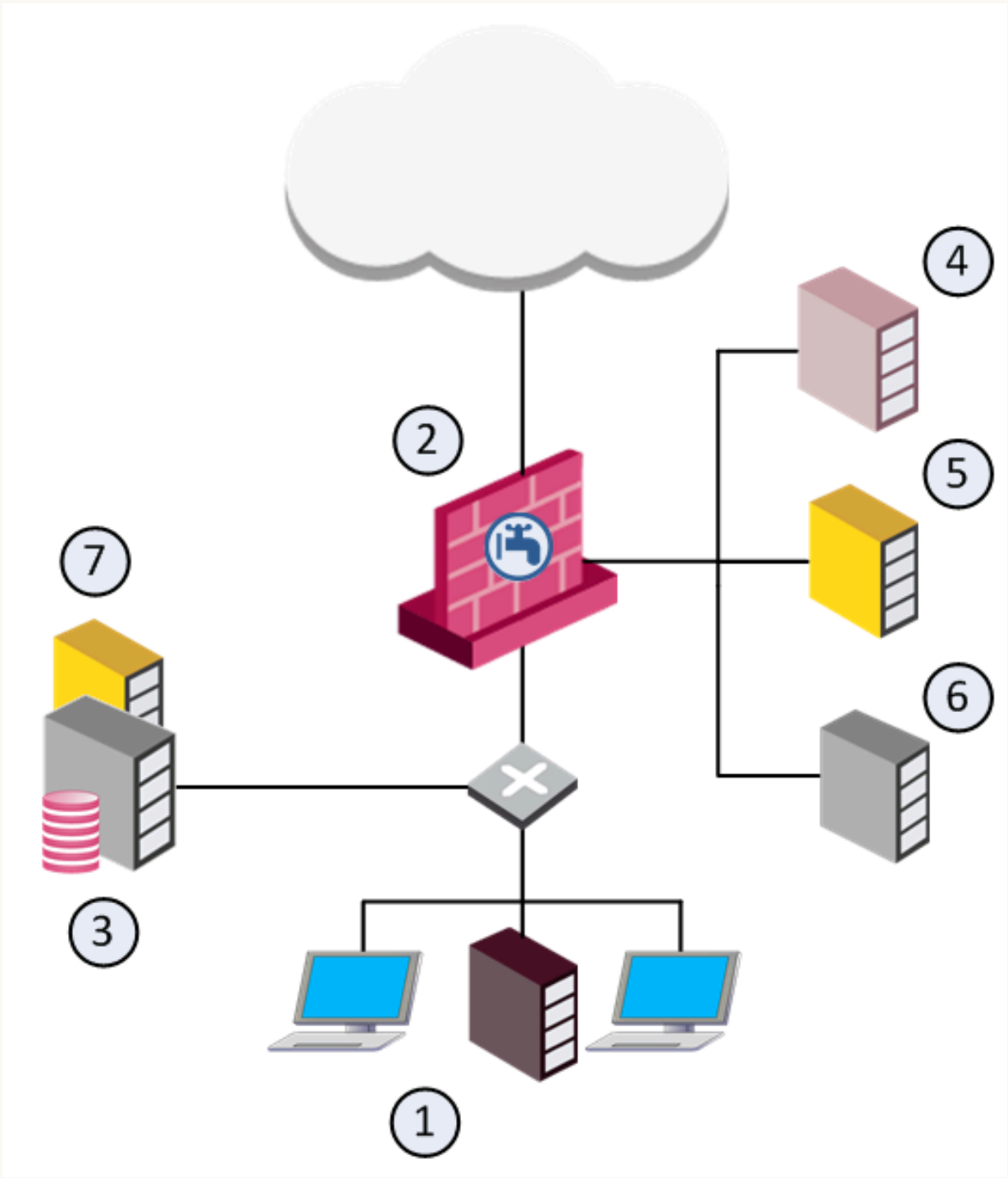
> *Data Loss Prevention identifies, monitors, and protects data movement through deep content inspection and analysis of transaction parameters (such as source, destination, data object, and protocol), with a centralized management framework.*
>
> — AdminGuide, "The Need for Data Loss Prevention" (p.12)

즉 DLP는 출발지·목적지·데이터 객체·프로토콜 을 함께 보고 콘텐츠를 깊이 검사해, 기밀 정보의 무단 전송을 탐지·차단합니다. 이메일 본문과 수신자, 첨부 파일(압축돼 있어도), FTP 업로드, 웹 게시, 웹메일 등이 모두 검사 대상입니다.

Check Point가 DLP를 푸는 방식

Check Point DLP의 강점은 설치 첫날부터 쓸 만한 정책이 준비돼 있고, 거기서부터 다듬어 간다는 데 있습니다. 이를 떠받치는 핵심 기능이 셋입니다. 첫째 **UserCheck** 는 사용자에게 실시간으로 위반을 알리고 처리를 맡깁니다 . UserCheck가 없으면 관리자가 모든 이메일과 데이터 이동을 일일이 검토·승인해야 하므로 다른 제품들은 탐지에만 머무는데, UserCheck는 결정을 사용자에게 분산 시킵니다. 사용자는 왜 걸렸는지를 보고 보낼 사유를 적어야 하며, 그 결정과 사유가 로그로 남아 실제 사용에 기반한 정책을 만들게 해 줍니다. 둘째 **MultiSpect** 는 여러 파라미터를 상관 분석 하고 Compound Data Type·CPcode까지 동원해 정확도를 높입니다. 셋째 **Out of the Box Security** 는 미리 정의된 풍부한 Data Type 으로 곧바로 효과적인 정책을 돌립니다. 여기에 데이터 책임자에게 자동 리포트를 주는 **Data Owner Auditing** 이 더해집니다.

DLP가 데이터를 잡는 흐름은 이렇습니다 — Security Gateway에 DLP Blade를 켜면 DLP Gateway가 되고, SmartConsole로 정책을 설치합니다. 게이트웨이는 지원 프로토콜로 흐르는 데이터를 모두 가로채 HTTP proxy나 메일 서버로 나가기 전에 검사하며, 필요하면 Active Directory/LDAP로 내부 조직 구성원을 식별합니다. Microsoft Exchange 클라이언트 간 내부 메일까지 검사하려면 Exchange 서버에 Exchange Security Agent 를 설치해 내부 메일을 게이트웨이로 넘깁니다(메일 서버와 Exchange 연동). 어느 규칙에도 안 걸리면 트래픽은 그냥 통과합니다.



① 내부 네트워크 ② DLP Blade를 켠 Security Gateway ③ Security Gateway ④ Security Management Server ⑤ HTTP proxy ⑥ 메일 서버 — Dedicated DLP Gateway 배치

두 가지 배치 — Integrated vs Dedicated

DLP Gateway는 두 가지로 둘 수 있습니다. **Integrated** 는 기존 Security Gateway에 DLP Blade를 함께 켜는 방식으로, Firewall 등 다른 블레이드와 한 장비에서 같이 돕니다. 둘레(perimeter)에 있으면 SMTP 서버가 외부 목적지 전송만 DLP로 넘깁니다. **Dedicated** 는 보호용 게이트웨이 뒤에 DLP 전용 게이트웨이를 따로 두는 방식입니다.

> 권 장
>
> Dedicated DLP Gateway는 Bridge Mode로 구성하세요. 다리는 네트워크 라우팅에 투명해 기존 토폴로지에 끼워 넣기 쉽습니다. 또 하드웨어 자원을 아끼려면 DLP Blade만 켜는 것이 좋습니다.

부서 간 데이터 이동까지 검사하고 싶다면 게이트웨이를 둘레가 아니라 사용자망과 서버 사이에 두는 대안 배치도 있습니다. 예컨대 출발지는 특정 네트워크, 목적지는 그 바깥(Outside Source)으로 둔 규칙은 이 배치에서만 동작합니다.

규칙에 걸리면 무슨 일이 일어나나

게이트웨이가 트래픽을 잡아 정책과 대조해 규칙에 걸리면, 먼저 사건(incident)이 로그로 남고 원본 데이터가 안전한 저장소에 보관 됩니다. 그다음 규칙의 Action이 실행됩니다 — **Detect** 는 사용자에게 알리지 않고 로그만, **Inform User** 는 위반을 알리되 통과, **Ask User** 는 메시지를 붙들고 DLP Portal 링크를 보내 사용자가 보낼지 버릴지 결정하게, **Prevent** 는 차단 합니다. 필요하면 Data Owner를 비롯한 관계자에게 알림이 갑니다. 동작별 세부는 UserCheck에서 다룹니다.

> 참 고
>
> DLP가 잡은 원본은 보안 검토 목적으로만 저장됩니다. 운영 전에 이 사실을 사용자에게 반드시 사전 공지 하세요. 위반 전송이 저장되고 보안 담당자가 열람할 수 있다는 점, 그리고 Ask User 위반을 어떻게 처리하는지를 미리 알리는 것이 모범 사례입니다.

DLP 관리자의 일

관리자의 작업은 한 번에 끝나는 게 아니라 돌고 도는 다듬기의 순환 입니다. Data Type을 정의하고 → Out of the Box 정책으로 강한 탐지를 첫날부터 켠 뒤 → 사전 정의 Data Type을 우리 조직 데이터에 맞게 손보고 → 필요한 규칙을 켜고 끄고 → 우리만의 Data Type을 만들고 → 사건을 모니터링하며 Data Owner와 소통하고 → 정책을 정밀 조정 합니다. 이 순환이 탐지(Detect)만 하던 정책을 점차 차단(Prevent) 정책으로 옮겨 가게 합니다(규칙 만들기).

관리자 권한은 통째로 줄 수도, 일부만 줄 수도 있습니다. 전체 권한이면 로그의 모든 필드, 잡힌 원본 데이터(실제 이메일·FTP 파일·HTTP 게시), 격리 메일의 전송/폐기 까지 다룰 수 있습니다. 권한은 **Manage & Settings** > **Permissions & Administrators** 에서 권한 프로파일로 나누는데, **Monitoring and Logging** 의 DLP logs including confidential fields (이게 없으면 기밀 필드가 `** Confidential **` 로 가려짐)와 View/Release/Discard DLP messages 옵션으로 세밀하게 조정합니다. 본격적인 설정은 빠른 시작에서 시작합니다.

03 빠른 시작 — 5단계 도입

빠른 시작 — 5단계 도입

DLP를 처음 켤 때의 전체 그림을 준비 → 게이트웨이 구성 → SmartDashboard 설정 → 정책 설치 → (선택) UserCheck Client 배포 의 다섯 단계로 잡습니다. 세부는 뒤 장에서 깊이 다루니, 여기서는 순서와 큰 흐름만 익히면 됩니다.

> 중 요
>
> DLP Blade를 켜기 전에 R82 Release Notes에서 DLP 요구사항과 지원 플랫폼을 먼저 확인하세요. 환경에는 DNS 서버가 반드시 있어야 합니다.

1·2단계 — 준비와 게이트웨이 구성

먼저 토대를 세웁니다. Management Server와 Security Gateway/Cluster Member를 설치 하고, SmartConsole로 Management Server에 접속한 뒤 **Gateways & Servers** 에서 게이트웨이 객체를 만듭니다. 그다음 그 객체의 **General Properties** > **Network Security** 에서 **Data Loss Prevention** Software Blade를 켜면 Data Loss Prevention Wizard가 떠 핵심 항목들을 차례로 묻습니다.

마법사가 묻는 것은 **Email Domain**(내부·외부 이메일을 구분하는 우리 도메인), **My Organization Name**(조직을 가리키는 이름·문구로 탐지 정확도를 높임), **DLP Portal과 Mail Relay**(자가 처리 포털과 메일 중계 서버), **Protocols**(정책을 적용할 프로토콜) 입니다. Active Directory 연결은 지금 해도 되고 나중에 해도 됩니다(AD·LDAP 연동). 마법사를 마치면 게이트웨이의 토폴로지에서 인터페이스가 내부/외부로 제대로 지정됐는지 확인합니다 — DLP는 기본적으로 내부망에서 외부망으로 가는 트래픽을 검사하므로 이 구분이 중요합니다. 메일 서버가 Microsoft Exchange라면 이 DLP Gateway를 향한 SMTP Relay 로 설정해 둡니다.

3단계 — Legacy SmartDashboard에서 세부 설정

DLP의 상세 설정은 옛 GUI인 **SmartDashboard** 에서 합니다. **Manage & Settings** > **Blades** 의 Data Loss Prevention 영역에서 **Configure in SmartDashboard** 를 누르면 DLP 탭이 열립니다. 여기서 **My Organization**(이메일·도메인·네트워크·사용자·VPN·조직명), **Data Types**, **Repositories**, (선택) **UserCheck** 상호작용 객체, **Additional Settings**(Protocols·Mail Server·Watermarks·Advanced), **Policy** 규칙, (선택) **Whitelist Policy** 를 차례로 구성합니다. 작업이 끝나면 상단 **Launch Menu** > **File** > **Update** 로 저장하고 **Exit** 합니다. 각 항목은 Out of the Box, Data Type 정의하기, UserCheck에서 자세히 다룹니다.

> 참 고
>
> UserCheck 상호작용 객체는 SmartDashboard에서만 만들고 고칠 수 있고, SmartConsole에서는 안 됩니다. DLP가 두 화면을 오가는 이유가 여기 있습니다.

4·5단계 — 정책 설치와 UserCheck Client

설정을 마치면 SmartConsole에서 **Install Policy** 를 눌러 **Access Control** 정책을 해당 게이트웨이에 설치 합니다. 다만 Dedicated DLP Gateway에는 DLP Policy만 설치되고 이는 보안 정책이 아니므로, 환경에 보안 정책을 집행할 별도 Security Gateway가 있어야 합니다.

마지막으로 원하면 엔드포인트에 **UserCheck Client** 를 배포 합니다. 클라이언트를 설치하고 해당 게이트웨이/클러스터에 연결되도록 설정하면, 사용자가 시스템 트레이 팝업으로 위반을 바로 처리할 수 있습니다(UserCheck). 설치·배치의 구체적 절차는 설치와 배치로 이어집니다.

04 설치와 배치 — Gateway·Bridge·Proxy

설치와 배치 — Gateway·Bridge·Proxy

DLP Blade를 어디에, 어떤 모드로 켤지를 정하는 장입니다. Integrated/Dedicated 선택, 클러스터, Bridge Mode, AD/LDAP 연동, Web Proxy 연동 까지 배치의 갈림길을 짚습니다.

DLP Blade 켜기 — Integrated와 클러스터

소개에서 본 두 배치 중 Integrated는 기존 Security Gateway에 DLP Blade를 함께 켜 고, Dedicated는 전용 게이트웨이에만 켭니다. SmartConsole에서 게이트웨이/클러스터 객체를 열어 **Software Blades** 의 **Data Loss Prevention** 을 누르면 Data Loss Prevention Wizard가 떠 설정을 묻습니다(빠른 시작). 클러스터에서 켜면 모든 멤버에 한꺼번에 적용 됩니다.

클러스터에는 주의할 점이 둘 있습니다. ClusterXL **Load Sharing** 에서는 **Ask** 동작을 지원하지 않 으므로, 정책이 Detect·Inform·Prevent만 쓸 때 DLP가 동작합니다. 또 상태 동기화가 2분 간격 이라, 페일오버가 나면 새 Active 멤버가 직전 2분의 DLP 사건을 모를 수 있습니다.

Bridge Mode — 투명하게 끼워 넣기

Dedicated DLP Gateway는 Bridge Mode로 두는 것이 권장 됩니다. 다리는 L2 장치처럼 동작해 네트워크 라우팅에 투명 하므로, 기존 토폴로지를 건드리지 않고 끼워 넣을 수 있습니다. 다만 제약이 분명합니다 — 같은 트래픽을 두 인터페이스에서 두 번 봐선 안 되고, bridge 간 라우팅(VLAN 간 포함)은 미지원 입니다. VLAN 트렁크에 연결하면 모든 VLAN이 검사 대상이 되어 특정 VLAN만 빼는 것은 안 되며, bridge와 Layer3 인터페이스 사이 라우팅도 지원하지 않습니다.

> 참 고
>
> Bridge Mode 게이트웨이도 R76부터 High Availability 클러스터에 들어갈 수 있지만, 이 경우 **Ask User** 동작과 UserCheck Agent는 지원되지 않 습니다. Bond HA/LS(Link Aggregation 포함)도 bridge 인터페이스와 함께 쓸 수 없습니다.

SMTP Mirror Port Mode — 위험 없이 평가부터

본격 차단 전에 정책을 집행하지 않고 데이터 유출 실태만 먼저 파악 하고 싶다면 **Mirror Port Mode** 가 유용합니다. DLP Gateway를 스위치의 SPAN 포트에 연결하면 통과하는 모든 패킷의 사본을 받 아 SMTP·HTTP 스트림을 재구성하고 DLP 엔진으로 검사하되, 실제 트래픽은 건드리지 않습니다. 최소한의 구성 위험으로 전체 아웃바운드 트래픽을 평가 하기에 좋습니다. Gaia에서는 Monitor Mode가 필요하며(sk70900), R77.10 이상은 인터페이스를 monitor/tap으로 잡으면 기본으로 켜집니다.

AD·LDAP와 Web Proxy 연동

대부분 조직은 사용자·그룹을 Active Directory 같은 LDAP 서버 로 관리합니다. DLP Gateway를 AD에 연결하면 사용자와 그룹이 자동으로 My Organization 정의를 채우 고 사용자 검증에도 쓰입니다(Out of the Box). 이 연결은 마법사에서 지금 하거나 나중에 해도 됩니다.

HTTP·HTTPS 트래픽이 Web Proxy를 거쳐 나가는 환경 이라면, 그 트래픽을 검사하도록 게이트웨이를 따로 구성해야 합니다. 프록시가 DLP Gateway와 인터넷 사이 또는 DMZ에 있을 때, **Data Loss Prevention** > **Protocols** 에서 HTTP를 켜고 **Network Management** > **Proxy** 에서 프록시를 지정합니다. 프록시가 DMZ에 있으면 사용자망과 프록시 사이 HTTP 트래픽을 DLP로 검사 하는 것이 모범 사례입니다. 암호화된 HTTPS까지 보려면 HTTPS Inspection을 함께 켭니다. 절차가 길고 세부적인 부분은 원문을 참고하세요.

05 메일 서버와 Exchange 연동

메일 서버와 Exchange 연동

DLP가 가장 많이 다루는 채널이 이메일입니다. 이 장은 메일 서버를 Mail Relay로 세우는 일, 그리고 Exchange 내부 메일까지 검사하는 Exchange Security Agent 를 정리합니다.

동작 설정 다시 보기

이메일을 다루려면 규칙의 **Action** 을 먼저 떠올려야 합니다. **Detect**(통과·로그), **Inform User**(통과·로그·알림), **Ask User**(보낼지 사용자가 확인할 때까지 보류), **Prevent**(차단) 가 기본이고, 여기에 **Watermark**(나가는 Office 문서에 보이는/안 보이는 표식을 넣어 추적) 가 더해집니다. 이 가운데 Ask User와 알림 기능이 메일 서버를 필수 부품으로 만듭니다.

> 중 요
>
> Data Owner에게 알림을 보내도록 설정하는 순간 메일 서버는 DLP 시스템의 필수 구성요소 가 됩니다. 게이트웨이는 사용자·Data Owner에게 알림 메일을 보내야 하므로, 메일 서버에 클라이언트로 접근할 수 있어야 합니다.

Mail Relay 구성

메일 서버는 **Mail Relay 로 동작하도록** 설정해야 합니다. 그래야 Ask User 규칙에서 DLP가 붙들어 격리한 이메일을, 권한 있는 사용자나 관리자가 **Send**(릴리스) 로 풀어 보낼 수 있습니다. 또 메일 서버는 DLP Gateway로부터 오는 익명 SMTP 연결을 신뢰 하도록 구성하거나, 환경이 요구하면 인증된 SMTP 연결을 신뢰하도록 설정합니다. 가장 쉬운 방법은 Data Loss Prevention Wizard에서 Mail Relay를 지정하는 것이고, 마법사 없이 SmartDashboard의 DLP 탭에서 직접 설정할 수도 있습니다. 메일 서버가 Microsoft Exchange면 이 DLP Gateway를 향한 **SMTP Relay** 로 세웁니다.

Exchange Security Agent — 내부 메일까지

여기서 한 가지 한계를 알아야 합니다. Microsoft Exchange 클라이언트 간 내부 메일은 Exchange 전용 프로토콜 을 쓰는데, 이는 DLP Gateway가 직접 지원하지 않습니다. 그래서 내부 메일까지 검사하려면 Exchange 서버에 **Exchange Security Agent** 를 설치합니다. 이 에이전트는 내부 메일을 TLS로 암호화한 SMTP로 DLP Gateway에 넘겨 검사를 받게 합니다. 조직이 모든 메일을 Exchange로만 처리한다면, 이 구성으로 외부로 나가는 메일까지 함께 검사 할 수 있습니다.

에이전트는 트래픽을 넘기는 Exchange 서버마다 하나씩 설치 하고, SmartConsole에서 중앙 관리되며, 하나의 에이전트는 하나의 DLP Gateway에만 메일을 보낼 수 있습니다. 설정은 SmartConsole(정확히는 SmartDashboard의 DLP 탭 > **Gateways** > **Actions** > **New Exchange Agent** 마법사)과 Exchange 서버 양쪽에서 합니다. 마법사는 General 등 네 페이지로 에이전트 정보를 받는데, 구체적 입력 항목은 분량이 많으니 원문을 참고하세요. 에이전트를 활용한 내부 메일 검사 시나리오는 Out of the Box에서 이어집니다.

> 팁
>
> 에이전트 동작에 영향을 주는 세부 값들은 고급 설정의 Exchange Security Agent 값 편집에서 손볼 수 있습니다. 사건 로그를 별도 서버에 두는 Incident Log Handling 설정도 함께 검토하세요.

06 HTTPS Inspection 설정

HTTPS Inspection 설정

오늘날 웹 트래픽의 대부분은 SSL로 암호화돼 있어, 암호화된 채널은 게이트웨이가 들여다볼 수 없습니다. 데이터가 HTTPS로 새어 나가는 것을 막으려면 HTTPS Inspection이 필요합니다.

왜 필요한가

HTTPS는 SSL(Secure Sockets Layer)로 데이터의 기밀성과 무결성을 지키지만, 같은 암호화가 불법 활동과 악성 트래픽을 숨기는 통로 도 됩니다. 게이트웨이는 암호화된 트래픽을 그대로는 검사하지 못하므로, HTTPS Inspection을 켜 게이트웨이가 외부 사이트와 새 SSL 연결을 맺게 합니다. 그러면 게이트웨이가 트래픽을 복호화해 검사할 수 있습니다. 종류는 둘로, **Outbound**(내부 클라이언트가 외부로 보내는 트래픽 보호) 와 **Inbound**(인터넷에서 내부 서버로 오는 요청 보호) 입니다. DLP 입장에서는 데이터 유출을 잡는 Outbound가 핵심입니다.

> *HTTPS traffic has a possible security risk and can hide illegal user activity and malicious traffic. Security Gateways cannot inspect HTTPS traffic because it is encrypted.*
>
> — AdminGuide, "Configuring HTTPS Inspection" (p.67)

게이트웨이는 인증서를 써서 클라이언트와 보안 웹사이트 사이의 중개자 가 됩니다. 이때 다뤄지는 데이터는 HTTPS Inspection 로그에 보관되며, HTTPS Inspection 권한이 있는 관리자만 모든 필드를 볼 수 있어 사생활을 지킵니다.

검사 흐름 — Outbound

내부 클라이언트가 외부 서버로 HTTPS 요청을 보내면 흐름은 이렇습니다. 요청이 게이트웨이에 도착하면(①) 게이트웨이가 이를 검사하고(②), HTTPS Inspection 규칙에 걸리는지 판단 합니다(③). 규칙에 안 걸리면 페이로드는 검사하지 않고 그냥 보냅니다. 규칙에 걸리면 게이트웨이가 OCSP 표준으로 외부 서버의 인증서를 검증 하고(④), 그 연결을 위한 새 인증서를 만들어(⑤) 연결을 복호화한 뒤(⑥) 검사 합니다(⑦). 검사가 끝난 트래픽은 다시 암호화돼 목적지로 갑니다.

DLP와의 연결

HTTPS Inspection을 켜면 Web Proxy를 거치든 직접 나가든 HTTPS로 흐르는 데이터까지 DLP가 검사 할 수 있게 됩니다(설치와 배치의 Web Proxy 연동과 함께 봅니다). 새 DLP 프로파일에서 HTTPS Inspection이 켜져 있으면 관련 검사가 HTTPS 트래픽에도 적용되는 식으로, 두 기능은 서로 맞물려 동작합니다.

HTTPS Inspection은 DLP 전용 기능이 아니라 게이트웨이 전반에서 쓰는 공통 기능 입니다. 인증서 발급·신뢰 체계, HTTPS Inspection Rule Base 설계, 카테고리별 우회 정책 같은 세부는 분량이 크고 다른 가이드와 겹치므로, 깊은 설정은 Security Gateway 가이드와 Threat Prevention 가이드의 HTTPS Inspection 부분 및 원문을 함께 참고하세요. 인증서 관련 보조 설정은 고급 설정의 Server Certificates에서도 다룹니다.

07 UserCheck — 사용자와 대화하기

UserCheck — 사용자와 대화하기

UserCheck는 Check Point DLP의 색깔을 결정짓는 기능입니다. 위반이 일어났을 때 사용자에게 실시간으로 알리고, 처리를 사용자 손에 맡겨 관리자가 모든 전송을 일일이 검토하는 부담을 덜어 줍니다.

왜 UserCheck인가

UserCheck가 없으면 보안 담당자나 팀이 모든 이메일과 데이터 이동을 실시간으로 검토해 승인·거부 해야 합니다. 그래서 다른 제품들은 탐지에만 머무는데, 소개에서 봤듯 UserCheck는 결정을 사용자에게 분산 시킵니다. 사용자는 무엇이 걸렸는지와 그 사유를 보고, 그래도 보낼 거면 사유를 적어야 하며, 그 결정과 사유가 모두 로그로 남 습니다.
이렇게 쌓인 실제 사용 기록이 정책을 효과적인 차단 정책으로 다듬는 밑거름이 됩니다. 특히 대부분의 유출이 악의 없는 실수 인 만큼, 사용자가 그 순간 모범 사례를 배우는 것이 미래의 유출을 줄입니다.

UserCheck Interaction Object

규칙의 **Action** 셀에 넣어 사용자와 소통하는 도구가 **UserCheck Interaction Object** 입니다. 이 객체는 사용자가 위험한 결정을 내리지 않도록 돕고, 바뀌는 인터넷 정책을 실시간으로 알리는 데 쓰입니다. 기본 제공 객체로는 규칙이 **Ask** 일 때 떠 회사 정책을 알리고 OK를 눌러야 진행되게 하는 **Ask User** 객체, 차단을 알리는 **Blocked Message** 객체 등이 있습니다.

> 참 고
>
> UserCheck 상호작용 객체는 SmartDashboard에서만 만들고 편집 할 수 있습니다.
> SmartConsole에서는 생성·편집이 안 되니, DLP 탭의 **UserCheck** 페이지에서 다루세요.

UserCheck Client — 브라우저 밖까지

알림은 두 경로로 갑니다. 하나는 SMTP 트래픽에 대한 이메일 이고, 다른 하나는 **UserCheck Client** 의 시스템 트레이 팝업 입니다(SMTP·HTTP·FTP 등). 엔드포인트에 설치하는 UserCheck Client는 Skype·iTunes나 브라우저 애드온처럼 웹 브라우저가 아닌 애플리케이션 의 알림도 띄울 수 있고, 브라우저에 알림을 제대로 못 띄우는 경우 컴퓨터 자체에서 보여 줍니다. 사용자는 팝업에서 옵션을 골라 실시간으로 응답 하고, Ask User 사건이면 팝업의 **Send/Discard** 링크로 바로 처리합니다.

설치·연결의 큰 흐름은 게이트웨이 객체에서 UserCheck와 클라이언트를 켜고 → 통신·신뢰 방식을 구성하고 → 엔드포인트에 클라이언트를 설치하고 → 게이트웨이에 연결한 뒤 → 정책을 위반하는 간단한 동작으로 알림 수신을 확인 하는 순서입니다. 클라이언트 요구사항과 단계별 세부는 R82 Release Notes와 원문을 참고하세요.

> 주 의
>
> 사용자에게 UserCheck Client의 목적을 반드시 알려 두세요. 사용자가 클라이언트를 종료하면 Ask User 옵션을 제공하는 대체 웹 페이지가 제대로 동작하지 않을 수 있습니다.

DLP Self Incident-Handling Portal

UserCheck Client 외에, 사용자는 브라우저 기반의 **DLP Self Incident-Handling Portal** 로도 자신의 보류 사건을 처리할 수 있습니다(기본 URL `https://<DLP Gateway IP>/dlp`). 이 포털과 알림 메시지는 현지화·맞춤화 할 수 있어, 회사 로고와 안내 문구로 꾸밀 수 있습니다. 관리자는 권한이 있으면 SmartConsole의 **Logs & Events** > **Logs** 에서도 격리 사건을 Send/Discard 할 수 있습니다. 사용자 알림과 Data Owner 알림의 설계는 Data Owner와 사용자 알림에서 이어집니다.

08 Out of the Box — My Organization과 정책

Out of the Box — My Organization과 정책

DLP는 설치 첫날부터 쓸 만한 정책 으로 시작해 점차 다듬어 갑니다. 이 장은 그 출발점인 Out of the Box 환경, 내부·외부를 가르는 My Organization 정의, 그리고 정책과 사건 분석의 큰 틀을 잡습니다.

첫 단계 — 탐지부터 시작한다

DLP 환경의 첫 단계는 기본 제공 정책으로 자동 검사를 켜되, 규칙을 모두 **Detect** 로 두는 것입니다. Check Point 전문가 휴리스틱과 각종 규제 준수에 기반한 검사가 곧바로 돌지만, 사용자를 방해하지 않으면서 사용 양상을 관찰하고 우리 조직의 실제 필요를 파악 할 수 있습니다. 경험에 기반한 심각도 등급과 Logs & Events로 핵심 유출을 찾아내며, 이해가 쌓이면 차단(Prevent)으로 옮겨 갑니다(규칙 만들기).

SmartDashboard의 DLP 탭

DLP의 상세 설정은 **Security Policies** > **Shared Policies** > **DLP** 에서 **Open DLP Policy in SmartDashboard** 로 들어가는 DLP 탭에 모여 있습니다. 핵심 페이지는 **Policy**(규칙 베이스 관리), **Whitelist Policy**(절대 매칭하지 않을 파일), **Data Types**(보호 대상 데이터 정의), **Repositories**(지문·화이트리스트 저장소), **My Organization**(내부 환경 정의), **Gateways**(블레이드·Exchange Agent), **UserCheck** 입니다. 여기에 **Additional Settings** 의 Protocols·Mail Relay·Email Addresses·Watermarks·Advanced 와, 별도 탭의 HTTPS Inspection이 더해집니다.

My Organization — 내부와 외부 가르기

DLP의 모든 판단은 무엇이 내부이고 무엇이 외부인지 에서 출발합니다. **My Organization** 페이지가 바로 그 경계를 정합니다.

> *The My Organization page shows what DLP recognizes as data movement in the internal network (where data leakage is not an issue) and what is external (where data transmission must be monitored).*
>
> — AdminGuide, "Defining My Organization" (p.115)

기본적으로 My Organization은 DLP Gateway의 내부 인터페이스 뒤에 있는 모든 호스트·네트워크 와, Management Server에 정의된 특정 사용자·그룹·LDAP 그룹의 모든 사용자 를 포함합니다. 여기에 우리 이메일 도메인과 특정 주소 를 더하는데, 도메인을 넣을 때는 `@` 없이 `example.com` 형태로 적고, 그러면 하위 도메인까지 자동 포함 됩니다 (`jsmith@uk.example.com` 도 내부로 인정). SMTP는 도메인이 My Organization에 있고 보낸 IP도 내부 인터페이스/네트워크일 때 내부로 간주됩니다.

> 중 요
>
> 기본 도메인 정의를 지우지 마세요 . My Organization에는 도메인(이메일 주소 도메인 또는 LDAP Account Unit)이 반드시 하나는 있어야 하며, 없으면 DLP가 이메일을 아예 검사하지 않습니다. 또 클라우드 서버는 추가하지 마세요 — 데이터 통제권이 제3자에게 넘어가므로, 신뢰하기보다 클라우드를 오가는 민감 데이터를 모두 탐지하는 편이 안전합니다.

사용자·그룹은 보통 외부 LDAP(Active Directory)로 관리하지만, LDAP를 쓰지 않거나 LDAP에 없는 사용자를 정의해야 할 때는 DLP 탭에서 내부 사용자 계정을 직접 추가 할 수 있습니다.

사건 분석 — Logs & Events

정책이 잡은 사건은 **Logs & Events** > **Logs** > **Queries** > **DLP** 에서 봅니다. DLP 로그는 필터링하기 좋게 분류 돼 있고, **DLP Log Details** 창에서 사건을 읽기 쉬운 형태로 보며 Data Type이나 SmartConsole의 DLP 탭으로 바로 이동할 수 있습니다. 다듬고 싶거나 동작이 최선인지 의심스러운 사건·Data Type·규칙에는 **Follow Up 플래그** 를 달아 두면 나중에 모아 보기 편합니다. R80부터 SmartEvent의 분석 뷰가 Logs & Events에 통합돼, 필터·차트·통계로 사건을 분석할 수 있습니다.

> 권 장
>
> 대부분의 사건을 손으로 일일이 검토하지 마세요. 원본 전송(이메일·첨부 등)은 보낸 사람이나 Data Owner의 문의에 대비해 그대로 보관됩니다. 다만 개인 이메일·웹 게시가 캡처·저장·열람될 수 있다는 점을 사용자에게 반드시 알려 현지 사생활 법규 문제를 피하세요.

09 Data Owner와 사용자 알림

Data Owner와 사용자 알림

DLP를 사람 중심으로 돌아가게 하는 것이 Data Owner와 알림 체계 입니다. 데이터의 책임자가 자기 영역의 움직임을 직접 받아 보고, 사용자가 위반 순간 안내를 받아 스스로 처리하게 하는 구조를 정리합니다.

Data Owner 정의하기

Data Owner 는 관리자나 팀장처럼 특정 데이터를 책임지는 사람 입니다. 일반 사용자보다 큰 책임을 지며, 어떤 데이터를 보호하고 어떤 데이터는 밖으로 내보내도 되는지 를 관리자와 상의해야 합니다. 정의는 Data Type 단위로 합니다 — SmartDashboard의 DLP 탭에서 **Data Types** 의 한 항목을 열어 **Data Owners** 에서 책임질 사용자나 그룹을 추가 하고 정책을 설치합니다. 한 Data Type에 필요한 만큼 여러 Data Owner를 둘 수 있습니다.

이렇게 두면 Data Owner가 자기 데이터가 어떻게 움직이는지 적시에 자동 알림과 리포트로 받아 보게 됩니다. 이는 관리자를 관리자와 직원 사이의 난처한 위치 에서 벗어나게 해 주는 핵심 장치입니다 — 사용 문제를 데이터 책임자가 직접 다루기 때문입니다.

사용자·Data Owner와 연결하고 알리기

알림이 가려면 먼저 누구에게, 어떻게 닿을지 를 정해야 합니다. Data Owner·사용자와 연결하는 설정을 마치면, 위반이 일어날 때 Data Owner에게는 사건 통지가, 사용자에게는 위반 안내가 갑니다. 사용자 알림은 UserCheck에서 본 대로 이메일이나 UserCheck Client 팝업으로 전달되며, Ask User 규칙을 두고 관리하는 방식 으로 사용자가 보낼지 버릴지 직접 결정하게 합니다. 알림 문구는 현지화·맞춤화 할 수 있고, 사용자는 **DLP Self Incident-Handling Portal** 이나 이메일에 회신하는 방식 으로도 사건을 처리할 수 있습니다.

> 권 장
>
> DLP를 켜기 전에 회사 가이드라인 페이지를 준비 해 사용자가 데이터 전송·보호 규칙을 익히게 하세요. "DLP 규칙을 위반한 모든 이메일은 캡처되어 검토될 수 있다"고 알리는 것만으로도 대부분의 사생활 법규 요건을 충족합니다.

Corporate Guidelines 링크 걸기

준비한 회사 가이드라인 페이지는 DLP 알림에 링크로 넣을 수 있습니다. 게이트웨이에서 `$DLPDIR/config/dlp.conf` 를 열어 `corporate_info_link` 파라미터를 가이드라인 URL(`http://www.example.com` 형식)로 바꾸 고 저장한 뒤 정책을 설치하면, 사용자·Data Owner 알림에서 가이드라인으로 바로 갈 수 있습니다(고급 설정에도 관련 항목이 있습니다).

Learning Mode — 같은 흐름은 한 번만 묻기

사용자를 같은 일로 거듭 귀찮게 하지 않도록 **Learning Mode** 가 있습니다. **Additional Settings** > **Advanced** 의 **Learn User Actions** 에서 켜는데, 이메일은 한 스레드에 한 번 결정하면 그 스레드 전체에 적용 (기본 꺼짐, 켜면 Exchange 메일에도 적용), 웹은 한 게시에 대한 결정이 12시간 내 이어지는 게시에 적용 (기본 켜짐, HTTPS Inspection 켜면 HTTPS 게시에도 적용), FTP는 한 업로드 결정이 12시간 내 업로드에 적용 (기본 꺼짐)됩니다. 끄면 같은 흐름에서 매번 알림이 갑니다.

> 참 고
>
> 웹 위반에서 Learn User Actions를 끄면 UserCheck Portal의 Send·Discard 버튼이 비활성화되어 사용자는 포털을 닫을 수만 있고, 의심 데이터는 사이트에 게시되지 않습니다.

10 규칙 만들기 — 시나리오별 접근

규칙 만들기 — 시나리오별 접근

Out of the Box 정책으로 시작했다면, 이제 사건을 관찰하며 우리 조직에 맞는 규칙으로 다듬어 갈 차례입니다. 이 장은 정책을 발전시키는 단계와 규칙을 짜는 실제 방법을 정리합니다.

다듬어 가는 단계 — Analytical에서 Prevent로

DLP 정책은 한 번에 완성되지 않고 관찰 → 분석 → 차단 으로 무르익습니다. 휴리스틱 규칙이 잡은 사건을 감사하다 보면 조직의 필요가 보이는데, 이때 **Analytical Configuration** 단계로 넘어가 더 많은 Data Type을 정책에 더하고, 규칙을 **Ask User** 로 바꿉니다 . Ask User로 두면 사용자가 무엇이 허용되고 무엇이 안 되는지 배우 면서 자가 처리 결정과 사유를 남기고, 관리자는 Logs & Events에서 그 결정과 설명을 검토해 정확도를 끌어올립니다. 충분히 이해가 쌓이면 핵심 규칙을 **Prevent** 로 옮겨 본격 차단에 들어갑니다. High·Critical 심각도 규칙부터 감사하고, 사용자가 기대치를 이해하면 가장 먼저 Detect에서 Ask로 올리는 것이 좋습니다.

DLP 규칙의 구성요소

DLP 규칙은 Firewall 규칙과 비슷해 보여도 결이 다릅니다. Firewall 규칙이 주로 밖에서 안으로 들어오는 트래픽을 보는 반면, DLP 규칙은 안에서 밖으로 나가는 데이터를 보고, 프로토콜·사람보다 **Data Type** 이 규칙의 중심입니다. 한 규칙은 보호할 **Data Type**, 전송 **Source**(기본 My Organization), **Destination**(기본 Outside My Org), **Protocol**(기본 Any), **Exceptions**, **Action**, **Tracking**, **Severity**, Install On, Time, Category, Comment 으로 이뤄집니다.

> 주 의
>
> **Exceptions** 는 가장 먼저 매칭 됩니다. 데이터 전송이 예외에 걸리면 그 자리에서 절차가 멈추니, 예외를 둘 때는 신중해야 합니다.

규칙 만드는 법

규칙은 SmartDashboard의 DLP 탭 > **Policy** 에서 **New Rule** 로 만듭니다. 흥미롭게도 DLP 규칙은 순서가 중요하지 않 습니다 — 각 게이트웨이가 설치된 모든 규칙을 검사하기 때문입니다. **Data** 열에서 매칭할 Data Type을 고르는데, 한 규칙에 여러 Data Type을 넣으면 OR로 묶 여 하나만 걸려도 규칙이 매칭됩니다. **Source** 는 기본 My Organization을 두거나 특정 사용자·이메일·네트워크를 고르고, **Destination** 은 조직 밖을 보는 **Outside My Org** 를 두거나 특정 대상을 고릅니다.

여기서 **Outside Source** 와 **Outside My Org** 의 차이 가 중요합니다. Source가 My Organization의 일부(예: Network_A)일 때 **Outside Source** 는 그 Source 바깥 전부 를 뜻해 부서 간 규칙 을 만들 수 있고, **Outside My Org** 는 조직 전체의 바깥만 봅니다. 단 Outside Source를 쓰려면 게이트웨이가 데이터 처리 서버보다 앞에서 검사 해야 합니다(예: SMTP라면 메일 서버보다 먼저). 예컨대 재무 부서가 급여 정보를 다른 부서로 흘리지 못하게 하는 규칙이 이렇게 만들어집니다.

Action 열에서는 소개에서 본 Detect·Inform User·Ask User·Prevent와 Watermark를 고릅니다(Watermark와 정밀 조정). Identity Awareness를 켜면 access role 객체를 Source/Destination에 쓰고, FTP·HTTP 위반에도 이메일 알림을 보내며, 미인증 사용자를 Captive Portal로 보낼 수 있습니다(Identity Awareness 가이드). 규칙 세부 옵션은 분량이 크니 원문을 함께 보세요.

11 Data Type 정의하기

Data Type 정의하기

Data Type 은 DLP 규칙의 building block 이자 정책의 토대입니다. 무엇을 지킬지를 Data Type 이 규정하므로, DLP를 잘 쓰려면 결국 규칙보다 Data Type에 집중 해야 합니다.

> *The data types are the building blocks of the Data Loss Prevention rule base, and the basis of the DLP policy that you install on DLP Gateways - the basis of DLP functionality. Each data type specifies a data asset to protect.*
>
> — AdminGuide, "Adding Data Types to Rules" (p.221)

어디서부터 시작하나

가장 좋은 출발점은 경험으로 이미 아는 명백한 데이터 입니다. 소스 코드, 직원 연락처, 비밀번호, 가격표처럼 "이건 밖으로 나가면 안 된다"가 분명한 것부터 잡고, 그다음 Data Owner와 상의해 조직의 기밀·무결성 절차에 맞는 복잡한 Data Type으로 넓혀 갑니다. Data Type은 카테고리별로 정렬 되는데, 그중 **Compliance** 카테고리가 중요합니다 — PCI 기준상 고객 신용카드 번호를 평문으로 외부에 보내선 안 되는 것처럼, 규제 기준을 그대로 강제하는 기본 제공 Data Type이 여기 모여 있습니다. Data Type을 만들면 규칙에 넣고 정책을 설치합니다.

Data Type Wizard — 다섯 가지 식별 방식

새 Data Type은 **Data Type Wizard** 로 만드는 것이 가장 좋습니다(DLP 탭 > **Data Types** > **New**). 마법사는 트래픽 종류를 고르고, 식별 방식을 정의 하는 식으로 진행됩니다. 대표적인 다섯 방식을 보면 다음과 같습니다.

Keywords 는 키워드 목록을 데이터와 대조 합니다. ALL(모두 일치)·ANY(하나면 충분)·특정 개수(Threshold) 중 매칭 기준을 고르는데, Threshold가 높을수록 결과가 정밀 해집니다. 예컨대 위원회 의원 이름이 한 이메일에 모두 들어 있어야 의심스럽다면 "모든 단어 일치"로 둡니다.

Pattern 은 정규식으로 콘텐츠를 매칭 합니다(참고의 정규식 문법). 패턴이 한 번이라도 걸리면, 또는 정해진 횟수까지 허용하다 그 이상이면 매칭하도록 설정할 수 있습니다 — 다섯 개 제품의 전체 가격표를 잡으려면 가격 패턴의 발생 횟수를 5로 두는 식입니다.

Template 은 사내 문서 템플릿을 기준으로 문서를 보호 합니다. 법원 명령서처럼 헤더·푸터·서식이 같은 문서를 잡을 때 쓰며, Similarity 슬라이더로 얼마나 닮아야 매칭할지 정합니다.

> 권 장
>
> Similarity 슬라이더는 처음엔 낮게 두세요. 높을수록 덜 잡힙니다. 슬라이더를 활용한 단계별 정책도 효과적입니다 — 같은 템플릿으로 10%는 Detect, 50%는 Ask User, 90%는 Prevent 규칙 을 만들면, 닮은 정도에 따라 다른 동작을 줄 수 있습니다.

> 중 요
>
> 템플릿에 이미지가 들어가면 파일 형식이 일치해야 합니다. 템플릿은 JPG인데 사용자 문서는 GIF면 규칙이 동작하지 않습니다.

Fingerprint 는 앞의 방식들과 결이 다릅니다. 데이터를 묘사하는 게 아니라, 파일마다 고유한 서명(지문)으로 식별 합니다. **Repository**(조직 밖으로 나가면 안 되는 파일들이 있는 네트워크 위치)를 지정하면 DLP가 그 파일들의 지문을 만들고, 게이트웨이를 지나는 파일의 지문을 저장소의 지문과 대조 해 일치하면 차단합니다. 마지막으로 **Compound Data Type**

은 여러 Data Type을 조합해 더 정밀하게 식별합니다(MultiSpect). 완전 맞춤형이 필요하면 CPcode 로 매칭 로직을 직접 짤 수도 있습니다.

Repository — 지문의 원천

Repository 는 문서 저장에 쓰이는 네트워크 위치 로 두 종류입니다. **Fingerprint Repository** 는 나가면 안 되는 문서 를 담아 지문 Data Type의 원천이 되고(지문 Data Type을 만들면 자동 생성), **Whitelist Repository** 는 나가도 되는 문서 를 담습니다. 저장소 파일은 계속 바뀌므로 기본적으로 매일 자동 스캔 되며(CIFS·NFS 지원), 변경 없는 파일은 건너뛰어 재스캔이 빠릅니다. 큰 저장소는 기밀 폴더만 지정하거나 특정 Data Type에 맞는 파일만 스캔 해 효율을 높입니다(예: spreadsheet 파일만). 전체 파일이 나가지 않아도 일부 구간만 복사돼 새는 것을 잡으려면 **부분 일치** 를 켜는데, 텍스트 구간의 비율 또는 일치 구간 개수로 매칭을 판단합니다.

Whitelist Policy — 절대 매칭하지 않을 파일

반대로 DLP가 절대 건드리지 않아야 할 파일 은 **Whitelist Policy** 로 지정합니다. 두 방법이 있는데, SmartConsole의 Whitelist Policy 창에 직접 추가 (파일 수가 적을 때 권장)하거나 네트워크의 Whitelist Repository에 두는 것입니다. 화이트리스트에서 제외되려면 파일이 목록의 파일과 정확히 동일 해야 합니다. 만든 Data Type을 규칙에 넣는 구체적 절차와 카테고리별 목록은 분량이 크니 원문을 참고하세요.

12 Watermark와 정밀 조정

Watermark와 정밀 조정

정책의 뼈대를 세웠다면, 이제 추적용 Watermark를 입히고, Source·Destination·Protocol을 세밀하게 손보는 단계입니다. 이 장은 정책을 우리 환경에 딱 맞게 조이는 도구들을 모았습니다.

Watermark — 나가는 문서에 표식 남기기

Watermark 는 규칙의 한 Action으로, 나가는 Microsoft Office 문서에 보이는 표식이나 보이지 않는 암호화 텍스트를 넣어 추적 합니다. 대상은 Office Open XML 형식인 DOCX·PPTX·XLSX 뿐입니다. 적용은 Policy에서 해당 Data Type의 Action 셀을 우클릭해 Ask·Inform User·Detect 같은 제한적 Action을 고른 뒤 Watermark 프로파일을 선택 합니다. 기본 프로파일은 셋으로, **Classified**(페이지 가운데 "Classified"), **Invisible only**(숨김 텍스트만), **Restricted**(아래쪽 "Restricted" + 발신자·수신자·발송일 필드) 입니다.

> 중 요
>
> 구형 형식(DOC·PPT·XLS)은 워터마크를 넣을 수 없 습니다. 확장자만 docx로 바꿔도 대상이 되지 않습니다. 또 Data Type이 문서 안이 아니라 이메일 본문에서만 발견되면 문서에 워터마크가 찍히지 않 습니다 — 예컨대 신용카드 번호가 첨부 문서가 아니라 메일 본문에 있으면 문서는 워터마킹되지 않습니다. 표식은 Data Type이 문서 안에 있을 때만 들어갑니다.

Source·Destination 정밀 조정

규칙의 기본값인 Source(My Organization)와 Destination(Outside My Org)은 SmartConsole에 정의된 어떤 네트워크 객체·사용자·그룹으로든 바꿀 수 있습니다. 사적 메일을 막으려고 Gmail·Hotmail 같은 특정 도메인을 목적지로 두려면, Object Explorer에서 **New** > **Network Object** > **More** > **Domain** 으로 도메인 객체를 만들어 씁니다(FQDN 체크는 해제).

규칙 만들기에서 본 **Outside Source** 와 **Outside of My Org** 의 차이 를 여기서 활용합니다. Source를 특정 사용자·그룹·호스트·네트워크·VPN으로 두고 Destination을 **Outside** 로 하면 그 그룹에 한정된 부서별 규칙 이 만들어집니다. 재무 부서가 급여 정보를 다른 부서로 흘리지 못하게 하거나, 두 그룹 사이 데이터 이동을 통제하는 규칙이 이렇게 나옵니다. 단 Outside Source는 게이트웨이가 데이터 처리 서버 앞에서 검사 할 때만 쓸 수 있습니다.

Protocol 지정 — 성능과의 균형

각 규칙은 검사할 **Protocol** 을 갖는데, 기본은 Any(켜진 모든 프로토콜 검사) 입니다. 지원 프로토콜은 전체 차원, 게이트웨이별, 규칙별 세 수준에서 조절합니다. 예컨대 성능이 문제가 되면 **Additional Settings** > **Protocols** 에서 HTTP 체크만 해제 해, 정책을 건드리지 않고도 HTTP 게시와 웹메일을 DLP 검사 없이 통과시킬 수 있습니다. 게이트웨이별로는 그 게이트웨이의 Data Loss Prevention 페이지에서 **Apply the DLP policy to these protocols only** 로 정합니다.

성능과 관련해, 극단적 상황에서 연결을 우선하도록 **Extreme Conditions** 를 둘 수 있습니다 — CPU 부하가 high watermark를 넘거나, 내부 오류·과도한 메시지 크기·큰 첨부·깊은 압축 같은 조건 에서 SMTP·FTP·HTTP 검사를 우회합니다. 기본값은 고급 설정에서 바꿀 수 있습니다. 그 밖에 SMTP·FTP·HTTP 할당량(Quota), 알림 맞춤화 등 세부 조정 항목도 고급 설정 장에서 이어집니다.

13 고급 설정

고급 설정

기본 정책이 자리 잡은 뒤 손보게 되는 세부 운영 항목들 을 모았습니다. 대부분 자주 건드리지 않는 설정이라, 여기서는 어떤 것이 있고 어디서 다루는지를 잡고 구체적 절차는 원문을 참고하면 됩니다.

게이트웨이 접근과 방화벽 정책

배치에 따라 게이트웨이 접근을 정리해야 합니다. Integrated DLP Gateway에서는 사용자가 DLP Portal·UserCheck에 닿을 수 있도록 접근을 구성 하고, Dedicated DLP Gateway에서는 전용 게이트웨이를 보호할 내부 방화벽 정책 을 둡니다. Dedicated는 보호용 게이트웨이 뒤에 두고 DLP Blade만 켜는 것이 권장이므로(설치와 배치), 이 게이트웨이 자체로 향하는 트래픽만 별도로 다룹니다.

보관 데이터 관리 — 만료와 정리

UserCheck 사건의 완전한 원본 데이터는 게이트웨이의 격리(quarantine)에 보관 됩니다. 큰 첨부가 걸리면 처리되거나 만료될 때까지 게이트웨이 공간을 차지하므로, 만료 데이터는 자동으로 정리 됩니다. 보관 일수·점검 주기는 게이트웨이의 `$FWDIR/conf/mail_security_config` 파일에서 `expiration_interval` (분 단위, 기본 1440 = 하루) 등으로 조절하고, `backend:expiration:db` 일수 가 지난 사건 데이터가 삭제됩니다. 사건이 만료되지 않으면 같은 파일의 `expiration_active=1` 로 만료 기능이 켜져 있는지 부터 확인합니다(메일 서버가 가득 차는 문제도 여기서 비롯됩니다).

할당량·알림·기타 임계값

운영 중 부하나 사용자 경험을 다듬는 항목이 여럿입니다. Advanced SMTP/FTP/HTTP Quotas 로 프로토콜별 처리 한도를, Advanced User Notifications와 DLP User-Related Notifications 맞춤화 로 사용자에게 가는 알림 문구를, Extreme Condition Values 편집 으로 Watermark와 정밀 조정에서 본 우회 임계값을 손봅니다. 그 밖에 UTF-8 LDAP 레코드 지원, Corporate Guidelines 링크(Data Owner와 알림), Exchange Security Agent 값 편집, 모든 포트에서의 HTTP 검사 같은 세부 항목이 있습니다.

새 File Type 정의하기

File Attributes Data Type은 여러 파일 형식 계열을 다루는데, 목록에 없는 새 file type을 추가 할 수도 있습니다. 다만 이는 SmartConsole이 아니라 **Database Tool(GuiDBEdit)** 로 직접 객체를 만드는 작업입니다 — SmartConsole 연결을 모두 닫고, `Other > dlp_data_tbl` 아래에 `file_type` 객체를 `file_type_<ID>` 이름으로 만들어 `visual_string` 에 이름을 적고 저장한 뒤 정책을 설치합니다. ID 목록과 지원 형식은 원문 표를 참고하세요.

인증서·Kerberos SSO

DLP Portal과 HTTPS Inspection(HTTPS Inspection)은 인증서를 씁니다. **Server Certificates** 로 포털·검사용 인증서를 다루고, **Kerberos Single Sign On** 으로 사용자가 다시 로그인하지 않고 DLP Portal에 접근하게 할 수 있습니다(Kerberos는 Active Directory의 인증 서버). 이들 설정은 분량과 환경 의존도가 커서, 단계별 절차는 원문과 Identity Awareness 가이드를 함께 보는 것이 좋습니다.

> 팁
>
> 고급 설정은 대부분 문제를 겪거나 특수 요구가 있을 때만 손대면 됩니다. 평상시 운영은 Out of the Box와 규칙 만들기의 흐름으로 충분합니다. 게이트웨이 측 진단·커널 디버그가 필요하면 R82 Quantum Security Gateway 가이드를 참고하세요.

14 참고 — 정규식·문자셋·CLI

참고 — 정규식·문자셋·CLI

마지막 장은 Data Type을 만들 때 쓰는 정규식 문법, 지원 문자셋, 그리고 게이트웨이에서 DLP 엔진을 제어하는 CLI 를 모은 참고 자료입니다. 필요할 때 찾아보는 용도로 가볍게 정리합니다.

정규식 — Pattern Data Type의 문법

Data Type 정의하기의 **Pattern** 방식은 정규식으로 콘텐츠를 매칭하는데, Check Point는 표준 메타문자를 다음과 같이 구현합니다. `\` (이스케이프), `[ ]` (문자 클래스), `( )` (서브패턴), `{n}` · `{n,m}` · `{n,}` (개수 한정), `.` (임의 문자), `?` (0~1회), `*` (0회 이상), `+` (1회 이상), `|` (택일), `^` · `$` (버퍼 시작·끝 고정), `-` (클래스 내 범위) 가 핵심입니다. 줄바꿈·탭 같은 Non-Printable Characters 와 숫자·문자 부류를 가리키는 Character Types 도 별도로 지원하며, 정확한 표는 원문을 보세요. 패턴을 만들 때는 반드시 Check Point가 지원하는 정규식 문법 을 써야 한다는 점만 기억하면 됩니다.

지원 문자셋

DLP는 다양한 언어의 데이터를 다루므로 폭넓은 Supported Character Sets 를 지원합니다. 한국어를 포함한 다국어 환경에서 키워드·패턴이 제대로 매칭되려면 해당 문자셋이 지원 목록에 있어야 하니, 비라틴 문자를 다룰 때 원문의 문자셋 목록을 확인하세요. LDAP 레코드가 UTF-8인 경우의 지원은 고급 설정에서 따로 다룹니다.

CLI — dlpcmd

게이트웨이에서 DLP 엔진을 직접 제어하는 명령이 **dlpcmd** 입니다. CLI 문법 표기에서 화살표(→)는 중첩된 하위 명령 을, 대괄호는 선택 항목 을 뜻합니다. 자세한 전체 CLI는 R82 CLI Reference Guide에 있고, 여기서는 dlpcmd의 핵심만 봅니다.

dlpcmd는 격리된 이메일을 관리하고 DLP RAM Disk를 제어 합니다. 격리 메일은 공개 GUID로 보내거나(action_by_admin 1) 삭제(action_by_admin 2) 하며, 이때 GUID는 반드시 중괄호 `{}` 로 감 싸고, 동작은 SmartConsole의 Audit 로그에 남습니다(sk117753). 현황은 `getquarantined` (목록), `getquarantinedcount` (개수), `getquarantinedsize` (총 크기) 로 확인합니다.

```
[Expert@MyGW:0]# dlpcmd getquarantined
[Expert@MyGW:0]# dlpcmd action_by_admin 1 {8698E6EC-340C-9115-0AB6-F6CA998614
```

`ramdisk` 하위 명령으로는 DLP RAM Disk를 on/off 하거나 크기(MB)를 정하고 status로 정보를 확인 합니다.

> 중 요
>
> Cluster에서는 모든 멤버를 똑같이 구성 해야 하고, Maestro·Chassis 같은 Scalable Platform에서는 해당 Security Group의 Expert 모드에서 명령을 실행합니다. 또 status 를 뺀 모든 ramdisk 작업은 전체 서비스 재시작(cpstop·cpstart) 이 필요합니다.

게이트웨이 측 Kernel Parameter 작업과 Kernel Debug는 이 가이드 범위를 넘어가니, R82 Quantum Security Gateway 가이드를 참고하세요. 핵심 용어가 헷갈리면 용어 정리로 돌아가면 됩니다.