



● 기업 전산 담당자를 위한 실행 매뉴얼

랜섬웨어 실전 방어 가이드

관리자 계정에서 탐지·격리 백업·복구까지
현장에서 점검하고 실행하는 7개 방어선

 이 전자책은 무료로 자유롭게 공유하셔도 됩니다

ROCKGATE
CORE

(rockgatecore.com / dfortress.kr)

제작·배포: (주)락게이트코어

이 가이드에 대하여

이 가이드는 기업 전산 담당자가 랜섬웨어 방어 상태를 직접 점검하고 개선할 수 있도록 만든 제품 중립적 실행 매뉴얼입니다. 관리자 계정 보호에서 시작해 외부 통로 차단, 서버 경화, 네트워크 분리, 탐지, 백업 전략, 사고 대응과 자가진단까지 다룹니다.

대상 독자는 명확합니다. **기업 IT 담당자 및 사이버보안 담당자**입니다. 그래서 모든 조치는 "별도 장비를 사야만 되는 것"과 "지금 그룹 정책(GPO)이나 방화벽 설정만으로 오늘 바로 시작할 수 있는 것"을 구분해서 담았습니다. 이미 랜섬웨어 피해를 겪고 재발을 막으려는 분에게도, 아직 겪지 않았지만 미리 대비하려는 분에게도 똑같이 쓸모 있도록 구성했습니다.

각 장은 같은 순서로 반복됩니다 — **왜 위험한가(실제 사건·통계) → 어떻게 막는가(실전 조치) → 지금 확인할 체크리스트 → 자주 묻는 질문**. 처음부터 순서대로 읽으셔도 좋고, 지금 가장 급한 장부터 골라 읽으셔도 무방합니다.

오늘 적용

계획 필요

인프라 필요

각 조치의 적용 수준을 위 세 단계로 표시합니다. '오늘 적용'은 기존 관리 도구로 시작할 수 있는 항목, '계획 필요'는 영향도 시험과 변경 승인이 필요한 항목, '인프라 필요'는 별도 플랫폼·구조 또는 외부 서비스가 필요한 항목입니다.

 **자유롭게 공유해 주세요.** 이 전자책은 판매용이 아니라 정보 공유를 위해 만들어졌습니다. 동료, 커뮤니티, 회사 내부 교육 자료로 자유롭게 전달·재배포하셔도 됩니다. 다만 내용을 유료로 재판매하거나 원문을 왜곡해서 사용하는 것은 삼가 주세요. 재배포 시 출처는 **(주)락게이트코어 (dfortress.kr)**로 표기해 주세요. 본문 중 소개하는 통계와 사건 사례는 함께 표시된 원출처를 확인해 주세요.

목차

1. 2026년 랜섬웨어는 이렇게 달라졌다

지금 누가, 왜, 어떻게 노리는가 — 위협조직 지형도

2. 관리자 계정이 뚫리면 다 끝나는 이유

MFA·Credential Guard로 첫 관문 지키기

3. RDP, 열어두셨나요?

외부 통로 차단 4중 방어

4. 리눅스 서버는 안전하다는 착각

SSH·ESXi 경화와 패치 속도

5. 망을 나누면 확산을 막을 수 있다

네트워크 분리와 제로트러스트 백업

6. 백업이 있어도 뚫리는 이유

3-2-1-1-0 백업과 감염 초기 대응 절차

7. 5개 방어선 자가진단

우리 조직은 지금 몇 점일까요

8. [보너스] 관리자 PC 보안 강화 체크리스트

공격받는 서버보다 먼저, 내 컴퓨터부터

9. [제작사 소개] D-FORTRESS

이 가이드를 만든 (주)락게이트코어의 하드웨어 백업 보안 제품

시리즈 한눈에 보기

회차	방어선	핵심 조치
①	위협 지형도	Qilin-Akira 등 위협조직 침투 경로 파악
②	신원과 접근 통제	MFA(가능하면 FIDO2), Credential Guard·LSA 보호 켜짐 확인, WDigest 꺼짐 확인
③	외부 통로 차단	NLA, IP 화이트리스트, VPN 의무화, 계정 잠금
④	시스템 경화	SSH root 로그인 차단, chattr +i, 빠른 패치
⑤	격리된 복구 체계 ①	네트워크 분리(User/Server/Backup), AD 도메인 미조인
⑥	탐지·격리된 복구 체계	고위험 행위 경보, 3-2-1-1-0 백업, 감염 초기 대응 절차
⑦	조직 준비도	5개 방어선 자가진단, 정기 복구 훈련

① 2026년 랜섬웨어는 이렇게 달라졌다

랜섬웨어는 운영 서버뿐 아니라 백업과 관리 계정까지 함께 노립니다. 주요 공격 경로와 최근 위협 흐름을 방어 관점에서 정리했습니다.



랜섬웨어 공격자는 운영 서버를 암호화하는 데서 그치지 않고 백업 저장소와 관리 계정까지 노립니다. 따라서 백업의 존재만 확인할 것이 아니라 운영 환경과 권한이 분리됐는지, 실제 복구가 가능한지까지 검증해야 합니다.

1. 지금 랜섬웨어가 노리는 진짜 약점

요즘 랜섬웨어 조직들이 공통적으로 노리는 지점은 세 가지로 정리됩니다.

첫째, **초기 침투 방식이 다양해졌습니다**. AI로 만든 정교한 사칭 메일, 패치되지 않은 VPN 취약점, SaaS 서비스 자격 증명 탈취까지 여러 경로를 동시에 두드립니다.

둘째, **공격 범위가 Windows 서버에만 머물지 않습니다**. Linux 서버와 VMware ESXi 같은 가상화 인프라까지 한 번에 노려서, 회사 전체 시스템이 동시에 마비되는 경우가 늘고 있습니다.

셋째, 가장 중요한 부분인데, **백업 저장소**를 첫 번째 표적으로 삼습니다. 운영 서버를 암호화하기 전에 백업부터 찾아서 무력화해야, 회사가 몸값 협상 테이블에 앉을 수밖에 없다는 걸 공격자들도 잘 알고 있는 것입니다.

공급망 공격에서는 조직이 사용하는 IT 유지보수업체나 원격관리 도구가 침투 경로가 될 수 있습니다. 외주 계정에도 MFA·최소 권한·접속 시간 제한을 적용하고, 유지보수 접속과 변경 이력을 중앙에서 감사해야 합니다.

2. 지금 가장 활발한 랜섬웨어 해킹그룹은 누구인가



위협조직 지형도는 빠르게 바뀌고 있습니다. 2025년까지 가장 활발했던 조직 중 하나였던 랜섬허브(RansomHub)는 2025년 4월 인프라가 갑자기 통째로 사라졌습니다. 이렇게 한 조직이 사라져도 그 소속 해커들은 없어지지 않고 다른 조직으로 옮겨가는데, 이때 대거 흡수한 곳이 바로 킬린(Qilin)입니다.

그 결과 킬린은 2026년 들어 전 세계에서 가장 활발한 랜섬웨어형 서비스(RaaS)로 올라섰고, 한국에서도 제조업체를 잇달아 공격했습니다.

2위는 아키라(Akira)로, VMware ESXi 등 가상화 인프라를 집중적으로 노리고 패치되지 않은 VPN 취약점을 뚫고 들어오는 방식을 주로 씁니다.

록빗(LockBit)은 예전만큼의 단독 위세는 줄었지만, 2025년 9월 드래곤포스(DragonForce)가 제안한 연합에 합류하면서 여러 조직이 공격 기술과 인프라를 공유하는 '카르텔' 형태로 다시 세력을 키우고 있습니다. 조직 간 경계가 흐려지고 기술이 공유되면서, 신생 조직도 순식간에 대형 조직 수준의 공격력을 갖추는 경우가 늘고 있습니다.

3. 왜 하필 지금 이렇게 심해졌나



이런 흐름의 배경에는 두 가지가 있습니다. 하나는 공격 기술의 상향 평준화입니다. 카르텔처럼 조직끼리 기술과 표적 정보를 공유하다 보니, 예전이라면 몇 년에 걸쳐 쌓았을 노하우를 신생 조직도 빠르게 흡수합니다. 다른 하나는 방어 쪽의 착시입니다. 많은 기업이 "백업을 하고 있으니 괜찮다"고 생각하지만, 정작 그 백업이 운영망과 같은 네트워크에 물려 있거나 관리자 계정으로 접근 가능한 상태라면, 공격자 입장에서는 원본과 백업을 한 번에 처리할 수 있는 손쉬운 표적일 뿐입니다.

4. 국내에서는 실제로 어떤 사고가 있었나 — 유형별로 보면

추상적인 통계보다 실제 사고 흐름을 보면 방어 우선순위가 더 명확해집니다. 2025년 한 해 국내에서 신고된 주요 침해사고를 유형별로 나눠보면, 업종은 다르지만 뚫린 지점은 몇 가지로 좁혀집니다. 아래는 실제로 피해가 확인된 사고를 업종만 남기고 유형별로 재구성한 것입니다.

① **웹서버 취약점 경유형** — 전자상거래 업종에서는 웹 서버에 웹셸(관리자 권한을 원격에서 실행할 수 있게 해주는 악성 스크립트)이 설치된 뒤 랜섬웨어가 전사 시스템으로 퍼져 수일간 서비스가 마비된 사고가 있었습니다. 금융보증 업종에서도 비슷한 경로로 랜섬웨어가 유입돼 나흘간 핵심 업무가 멈췄습니다. **근본 원인**은 웹 애플리케이션 패치 지연과, 웹서버가 뚫렸을 때 내부망으로 곧바로 확산되는 걸 막을 세그멘테이션이 없었다는 점입니다. **재발 방지**는 웹셸 탐지 체계와 정기 취약점 점검 주기 단축, 그리고 웹서버와 내부 업무망 사이의 망분리(6화 참고)입니다.

② **임직원 개인 계정 경유형** — 보안 전문 업체 한 곳은 임직원의 개인 이메일 계정이 먼저 유출되면서, 그 계정과 연결된 접근 경로를 통해 내부 자료가 빠져나가 신종 랜섬웨어 조직에 의해 거래 고객사 정보까지 함께 노출된 사고를 겪었습니다. **근본 원인**은 업무 시스템 인증이 개인 계정과 완전히 분리되지 않았고, 계정 탈취 이후의 이상 로그인을 탐지할 체계가 없었다는 점입니다. **재발 방지**는 업무 시스템에 개인 이메일 계정 연동을 금지하고, 2화에서 다룬 MFA를 전 임직원 계정에 예외 없이 적용하는 것입니다.

③ **협력사·공급망 경유형** — 앞서 소개한 미드나이트·엔드포인트 사례처럼, 회사 자체 보안은 문제가 없어도 IT 유지보수업체 같은 협력사 한 곳이 뚫리면 그 업체가 관리하는 고객사 여러 곳이 동시에 감염되는 경우입니다. **근본 원인**은 협력사의 보안 수준을 점검·요구할 절차 자체가 없었다는 점입니다. **재발 방지**는 외주·협력사 계약 시 최소한의 보안 요건(MFA, 접근 로그 보관)을 명시하고, 협력사 계정에도 우리 회사 계정과 동일한 접근 통제를 적용하는 것입니다.

④ **가용성 중시 업종 표적형** — 의료처럼 서비스 중단의 영향이 큰 조직은 복구 압박이 큼니다. 의료기기·레거시 시스템 때문에 패치와 망분리가 어렵더라도 의료기기망과 일반 업무망을 분리하고, 필수 시스템의 복구 우선순위와 절차를 미리 시험해야 합니다.

위 유형을 관통하는 공통점은 계정 관리, 로그 기록, 권한 통제 같은 운영 기본기의 실패입니다. 조직 규모와 무관하게 인터넷 노출 자산과 외주 접속 경로를 파악하고 통제해야 합니다.



공통점: 기술이 아니라 "운영"이 뚫렸다 — 계정관리·로그·권한통제

2025년 국내 주요 랜섬웨어 사고 유형 × 근본원인·재발방지

✓ 지금 바로 확인해 볼 체크리스트

- 회사의 백업 서버가 운영 서버와 같은 관리자 계정으로 접근 가능한 상태는 아닌지 확인해 보세요
- 서버 관리자 계정 로그인에 다중 인증(MFA)이 걸려 있는지 확인해 보세요
- RDP(원격 데스크톱) 포트가 외부 인터넷에 그대로 노출돼 있지는 않은지 확인해 보세요
- Windows 서버뿐 아니라 Linux·가상화(ESXi)·NAS(시놀로지·QNAP 등)도 같은 수준으로 점검하고 있는지 확인해 보세요
- 백업이 최소 한 곳이라도 네트워크와 완전히 분리된(에어갭) 형태로 존재하는지 확인해 보세요
- 견적 문의·입사 지원·컨설팅 요청으로 위장한 이메일 첨부파일을, 특히 외주·유지보수업체를 통해 받았을 때 발신자를 재확인하지 않고 바로 여는 습관은 없는지 점검해 보세요

Q. 이 연재는 어떤 순서로 진행되나요?

관리자 계정 보호, 외부 통로(RDP) 차단, 리눅스·가상화·NAS 서버 보안, 네트워크 분리와 백업 전략, 그리고 실제 감염 시 대응 순서까지 실무자가 바로 따라 할 수 있는 순서로 이어집니다.

Q. 중소기업도 이런 조치를 적용할 수 있나요?

네, 오히려 그런 회사를 염두에 두고 구성했습니다. 한 번에 모든 걸 갖추긴 어렵더라도, 매 회 소개하는 항목을 하나씩만 적용해도 실질적인 방어력이 쌓입니다.

랜섬웨어 조직의 이름과 수법은 계속 바뀌지만, 이들이 결국 노리는 지점은 크게 다르지 않습니다. 관리자 계정, 외부에 열린 통로, 그리고 운영망과 분리되지 않은 백업입니다. 다음 장부터 이 세 가지를 하나씩 실제로 막는 방법을 다룹니다.

관리자 권한 침해가 백업 관리 영역까지 번지지 않도록 운영 계정·관리 인터페이스·저장소 권한을 분리하고, 오프라인 또는 불변 사본을 별도로 유지해야 합니다.

② 관리자 계정이 뚫리면 다 끝나는 이유

관리자 계정이 탈취되면 공격자가 보안 설정을 변경하고 백업 관리 영역까지 이동할 위험이 크게 커집니다. MFA 도입과 자격 증명 탈취 차단 설정으로 첫 관문부터 지키는 방법을 정리했습니다.

랜섬웨어 예방의 핵심: 관리자 계정 사수 가이드

1. MFA 도입 및 업그레이드



OTP는 기본, 피싱 방지
FIDO2 보안키 권장

2. 윈도우 서버 보안 설정



Credential Guard
활성화 (가상화 격리)

디버깅 권한 정리

WDigest 비활성화
(평문 비밀번호 차단)

LSA 보호 활성화
(자격 증명 파기)

3. 직원 보안 교육 강화



IT 지원팀 사칭 등 별도
별, 채널 재확인 절차 수립

오늘 바로 시작하는 관리자 계정 보안 강화

1장에서는 2026년 랜섬웨어가 어떻게 진화했는지, Akira·Qilin·RansomHub 같은 위협조직이 어떤 경로로 침투하는지 살펴보았습니다. 이번 장에서는 그 침투 경로 중에서도 가장 치명적인 관문, 바로 '관리자 계정'을 지키는 방법을 다룹니다.

서버 접속(RDP)이나 VPN에 쓰는 관리자 계정이 탈취되면 공격자가 보안 설정을 바꾸고 백업 관리 영역으로 이동할 위험이 크게 증가합니다. 관리자 계정은 업무용 계정과 분리하고 접근 경로와 사용 시간을 제한해야 합니다.

관리자 계정 하나가 왜 전체 시스템을 무너뜨릴까요

관리자 계정이 뚫리면 해커는 서버 내부를 자유롭게 돌아다니면서 백업 서버까지 손댈 수 있는 최고 권한을 손에 넣게 됩니다. 그래서 가장 먼저 막아야 할 건 패스워드가 유출되더라도 OTP 같은 추가 인증 없이는 접근 자체가 불가능하게 만드는 다중 인증(MFA)입니다. 여기에 더해 윈도우 서버라면 자격 증명 탈취 도구(Mimikatz류)를 무력화하는 설정도 함께 챙겨야 하는데, 자격 증명을 가상화된 별도 공간에 격리하는 **Credential Guard**가 켜져 있는지(최신 Windows 11 Enterprise-Server 2025는 기본 켜짐, 이전 버전은 수동 활성화 필요), 레거시 호환을 위해 되살려진 경우가 있는 **WDigest**(메모리에 평문 비밀번호를 남기는 옛 인증 방식)가 꺼져 있는지, LSASS 프로세스를 보호 프로세스로 격리해 Mimikatz류 도구의 메모리 덤프를 막는 **LSA 보호 (RunAsPPL)**가 켜져 있는지까지 함께 확인해야 하고, Administrators 그룹의 불필요한 디버깅 권한도 정리해두는 게 한 세트입니다.

문제는 이 MFA조차 요즘은 뚫리는 경우가 늘고 있다는 점입니다. 최근 보안 업계에서는 AI로 만든 음성이나 영상으로 IT지원팀 직원을 사칭해 관리자에게 전화를 걸어 '보안 인증 절차'라며 유도한 뒤, 그 자리에서 입력하는 계정 정보와 OTP 코드를 실시간으로 가로채는 수법이 확인되고 있습니다. 몇 초 분량의 음성 샘플만 있어도 특정 인물의 목소리를 그대로 복제할 수 있는 수준이라, 전화기 너머 목소리만 듣고는 진짜 상사인지 해커인지 구분하기 어려워진 것입니다.



전화기 너머 목소리만으로는 진위를 구분하기 어렵습니다 — 반드시 별도 채널로 재확인

AI 음성 사칭 보이스피싱 4단계 흐름도

왜 지금 특히 위험한가

랜섬웨어 조직의 이름과 제휴 관계는 빠르게 바뀌지만, 인터넷에 노출된 VPN·RDP와 탈취된 관리자 자격 증명이 반복적으로 초기 접근 경로가 됩니다. 특정 조직명보다 외부 노출과 계정 보호 상태를 지속적으로 점검하는 것이 중요합니다.

생성형 AI는 사칭 문구·음성의 제작과 공격 코드의 반복 수정을 빠르게 만들 수 있습니다. 또한 중간자 피싱(AiTM)은 사용자가 입력한 로그인 정보와 세션을 실시간으로 가로챌 수 있으므로, 관리자 계정에는 숫자 코드 방식보다 피싱 저항성 인증을 우선 적용해야 합니다.

이렇게 대비하세요

가장 먼저 손봐야 할 건 관리자 계정의 MFA입니다. 다만 OTP 방식도 AiTM 피싱 앞에서는 완전히 안전하지 않기 때문에, 예산이 허락한다면 피싱 자체가 통하지 않는 하드웨어 보안키(FIDO2) 방식의 MFA로 단계적으로 옮겨가는 걸 검토해보는 게 좋습니다.

동시에 윈도우 서버 설정도 함께 점검해야 합니다. Credential Guard는 자격 증명을 가상화된 공간에 격리하고, LSA 보호(RunAsPPL)는 LSASS에 대한 비인가 코드 삽입과 메모리 접근을 어렵게 합니다. WDigest는 Windows 8.1·Server 2012 R2 이후 기본적으로 평문 자격 증명을 저장하지 않으므로, 레거시 호환을 위해 UseLogonCredential=1로 되살아나 있지 않은지 확인합니다.

Credential Guard는 하드웨어·VBS·운영체제 호환성 조건을 먼저 점검하고, 도메인 컨트롤러에는 적용하지 않는 것이 Microsoft 권고입니다. 따라서 네 설정을 모두 'GPO만으로 오늘 적용'하기보다 지원 여부를 확인하고 단계적으로 배포·검증해야 합니다. [출처: Microsoft Credential Guard](#)

Administrators 그룹에 남아있는 불필요한 디버깅 권한(SeDebugPrivilege)을 정리하는 것도 유효한 조치이지만, 일부 모니터링·APM·백업 에이전트가 이 권한에 의존해 함께 멈출 수 있고, 관리자 스스로 권한을 되돌릴 수 있어 근본적인 차단책은 아니라는 점을 감안해 적용 전 영향도를 점검해야 합니다.

그리고 무엇보다 사람에 대한 교육이 중요합니다. IT지원팀을 사칭한 전화나 화상통화로 계정 정보나 인증 코드를 요구받으면, 그 자리에서 응하지 말고 반드시 별도 채널(사내 메신저, 등록된 내선번호)로 재확인하는 절차를 만들어두는 게 AI 음성 사칭에 대한 가장 현실적인 방어입니다.

서로 다른 자격 증명 공격 경로를 줄이는 다층 통제입니다



관리자 계정 보호 4중 설정 관계도

클라우드·SaaS 계정도 조건부 액세스로 지켜세요

1장에서 짚은 것처럼 최근 침투 경로는 온프레미스 관리자 계정에만 머물지 않습니다. Microsoft 365·Google Workspace 같은 SaaS 관리자 계정과 AWS·Azure IAM 계정도 같은 수준으로 지켜야 합니다. Microsoft Entra ID(옛 Azure AD)의 조건부 액세스(Conditional Access)나 Google Workspace의 컨텍스트 인식 액세스를 켜면, 등록되지 않은 기기·비정상 위치·위험 신호가 감지된 로그인 시도를 로그인 단계에서부터 차단하거나 추가 인증을 요구할 수 있습니다.

퍼블릭 클라우드라면 AWS IAM이나 Azure AD의 관리자·루트 계정에 MFA를 강제하고, 상시 권한 대신 필요할 때만 권한을 부여받는 방식(Just-In-Time 권한 상승)을 적용하는 것이 IAM 계정 탈취로 인한 피해 범위를 줄이는 핵심입니다.

✓ 지금 바로 확인해 볼 체크리스트

- RDP나 VPN 접속 계정 중에 OTP나 인증 앱 없이 패스워드만으로 로그인되는 계정이 남아있지 않은지 확인해보세요.
- Administrators 그룹 계정에 불필요한 프로그램 디버깅 권한이 남아있는지 점검해보세요.
- 최근 IT지원팀을 사칭한 전화나 화상통화로 계정 정보·인증 코드를 요청받은 적이 있는지 직원들에게 물어보세요.
- LSASS 프로세스가 보호 프로세스(RunAsPPL)로 실행되고 있는지, Mimikatz류 자격 증명 덤프 도구가 차단되는지 확인해보세요.
- 평소보다 새벽 시간대 관리자 계정 로그인 시도나 실패 기록이 급증하지 않았는지 로그를 살펴보세요.

Q. OTP 인증만 있으면 충분히 안전한가요?

예전만큼 안전하지 않습니다. 실시간으로 로그인 정보와 OTP 코드를 그대로 가로채는 중간자 피싱(AiTM) 기법이 상용화되면서, OTP도 그 순간 함께 탈취될 수 있습니다. 가능하다면 피싱 자체가 통하지 않는 하드웨어 보안키 방식으로 단계적으로 옮겨가는 걸 추천합니다.

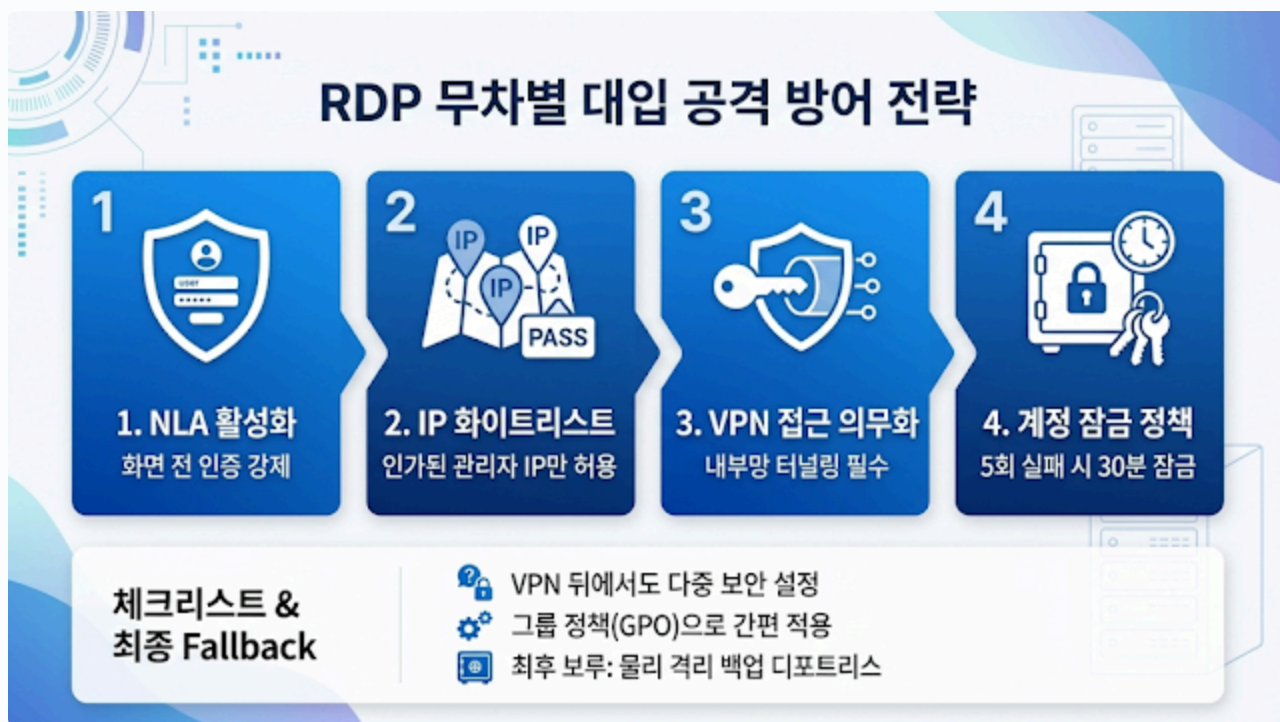
Q. 전산이나 보안 담당 인력이 소규모인 중소기업에서도 이런 설정이 필요한가요?

오히려 더 필요합니다. 대기업은 전담 보안팀이 이상 징후를 빠르게 잡아내지만, 인력이 적은 곳일수록 관리자 계정 하나가 뚫렸을 때 알아채는 데 시간이 오래 걸립니다. 다행히 이번에 소개한 설정 대부분은 별도 장비 없이 그룹 정책만으로 적용할 수 있어서 큰 예산 없이도 시작할 수 있습니다.

관리자 계정은 회사 시스템으로 들어가는 첫 번째이자 가장 중요한 문입니다. 이 문 하나만 제대로 잠가도 랜섬웨어 공격의 상당수를 초기 단계에서 막을 수 있습니다. 문제는 그 문을 여는 방법이 예전보다 훨씬 교묘해졌다는 것입니다 — 사람의 목소리마저 흉내 내는 시대니까요.

③ RDP, 열어두셨나요?

RDP 포트를 인터넷에 그대로 열어두면 계정 공격과 취약점 악용에 지속적으로 노출됩니다. NLA·허용 원본 제한·보호된 원격접속 경로·계정 정책을 함께 적용해 외부 통로를 줄이는 방법을 정리했습니다.



2장에서는 관리자 계정이 뚫렸을 때 MFA와 Credential Guard가 왜 마지막 방어선이 되는지 살펴보았습니다. 이번 장에서는 그 관리자 계정을 노리는 공격자가 애초에 어디로 들어오는지, 즉 RDP(원격 데스크톱)라는 통로 자체를 짚어봅니다.

RDP가 왜 해커들의 첫 관문이 될까요

랜섬허브(RansomHub)는 2025년 4월 와해됐지만, 그 자리를 흡수한 킬린(Qilin)을 비롯해 아키라(Akira), 블랙수트(BlackSuit) 같은 후계 조직들도 RDP를 주요 초기 접근·원격 관리 경로 중 하나로 악용합니다. 이유는 단순합니다. 방화벽이나 EDR 같은 정교한 우회 기법 없이도, 그냥 포트가 열려 있고 계정이 뚫리면 곧바로 서버 안으로 들어갈 수 있기 때문입니다.

CrowdStrike 2026 Global Threat Report에 따르면 eCrime 침입에서 횡적 이동까지의 평균 breakout time은 29분, 관측된 최단 기록은 27초였습니다. 이는 모든 랜섬웨어 공격의 평균 완료 시간이 아니라 CrowdStrike가 관측한 eCrime 활동의 지표입니다. [출처: CrowdStrike 2026 Global Threat Report](#)

DATA NOTE — 지표: CrowdStrike가 관측한 eCrime 침입의 breakout time(초기 침해 후 횡적 이동까지). 통계 범위가 '전체 랜섬웨어 공격 시간'은 아닙니다. 보고서: 2026 Global Threat Report. 확인일: 2026-09-04.

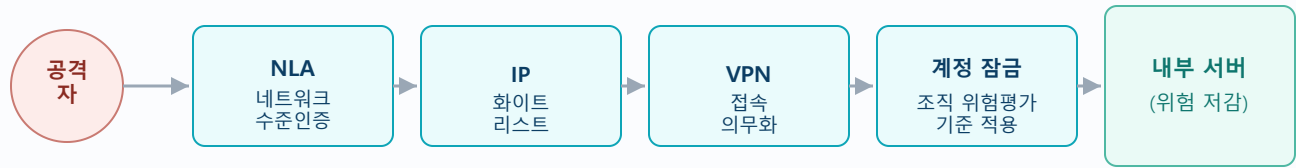
이렇게 대비하세요

가장 먼저 할 일은 RDP 포트(3389)를 인터넷에 직접 노출하지 않는 것입니다. NLA(네트워크 수준 인증)를 활성화해 화면이 뜨기 전 단계에서 인증을 강제하고, 방화벽에는 인가된 관리자 IP만 등록합니다. 'Any'나 '0.0.0.0' 같은 전체 허용 규칙이 남아 있는지 지금 바로 확인해 볼 가치가 있습니다.

그다음은 VPN을 통한 접근 의무화입니다. 관리자가 반드시 VPN 터널을 거쳐야만 내부망에 닿을 수 있게 하면, 설령 RDP 계정 정보가 유출돼도 공격자가 곧바로 서버에 붙을 수 없습니다.

다만 VPN도 장비 자체의 취약점이 반복적으로 노출되는 통로라는 점은 1장에서 이미 짚었습니다. 예산과 여건이 된다면 접속마다 사용자·기기 상태를 검증하고 애플리케이션 단위로만 접근을 허용하는 ZTNA(제로 트러스트 네트워크 액세스)로 단계적으로 전환하는 것이 중장기적으로 더 안전합니다. 다만 초기 구축·운영 부담이 있으므로, 중소 조직이라면 지금 당장은 VPN + NLA + IP 화이트리스트 조합부터 확실히 갖추고 ZTNA는 다음 단계 투자로 검토하는 것이 현실적입니다.

내부로 한 발 들어왔더라도 확산을 늦추는 장치가 필요합니다. 계정 잠금 임계값과 잠금 시간은 무차별 대입 위험, 사용자 수, 서비스 계정, 잠금 악용에 따른 서비스 거부 위험을 함께 평가해 조직별로 정하고 GPO로 강제합니다. 또 오래된 SMBv1 프로토콜을 제거하고 SMB 서명(Signing)을 필수로 설정하면 측면 이동 경로를 줄일 수 있습니다.



RDP 4중 방어 구조도

✓ 지금 바로 확인해 볼 체크리스트

- 방화벽 규칙에 'Any' 또는 '0.0.0.0'으로 열린 RDP 포트가 남아 있는지 확인해 보세요.
- 최근 접속 로그에 새벽 시간대나 낯선 해외 IP에서의 로그인 시도가 반복되는지 살펴보세요.
- 조직의 위험평가에 맞춘 계정 잠금 임계값·잠금 시간이 적용돼 있고, 잠금 악용에 따른 서비스 거부 위험도 검토했는지 확인하세요.
- 이벤트 뷰어의 4625(로그인 실패) 이벤트가 평소보다 급증한 구간이 있는지 확인해 보세요.
- SMBv1이 아직 활성화된 서버나 SMB 서명이 꺼진 공유 폴더가 남아 있는지 점검해 보세요.
- 관리자 계정이 VPN 없이 RDP 포트로 직접 접속되는 경로가 있는지 다시 확인해 보세요.

Q. VPN을 쓰고 있으니 RDP를 직접 노출한 건 아니라서 안전한가요?

VPN을 거친다고 완전히 안전한 건 아닙니다. VPN 장비 자체의 취약점이나 유출된 VPN 계정 정보를 노리는 공격도 많아서, VPN 뒤에서도 NLA와 계정 잠금 정책, IP 화이트리스트를 함께 적용해야 실제 방어 효과가 납니다.

Q. 중소기업도 이런 조치를 적용할 수 있나요?

네, 여기서 소개한 항목 대부분은 별도 장비 구매 없이 방화벽 규칙과 그룹 정책(GPO) 설정만으로 반나절 안에 적용할 수 있습니다. 비용보다 담당자가 이 항목들의 존재를 알고 있는 지가 더 중요합니다.

RDP는 편리하지만, 그 편리함이 그대로 공격자의 편리함이 되는 통로입니다. NLA와 IP 화이트리스트, VPN, 계정 잠금이라는 네 겹의 자물쇠를 지금 다시 점검해 보세요.

④ 리눅스 서버는 안전하다는 착각

리눅스·가상화·NAS도 랜섬웨어의 예외가 아닙니다. 인터넷에 노출된 관리 서비스, 취약한 인증, 패치되지 않은 소프트웨어를 줄이고 서버별 접근 통제와 복구 체계를 갖춰야 합니다.

[랜섬웨어 예방 가이드 ⑤] 리눅스 서버는 안전하다는 착각

1 리눅스·ESXi 정조준
상대적으로 안전하다는 오해. 킬린, 아키라 같은 조직의 표적. 가상화 인프라 위협.

2 AI로 빨라진 위협
AI 에이전트 해킹 가속화. 침투~확산 시간 단축. 패치 며칠 미루면 침해.

3 SSH 및 계정 강화
PermitRootLogin no, 키 기반 인증, 기본 포트 변경, 관리자 IP 허용.

4 파일 무결성 & 신속 패치
핵심 파일 'chattr +i' (불변 속성). CVE 공개 당일~약일 패치 적용 프로세스.

5 최후 보루: 격리 백업
관리자 권한 뚫려도 보호. 물리적 격리 이중 다이오드 구조.

지금 바로 점검하세요

3장에서는 RDP라는 외부 통로를 걸어 잠그는 법을 다뤘습니다. 이번 장에서는 "리눅스는 윈도우보다 안전하다"는 오래된 통념이 왜 유효하지 않은지, 리눅스·ESXi 서버는 물론 NAS 장비를 노리는 실제 공격과 방어법을 짚어봅니다.

랜섬웨어 운영자는 Windows 엔드포인트뿐 아니라 Linux 서버와 VMware ESXi 같은 가상화 기반까지 표적으로 삼습니다. 따라서 운영체제가 다르다는 이유로 관리 인터페이스 노출, 취약한 SSH 인증, 패치 지연, 백업 접근권한 문제를 별도 위험으로 취급하지 않아서는 안 됩니다.

리눅스·ESXi 서버, 어떻게 뚫리나

공격은 크게 두 경로입니다. 하나는 SSH입니다 — 리눅스에서 가장 많이 쓰이는 서비스인 만큼 무차별 대입 공격도 SSH 포트에 몰립니다. 다른 하나는 알려진 취약점입니다. 리눅스 커널 nftables 결함 CVE-2024-1086은 실제 공격에 악용된 취약점으로 알려져 있어 우선 패치 대상이며, ESXi 인증 우회 취약점 CVE-2024-37085는 아키라·블랙바스타가 삭제된 관리자 그룹을 재생성해 호스트를 장악하는 데 썼습니다. 하이퍼바이저 하나만 뚫리면 그 위 가상머신 수십 대가 한꺼번에 암호화됩니다.



SSH·ESXi 침투 경로와 하이퍼바이저 장악 시 VM 전체 확산도

공개된 취약점 정보가 실제 공격에 활용되는 시간은 짧아질 수 있습니다. 특히 인터넷에 노출된 서비스는 자산 식별, 완화 조치, 긴급 패치를 우선 처리하고 패치가 어려우면 접근 제한이나 서비스 격리를 적용해야 합니다.

이렇게 경화하세요

SSH 설정부터 손봐야 합니다. PermitRootLogin no로 root 직접 로그인을 막고, 키 기반 인증으로 전환하고, 가능하면 기본 22번 포트도 바꿔주세요. iptables 방화벽에서 인가된 관리자 IP만 SSH 접속을 허용하도록 좁혀두는 것도 중요합니다.

파일 무결성도 챙기세요. 설정 파일·백업 스크립트에 chattr +i로 불변 속성을 걸면 우발적이거나 일반 권한의 변경을 어렵게 할 수 있습니다. 그러나 root 또는 적절한 capability를 얻은 공격자는 chattr -i로 해제할 수 있으므로 보안 경계나 불변 백업·에어갭의 대체 수단으로 보아서는 안 됩니다. 변경 탐지(AIDE 등)와 별도 불변 사본을 함께 운영하세요.

마지막은 위험 기반 패치 관리입니다. 인터넷 노출 여부, 악용 확인 여부, 자산 중요도를 기준으로 우선순위를 정하고 긴급 변경 절차를 마련하세요. 패치가 즉시 어려우면 관리 콘솔 비노출, 접근 제한, 탐지 규칙 같은 보완 통제를 적용합니다.

그 외 리눅스 서버 기본기도 놓치지 마세요

SSH 설정과 패치 외에도 리눅스 서버 자체를 단단히 하는 기본기가 있습니다. fail2ban은 반복되는 인증 실패를 바탕으로 접근을 제한할 수 있지만 중앙 인증·MFA·방화벽 정책을 대신하지는 않습니다. unattended-upgrades(데비안·우분투 계열)나 dnf-automatic(RHEL 계열)은 보안 업데이트 지연을 줄일 수 있으므로 시험 환경과 재부팅·롤백 절차를 포함해 운영합니다.

SELinux(RHEL 계열)나 AppArmor(우분투 계열) 같은 강제 접근 제어(MAC)를 꺼두지 말고 활성 상태로 유지하세요. 취약점 하나가 뚫려도 해당 프로세스가 손댈 수 있는 파일·권한 범위 자체를 좁혀주기 때문에, root 권한을 통째로 내주는 사고를 줄여줍니다. AIDE 같은 파일 무결성 모니터링 도구로 시스템 바이너리·설정 파일의 변경을 감지하도록 해두면, 침투 이후 조용히 심어지는 백도어나 변조를 더 빨리 알아챌 수 있습니다. 마지막으로 불필요한 서비스·포트는 꺼두고, sudo 권한은 꼭 필요한 계정에만 최소 범위로 주는 것도 기본이지만 자주 빠지는 항목입니다.

NAS 장비도 같은 원리로 뚫립니다

NAS는 웹 관리 화면·앱·원격 접속 기능을 갖춘 서버로 취급해야 합니다. 관리 화면을 인터넷에 직접 노출하지 말고, 지원되는 펌웨어와 앱 업데이트를 적용하며, 기본 관리자 계정 비활성화·MFA·접근 로그·별도 백업을 운영하세요. 제조사 지원이 끝난 장비는 교체 계획을 세웁니다.

NAS 방어 핵심은 서버와 다르지 않습니다. 관리 웹 화면(DSM·QTS·QVR Pro 등)을 포트포워딩으로 인터넷에 직접 열어두지 말고 VPN을 거치도록 바꾸세요. 기본 admin 계정은 비활성화하고 별도의 강력한 관리자 계정에 2단계 인증을 걸어두세요. 펌웨어·앱 자동 업데이트를 켜서 패치 공백을 최소화하세요. 그리고 Btrfs 스냅샷 같은 버전 관리 기능을 켜두면, 랜섬웨어가 파일을 암호화해도 감염 이전 스냅샷으로 되돌릴 여지가 남습니다 — 다만 6장에서 다루듯 NAS 자체가 뚫리면 스냅샷까지 함께 삭제될 수 있으므로, NAS를 유일한 백업 사본으로 삼지 않는 것이 원칙입니다.

✓ 지금 바로 확인해 볼 체크리스트

- root 계정으로 SSH 원격 로그인 이 그대로 허용돼 있지는 않은지 확인해 보세요
- SSH가 인터넷 전체에 노출돼 있거나 전 세계 각지에서 반복 인증 공격을 받고 있지 않은지 로그를 확인해 보세요
- iptables·방화벽에 인가된 관리자 IP 외 접속이 차단돼 있는지 점검해 보세요
- 핵심 설정 파일·백업 스크립트에 chattr +i와 변경 탐지를 적용하되, root 탈취 시 해제 가능하다는 전제로 별도 불변 사본도 갖췄는지 확인해 보세요
- fail2ban 등으로 SSH·로그인 실패 반복 IP가 자동 차단되고 있는지, 자동 보안 업데이트 (unattended-upgrades·dnf-automatic)가 켜져 있는지 확인해 보세요
- SELinux·AppArmor가 꺼져 있지는 않은지, 불필요한 서비스·포트가 열려 있지는 않은지 점검해 보세요
- ESXi·Hyper-V 등 가상화 관리 인터페이스가 인터넷에 그대로 노출돼 있지는 않은지, 최신 보안 패치가 적용됐는지 확인해 보세요
- NAS(DSM·QTS 등) 관리 웹 화면이 포트포워딩으로 공인 IP에 그대로 노출돼 있지는 않은지 확인해 보세요
- NAS 기본 admin 계정을 그대로 쓰고 있지는 않은지, 2단계 인증과 펌웨어 자동 업데이트가 켜져 있는지 확인해 보세요
- 인터넷 노출·실제 악용·자산 중요도를 기준으로 긴급 패치 대상과 SLA가 정해져 있는지 확인해 보세요

Q. 리눅스가 윈도우보다 원래 안전하다고 들었는데, 지금도 그런가요?

공격 표면이 상대적으로 작았던 건 사실이지만, 킬린·아키라처럼 리눅스·ESXi 전용 도구를 갖춘 조직이 늘면서 격차가 많이 좁혀졌습니다. "안전하다"는 인식 때문에 관리를 소홀히 하는 게 오히려 더 위험합니다.

Q. 중소기업도 이런 조치를 적용할 수 있나요?

네, root 로그인 차단과 관리자 IP 화이트리스트는 설정 자체는 몇 분이면 끝납니다. 전산 인력이 적을수록 초기 설정 한 번으로 오래 방어 효과를 보는 항목부터 우선순위를 두는 게 현실적입니다.

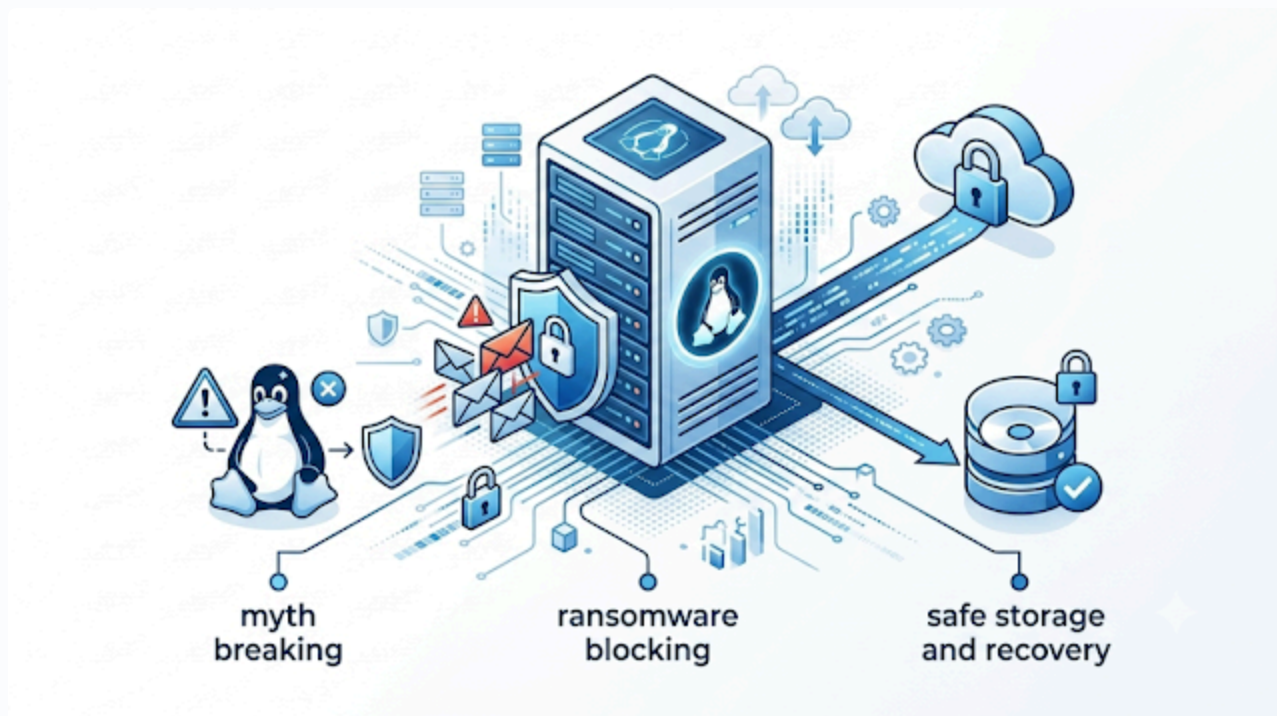
Q. NAS는 그냥 저장장치인데, 서버처럼 관리해야 하나요?

네. NAS는 앱·원격 접속·미디어 서버 기능까지 갖춘 서버입니다. 관리 화면을 인터넷에 직접 노출하지 않고, 지원되는 업데이트와 MFA를 적용하며, NAS 자체와 분리된 복구 사본을 유지해야 합니다.

리눅스·ESXi 서버, 그리고 NAS까지 더 이상 "상대적으로 안전한 영역"이 아닙니다. 하이퍼바이저 하나가 뚫리면 가상머신 수십 대가, NAS 관리 화면 하나가 뚫리면 그 안의 파일과 스냅샷까지 한꺼번에 암호화될 수 있는 만큼, 파급력은 윈도우 서버보다 클 수도 있습니다.

⑤ 망을 나누면 확산을 막을 수 있다

관리자 계정을 지키고 RDP를 막아도 단말과 서버가 같은 망이면 랜섬웨어의 측면 이동 위험이 크게 높아집니다. 망을 User-Server-Backup으로 나누고 백업망의 계정·관리 경로를 운영망과 분리하는 구조가 피해 범위를 줄이는 이유를 짚어봅니다.

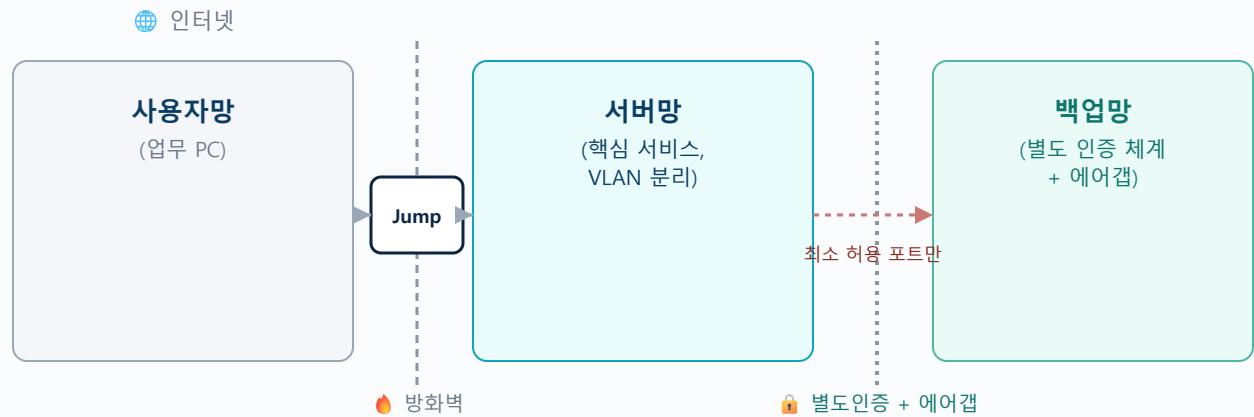


4장에서는 "리눅스는 원래 안전하다"는 통념이 왜 더 이상 유효하지 않은지, 킬린·아키라 같은 조직이 SSH와 ESXi를 어떻게 노리는지 다뤘습니다. 이번 장에서는 관리자 계정을 뚫은 RDP로 들어오는 SSH로 침투하든, 결국 공격자가 내부에서 마음껏 옆으로 이동하지 못하게 막는 방법 — 네트워크 분리와 제로트러스트 백업을 짚어봅니다.

망이 하나로 뚫려 있으면 왜 위험한가

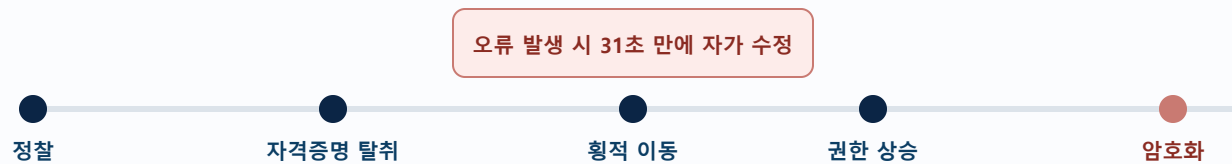
업무용 PC가 모여 있는 사용자망, 핵심 서비스가 돌아가는 서버망, 백업 데이터가 보관된 백업망이 방화벽 없이 하나로 이어져 있으면 처음 침해된 PC에서 다른 자산으로 이동하기 쉬워집니다. 서버망은 VLAN과 방화벽으로 분리해 필수 흐름만 허용하고, 백업망은 별도 관리 계정과 오프사

이트·오프라인 또는 불변 사본으로 보호합니다. Zone 간 관리 통신은 통제된 Jump Server나 PAM 을 거치게 하고, 원격 접속은 ZTNA 등 신원·기기 상태 기반 통제를 검토합니다.



User·Server·Backup 3존 네트워크 분리 구조도

2026년 7월 Sysdig는 JADEPUFFER를 LLM이 종단간 수행한 최초의 문서화된 에이전트형 랜섬웨어 사례로 평가했습니다. 이 에이전트는 실패한 로그인 뒤 31초 만에 수정된 페이로드를 내놓았습니다. 원문은 전체 공격이 15분 안에 끝났다고 밝히지 않으므로 해당 시간 주장은 사용하지 않습니다. [출처: Sysdig JADEPUFFER 분석](#)



실패 진단 후 수정 페이로드 발행 — 31초
Sysdig가 문서화한 첫 완전자율형 LLM 에이전트 랜섬웨어

JADEPUFFER 에이전트형 랜섬웨어 공격 흐름(시간 비례 아님)

침입을 놓치지 않는 탐지·모니터링 운영

예방 통제만으로 모든 침입을 막을 수는 없습니다. 외부 노출 자산과 계정, 엔드포인트, 서버, 백업 플랫폼의 신호를 한곳에 모으고 담당자가 실제로 대응할 수 있는 경보로 바뀌어야 합니다. 소규모 조직은 모든 로그를 수집하기보다 아래 고위험 행위부터 시작하는 편이 현실적입니다.

공격 단계	우선 탐지 신호	대응 통제	적용 수준
VPN·외부 서비스 취약점	미등록 인터넷 노출 자산, 긴급 취약점, 비정상 국가·시간대 접속	자산 목록·외부 노출 점검, 긴급 패치, 접근 원본 제한	오늘 적용
계정 탈취	로그인 실패 급증, 불가능한 이동, 신규 MFA 등록, 특권 역할 변경	피싱 저항성 MFA, 조건부 접근, 관리자 계정 분리	계획 필요
횡적 이동·권한 상승	여러 서버 연쇄 로그인, 원격 서비스 생성, 비정상 PowerShell·SMB·WinRM	EDR, 중앙 로그, 세그멘테이션, Jump Server·PAM	인프라 필요
보안·백업 무력화	EDR 중지, VSS·스냅샷·백업 작업 삭제, 보존정책·관리자 변경	변조 방지, 별도 백업 계정, 삭제 지연·불변 보존, 즉시 경보	인프라 필요
대량 변경·반출	파일 확장자·엔트로피 급변, 대량 이름 변경, 평소와 다른 외부 전송	행위기반 차단, 호스트 격리, 전송 통제, 사고대응 호출	인프라 필요

경보에는 소유자, 심각도, 확인 시간, 격리 권한과 연락 경로를 지정합니다. 월 1회 이상 표본 경보를 끝까지 처리해 보고, 분기별로 '관리자 계정 이상 로그인 → 여러 서버 접근 → 백업 삭제 시도' 시나리오를 훈련해 탐지부터 격리까지 걸린 시간을 기록합니다. 자체 24시간 대응이 어렵다면 MDR 등 외부 운영을 검토하되, 자산·로그 범위와 격리 승인 절차는 조직이 직접 정의해야 합니다.

적용 근거 — NIST CSF 2.0 랜섬웨어 프로파일의 Detect·Respond 성과와 CISA #StopRansomware Guide의 중앙 로그·EDR·이상행위 탐지 권고를 운영 절차로 재구성했습니다. [NIST IR 8374 Rev.1](#) · [CISA #StopRansomware Guide](#)

왜 백업까지 같은 원리로 지켜야 하는가

요즘 공격은 정상 로그인 정보를 그대로 들고 관리자 권한까지 올라가는 방식이라, 단순히 경계를 지키는 것만으로는 막을 수 없습니다. 그래서 백업 시스템의 계정 체계 자체를 운영 시스템과 완전히 갈라놓아야 합니다. 백업 인프라를 별도의 인증 영역으로 독립시켜, 운영 쪽 최고 권한 계정

하나가 통째로 넘어가더라도 그 권한으로는 백업 쪽에 로그인 시도조차 할 수 없게 만드는 것이 핵심입니다. 여기에 WORM(Write Once Read Many) 방식으로 보존 기간 동안은 해커는 물론 최고 관리자조차 데이터를 수정·삭제할 수 없게 잠가두면, 관리자 계정이 뚫린다고 백업까지 함께 파괴되는 최악의 시나리오를 막을 수 있습니다.

이렇게 대비하세요

먼저 지금 네트워크 구성도를 꺼내서 사용자망·서버망·백업망이 실제로 물리적·논리적으로 분리돼 있는지부터 확인해 보세요. VLAN으로만 나뉘어 있고 방화벽 정책이 느슨하면 나뉜 게 아닙니다 — Zone 간 통신은 반드시 필요한 포트만, Jump Server를 거쳐서만 허용되도록 정책을 좁혀야 합니다.

백업 서버는 별도의 계정 체계로 운영하세요. 운영 서버 관리자와 백업 서버 관리자를 아예 다른 사람, 다른 인증 체계로 두면 한쪽이 뚫려도 다른 쪽은 그대로 살아남습니다.

마지막으로 접근 제어를 "한 번 인증하면 계속 신뢰"하는 방식에서 "매번 확인하는" 방식으로 바뀌어야 합니다. 정상 계정으로 로그인했다고 무한 신뢰하지 않고, 단말 상태·접근 위치·행동 패턴이 평소와 다르면 추가 인증을 요구하거나 접근을 제한하는 구조가 AI 기반 자동 공격 시대에는 특히 중요합니다.

✓ 지금 바로 확인해 볼 체크리스트

- 사용자 PC에서 서버망 핵심 자원으로 직접 접속되는 경로가 남아 있는지는 않은지 확인해 보세요
- 백업 서버가 운영망 통합 인증 체계에 걸쳐 있어, 운영망 관리자 권한만으로도 로그인 되는 상태는 아닌지 점검해 보세요
- 백업 스토리지에 WORM(수정 불가) 정책이 실제로 걸려 있는지, 관리자 계정으로도 삭제가 안 되는지 테스트해 보세요
- Zone 간 통신이 방화벽·Jump Server 없이 직접 연결돼 있는 구간이 있는지 점검해 보세요
- 평소보다 짧은 시간 안에 여러 서버로 연쇄 접속 시도가 발생한 로그가 있는지 확인해 보세요

Q. 기업인데 서버가 몇 대 안 돼도 망을 꼭 나눠야 하나요?

서버 대수와 무관하게 사용자망과 서버망, 백업망만이라도 물리적으로든 VLAN으로든 나눠두는 게 가장 비용 대비 효과가 큰 방어입니다. 서버가 적을수록 한 대가 뚫렸을 때 파급력이 상대적으로 더 크기 때문입니다.

Q. 백업 서버를 AD에서 분리하면 관리가 너무 불편해지지 않나요?

초기 계정 체계를 따로 만드는 번거로움은 있지만, 그 불편함이 바로 해커도 넘어오지 못하는 이유입니다. 편의성과 맞바꾼 만큼 최후의 보루로서 가치가 생기는 것입니다.

관리자 계정을 지키고 RDP를 막고 리눅스 서버를 경화해도, 망이 하나로 뚫려 있으면 결국 공격자는 어딘가로 옆길은질쳐 들어옵니다. 애초에 옆으로 갈 길 자체를 끊어두는 네트워크 분리와 백업망 격리가 마지막 안전판입니다.

⑥ 백업이 있어도 뚫리는 이유 — 3-2-1-1-0과 초기 대응법

Veeam의 피해 조직 대상 조사에서 조사된 공격의 96%가 백업 저장소를 표적으로 삼았습니다. 3-2-1-1-0 백업 원칙과 감염 직후 담당자가 수행할 초기 대응을 정리했습니다.

랜섬웨어 백업 공격 시대: 완벽 대비 전략

1. KISA 3-2-1 백업 보안수칙

- 3** **사본 유지**
원본 1개 + 백업 2개 이상 = 총 3개
- 2** **다른 매체**
디스크, 테이프, 클라우드 등
- 1** **격리 보관**
네트워크 차단, 오프라인/오프사이트

2. 5분 골든타임 S.T.O.P 대응법

- 1 S** **SEPARATE**
(랜선 분리)
- 2 T** **TURN ON**
(전원 유지!)
- 3 O** **OFF**
(외장장치 분리)
- 4 P** **PRESERVE & REPORT**
(전문가 신고)

핵심요약:

랜섬웨어 96%가 백업 겨냥, 44.4%는 백업까지 파괴

백업 개수보다 중요한 건 격리 상태와 복구 훈련입니다.

지금 바로 실천하세요!
보안 전문가 가이드

Veeam의 2024 Ransomware Trends Report는 2023년에 랜섬웨어 또는 다른 사이버공격을 겪은 조직의 관계자 1,200명을 조사했습니다. 조사된 공격의 96%에서 백업 저장소가 표적이 됐고, 76%에서는 백업 저장소가 영향을 받았습니다. 이는 전 세계 전체 기업의 발생률이 아니라 피해 조직 대상 설문 결과입니다. [출처: Veeam 2024 Ransomware Trends Report](#)

DATA NOTE — 모집단: 2023년에 랜섬웨어 또는 다른 사이버공격을 한 차례 이상 겪은 조직의 관계자 1,200명. 96%와 76%는 이 피해 조직 표본의 응답이며 전체 기업의 발생률이 아닙니다. 확인일: 2026-09-04.

왜 백업이 있어도 뚫리는가

가장 흔한 원인은 백업 서버가 운영 서버와 같은 계정 체계를 쓰는 경우입니다. 백업 서버가 운영망의 Active Directory(AD) 도메인에 그대로 조인돼 있으면, 해커가 운영 서버 관리자 권한 하나만 탈취해도 백업 서버까지 같은 계정으로 로그인할 수 있습니다. 여기에 백업이 네트워크로 상시 연결된 NAS나 스토리지에만 저장돼 있으면, 랜섬웨어가 운영 서버를 암호화하는 김에 연결된 백업 볼륨까지 그대로 훔고 지나갑니다. 실제로 최근 공격 그룹들은 데이터를 암호화하기 전에 먼저 백업 스냅샷과 백업 관리 콘솔부터 찾아 삭제하는 순서로 움직이는 경우가 많습니다. 백업을 만들어 두는 것과, 그 백업이 공격자 손이 닿지 않는 곳에 있는 것은 완전히 다른 이야기입니다.

지금 특히 위험한 이유

여기에 AI가 공격뿐 아니라 협상 단계까지 자동화하면서 골든타임을 더 짧게 만들고 있습니다. 보안업계에서는 2026년을 'AI 에이전트 해킹 원년'으로 부르는데, 공격자 쪽 AI 봇이 표적 탐색과 침투는 물론 피해 기업과의 몸값 협상까지 사람 없이 자율적으로 수행하는 사례까지 등장했습니다. 사람이 대응팀을 소집하고 상황을 파악하는 사이, 공격자 쪽은 이미 다음 단계로 넘어가 있는 셈입니다.

3-2-1-1-0 백업과 골든타임 대응, 이렇게 준비하세요

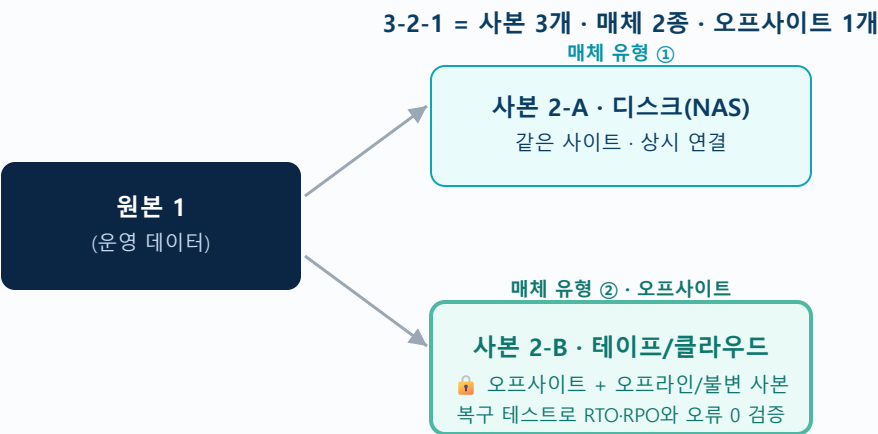
3-2-1은 원본을 포함한 사본 3개를 2종 이상의 매체에 보관하고 그중 1개를 오프사이트에 두는 원칙입니다. 오프사이트 사본이 반드시 물리적 에어갭이라는 뜻은 아닙니다. 현대적인 3-2-1-1-0은 여기에 오프라인 또는 불변 사본 1개와 복구 검증 오류 0개를 더합니다. 백업 관리 계정은 운영 계정과 분리하고 MFA, 보존 잠금, 삭제 지연, 백업 구성 자체의 백업을 적용합니다. 정기 복구 테스트에서는 목표 복구 시간(RTO)과 허용 데이터 손실 범위(RPO)를 모두 충족하는지 검증하고, 깨끗한 복구 환경(클린룸)에서 실행 절차까지 확인합니다.

불변(Immutable) 백업과 유출 통제도 함께 챙기세요

"오프라인 또는 불변 사본"에서 불변은 물리적 테이프만을 뜻하지 않습니다. 퍼블릭 클라우드를 쓴다면 AWS S3 Object Lock, Azure Blob 불변 스토리지, 대부분의 최신 NAS·백업 소프트웨어가 제공하는 WORM(Write Once Read Many) 스냅샷으로 소프트웨어 기반의 논리적 에어갭을 구현

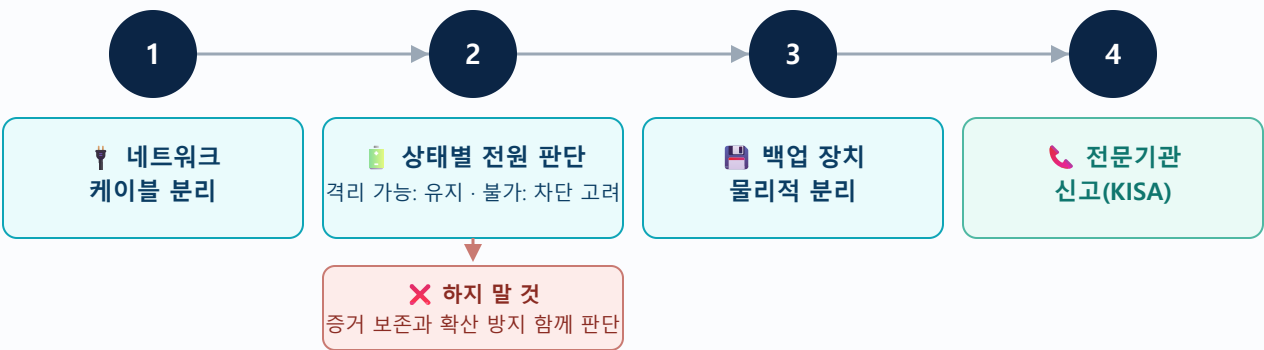
할 수 있습니다. 보존 기간 동안은 관리자 권한으로도 삭제·수정이 되지 않도록 잠그는 것이 핵심이며, 잠금 설정 자체를 바꿀 수 있는 계정은 백업 운영 계정과 분리해야 합니다.

3-2-1-1-0과 불변 백업은 암호화로 인한 가용성 파괴는 막아도, 공격자가 정상 세션 중에 데이터를 밖으로 빼가는 유출(이중 협박)까지는 막지 못합니다. 유출은 서버가 이미 켜져서 정상 권한으로 접근 가능한 상태에서 일어나므로, 대량 다운로드·비정상 아웃바운드 트래픽을 탐지하는 DLP(데이터 유출 방지) 솔루션이나 방화벽의 아웃바운드 트래픽 통제를 별도로 갖춰야 합니다.



KISA 3-2-1 백업 전략 구조도

감염이 의심되면 가장 먼저 해당 호스트를 네트워크에서 격리하고 연결된 백업 장치를 보호합니다. 격리에 성공했다면 전원을 유지해 휘발성 증거를 보존하고 전문가에게 인계합니다. 그러나 네트워크 분리가 불가능하고 암호화·확산이 계속된다면 추가 피해를 막기 위해 전원 차단을 고려해야 합니다. 이후 KISA·침해사고 대응 조직에 신고하고, 법무·개인정보 담당·경영진·보험 담당자가 유출 신고와 고객 통지 의무를 함께 판단합니다. 출처: CISA #StopRansomware Guide



감염 직후 골든타임 대응 순서도

신고는 침해 범위 분석, 증거 보존, 복호화 도구 존재 여부 확인과 법적 통지 판단에 도움이 될 수 있습니다. 자체 복구를 서두르기보다 증거를 보존하고 KISA 및 수사기관 등 관계 기관과 협의해야 합니다.

✓ 지금 바로 확인해 볼 체크리스트

- 최근 복구 테스트에서 RTO·RPO 충족 여부와 복구 데이터 오류 0건을 검증했는지 확인하세요.
- 백업 서버가 운영 서버와 같은 관리자 계정이나 AD 도메인을 쓰고 있어요.
- 백업 사본이 전부 네트워크로 상시 연결된 NAS나 스토리지에만 저장돼 있고, 오프라인 .에어갭 사본은 따로 없어요.
- 백업 파일이 삭제되거나 수정되면 관리자에게 알림이 오도록 설정돼 있지 않아요.
- 감염 발생 시 누가 네트워크를 차단하고 누가 신고할지 정해진 담당자나 매뉴얼이 없어요.
- 감염 시 네트워크 격리를 우선하고, 격리가 불가능해 확산이 계속될 때만 전원 차단을 고려하는 조건부 절차가 있는지 확인하세요.

Q. 백업이 3개나 있는데도 왜 위험하다는 건가요?

사본 개수보다 중요한 건 그 사본들이 서로 얼마나 격리돼 있는가입니다. 세 개의 백업이 전부 같은 네트워크, 같은 관리자 계정으로 접근 가능하다면 공격자 입장에서는 사실상 하나의 표적과 다르지 않습니다. 최소 한 사본은 운영 환경과 독립된 오프사이트에 두고, 랜섬웨어 복원력을 높이려면 그 사본을 오프라인·불변 또는 물리적 에어갭 형태로 보호하는 것이 좋습니다.

Q. 감염 초기 대응에서 가장 많이 하는 실수는 뭔가요?

상황을 확인하지 않고 전원부터 끄거나, 반대로 무조건 켜두는 것입니다. 먼저 네트워크에서 격리합니다. 격리가 가능하면 휘발성 증거 보존을 위해 전원을 유지하고 전문가에게 인계하되, 격리할 수 없고 암호화·확산이 계속되면 추가 피해를 막기 위해 전원 차단을 고려합니다.

Q. 몸값을 내지 않고도 복구할 수 있나요?

암호화 방식에 결함이 있는 변종이라면 가능합니다. KISA·경찰청이 실제로 공격자가 쓴 암호화 방식의 허점을 분석해 복구 도구를 만들어 피해 기업의 데이터를 전량 복구하고 수억 원대 복호화 비용 지급을 막은 사례가 있습니다. 자체 복구를 시도하다 흔적을 훼손하기 전에, 먼저 신고하고 전문기관의 분석을 받아보는 게 순서입니다.

결국 랜섬웨어 방어 of 마지막 단계는 늘 백업이었는데, 이제는 공격자들도 그걸 잘 알고 있습니다. 백업의 개수를 늘리는 것보다, 그 백업이 운영망과 얼마나 확실히 격리돼 있는지, 그리고 실제로 복구가 되는지를 검증하는 게 훨씬 중요해졌습니다.

관리자 권한 침해 시에도 복구 사본까지 같은 경로로 훼손되지 않도록 운영망과 백업 관리 영역의 계정·권한·접속 경로를 분리해야 합니다.

⑦ 5개 방어선 자가진단 — 우리 조직은 지금 몇 점일까요

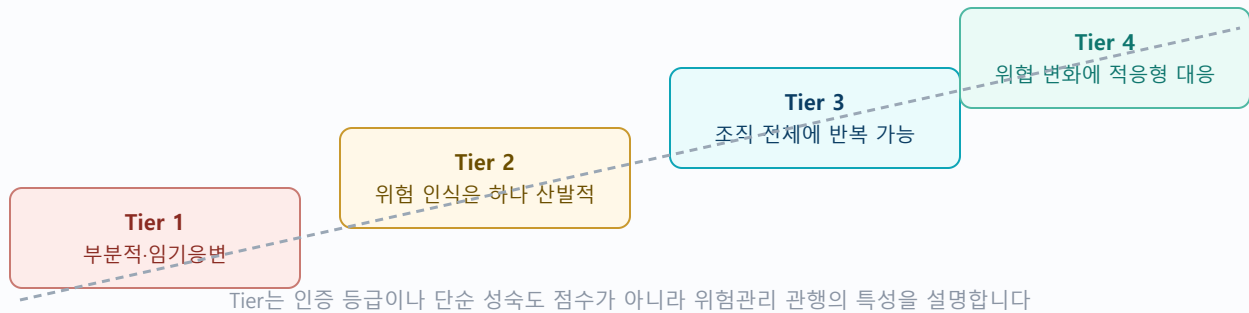
"체크리스트를 다 지켰는가"보다 "어느 방어선이 가장 약한가"가 중요합니다. 7개 장의 핵심을 NIST의 최신 랜섬웨어 대응 기준으로 5개 영역 자가진단표로 압축해서 마무리합니다.

랜섬웨어 5단계 철벽 방어



designed by freepik

관리자 계정 보호를 시작으로 RDP 통제, 리눅스 서버 경화, 네트워크 분리, 백업 전략까지 6개 주제를 다뤘습니다. NIST IR 8374 Rev.1은 2026년 6월 발표된 CSF 2.0 랜섬웨어 커뮤니티 프로파일입니다. 아래 표와 점수는 NIST가 제시한 공식 평가표가 아니라, 본서가 해당 프로파일의 보안 성과를 참고해 구성한 간이 자가진단입니다. CSF Tier는 거버넌스와 위험관리 관행의 엄격성을 설명하는 개념이며 단순 성숙도 점수로 사용하지 않습니다.



NIST CSF Implementation Tier 개요

왜 체크리스트가 아니라 자가진단이어야 할까요

단순 체크리스트의 함정은 모든 항목을 "예/아니오"로만 답하게 만든다는 것입니다. 이 장의 5개 영역은 본서가 실무 점검을 위해 재구성한 것이며 NIST 공식 분류나 점수표가 아닙니다. NIST IR 8374 Rev.1은 CSF 2.0의 Govern·Identify·Protect·Detect·Respond·Recover 성과를 랜섬웨어 위험에 맞춰 선별한 프로파일이고, Tier 1(Partial)부터 Tier 4(Adaptive)는 조직의 위험관리 관행을 설명합니다. [출처: NIST CSF 2.0 Tiers](#) · [출처: NIST IR 8374 Rev.1](#)

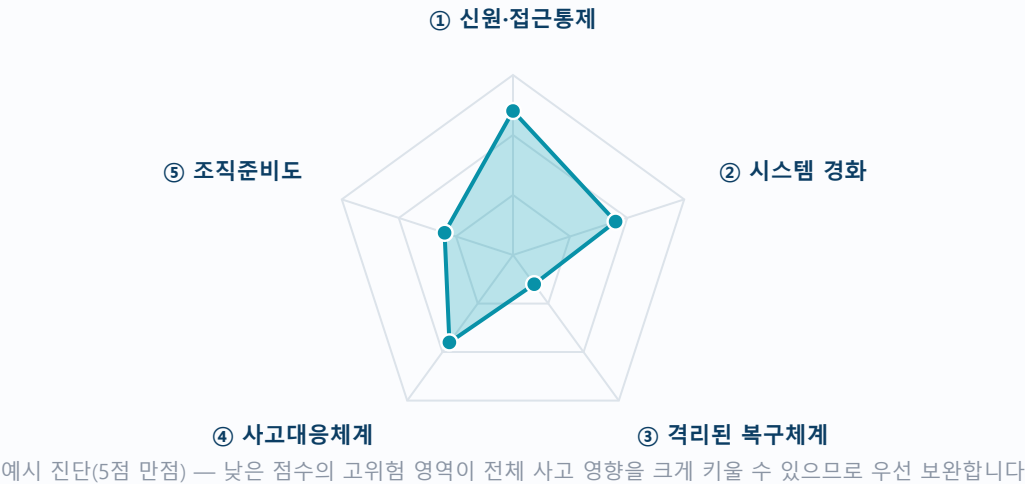
5개 방어선, 지금 우리는 몇 점일까요

- ① **신원과 접근 통제** — 2장에서 다룬 관리자 계정 MFA와 Credential Guard가 실제로 적용돼 있고, 그 MFA가 피싱에도 뚫리지 않는 방식인가요. 비밀번호만으로 로그인되는 관리자 계정이 하나라도 남아있다면 이 영역부터 손봐야 합니다.
- ② **시스템 경화** — 3장의 RDP IP 화이트리스트·VPN 통제, 4장의 리눅스 SSH 제한·fail2ban·자동 보안 업데이트·chattr +i 설정과 NAS 관리 화면 비노출·2단계 인증이 실제 서버·장비에 반영돼 있나요. 문서에만 있고 실제 장비에는 적용 안 된 경우가 의외로 많습니다.
- ③ **격리된 복구 체계** — 5장의 네트워크 분리, 6장의 3-2-1 백업 전략이 실제로 지켜지고 있나요. 백업 서버가 운영 서버와 같은 관리자 계정을 쓰고 있다면 이 영역은 1점 수준으로 봐야 합니다.
- ④ **탐지·사고 대응 체계** — 관리자 이상 로그인, 연쇄 원격접속, 보안도구 중지, VSS·백업 삭제 시도가 중앙 경보로 연결되고, 네트워크 격리·증거 보존·전문기관 신고 절차를 담당자가 실제로 수행할 수 있나요.

⑤ 복구·조직 준비도 — 정기 복구 훈련에서 RTO·RPO를 충족했는지, 책임자와 대체자가 정해져 있는지, 사칭 시나리오를 포함한 직원 교육이 실행되는지를 보는 영역입니다.

점수 매기는 법 — 아래는 NIST 기준이 아니라 **본 가이드 자체의 채점 기준**입니다. 각 영역을 1~5점으로 평가할 때 이 기준을 그대로 적용하세요.

점수	기준
1점	통제가 거의 없거나 담당자 개인 경험에 의존
2점	일부 적용됐지만 조직 전체에 일관되지 않음
3점	주요 시스템에 정책으로 적용
4점	로그·경보·정기 테스트로 효과를 검증
5점	측정 결과를 바탕으로 지속 개선·자동화



5개 방어선 자가진단 레이더 차트 예시

AI가 방어선의 기준 자체를 바꾸고 있습니다

AI는 사칭 콘텐츠 제작, 취약점 탐색, 공격 코드 수정과 반복 실행의 속도를 높이고 있습니다. Sysdig는 2026년 7월 JADEPUFFER를 LLM이 종단간 수행한 최초의 문서화된 에이전트형 랜섬웨어 사례로 평가했습니다. 다만 31초는 실패한 로그인 뒤 수정 페이로드를 낸 시간이며 전체 공격

시간이 아닙니다. CrowdStrike가 발표한 89%는 'AI 지원 공격자에 의한 공격 증가율'로, 자율 AI 침해 전체의 연간 증가율을 뜻하지 않습니다. [출처: Sysdig JADEPUFFER 분석](#) · [출처: CrowdStrike 2026 Global Threat Report](#)

✓ 5개 방어선 자가진단

- 관리자 계정 MFA가 피싱에도 뚫리지 않는 방식인가요, 아니면 문자 OTP 방식에 머물러 있나요?
- RDP 포트가 인터넷에 그대로 노출돼 있지는 않나요?
- 백업 서버가 운영 서버와 같은 관리자 계정이나 도메인으로 접근 가능한 상태는 아닌가요?
- EDR 중지, VSS·백업 삭제, 여러 서버 연쇄 로그인 경보가 중앙에서 수집되고 담당자에게 전달되나요?
- 가장 최근 복구 훈련을 실제로 해본 게 언제인가요? 문서로만 있고 실행해본 적 없다면 그 자체가 약점입니다.
- 감염 발생 시 첫 5분 안에 누가 뭘 해야 하는지, 담당자 전원이 그 자리에서 바로 말할 수 있나요?
- AI가 만든 사칭 메일·음성을 구분하는 교육을 최근 1년 내에 받아본 적 있나요?

Q. 다섯 영역 중 하나라도 점수가 낮으면 위험한가요?

네, 낮은 점수의 고위험 영역이 전체 사고 영향을 크게 키울 수 있습니다. 나머지 네 영역이 잘 갖춰져 있어도 복구 체계(③번)가 운영망과 분리 안 돼 있으면, 원본과 백업이 동시에 암호화되는 최악의 시나리오로 이어질 수 있습니다.

Q. 중소기업도 이 5개 영역을 다 갖춰야 하나요?

한 번에 다 갖추려 하지 않아도 괜찮습니다. 가장 낮은 영역 하나만 다음 분기 목표로 잡고 순서대로 적용하는 게 현실적입니다 — 이 시리즈가 다룬 순서(계정 보호 → 시스템 경화 → 네트워크 분리 → 백업 → 대응)도 실제 방어 우선순위가 높은 순서로 짠 것입니다.

Q. 이 자가진단, 한 번만 하면 되나요?

아니요. 위협조직의 침투 경로와 AI 활용 수법이 계속 바뀌기 때문에, 최소 반기에 한 번은 같은 5개 영역을 다시 채점해보는 걸 권합니다.

관리자 계정부터 사고 대응까지 모든 장을 관통하는 메시지는 하나입니다. 방어선은 여러 겹이어야 하며, 예방 설정의 유무뿐 아니라 탐지 경보가 실제로 담당자에게 도달하는지, 격리된 사본으로 목표 시간 안에 복구되는지를 함께 시험해야 합니다.

기업 환경에서 빠뜨리기 쉬운 통제

이메일·엔드포인트 — 메일 게이트웨이와 첨부파일 샌드박스, SPF·DKIM·DMARC, 인터넷에서 내려받은 Office 매크로 차단을 적용합니다. EDR 또는 Microsoft Defender의 ASR 규칙을 단계적으로 배포하고 탐지·차단 결과를 중앙에서 확인합니다.

Active Directory·관리 접속 — 관리자용 계정과 업무용 계정을 분리하고, LAPS로 로컬 관리자 암호를 장비별로 관리합니다. 특권 작업은 PAW·PAM과 승인된 Jump Server를 통하며, RDP는 RD Gateway·Remote Credential Guard·JIT/JEA 등으로 노출 시간과 자격 증명 전달을 줄입니다.

중앙 로그·VSS 탐지 — 서버별 이벤트 뷰어 확인에 의존하지 말고 SIEM으로 Windows 로그인(4624·4625), 서비스 설치(7045), VSS·백업 카탈로그 삭제와 보안 도구 무력화 징후를 수집·경보합니다. 필요하면 Sysmon으로 프로세스·네트워크·지속성 가시성을 보강합니다.

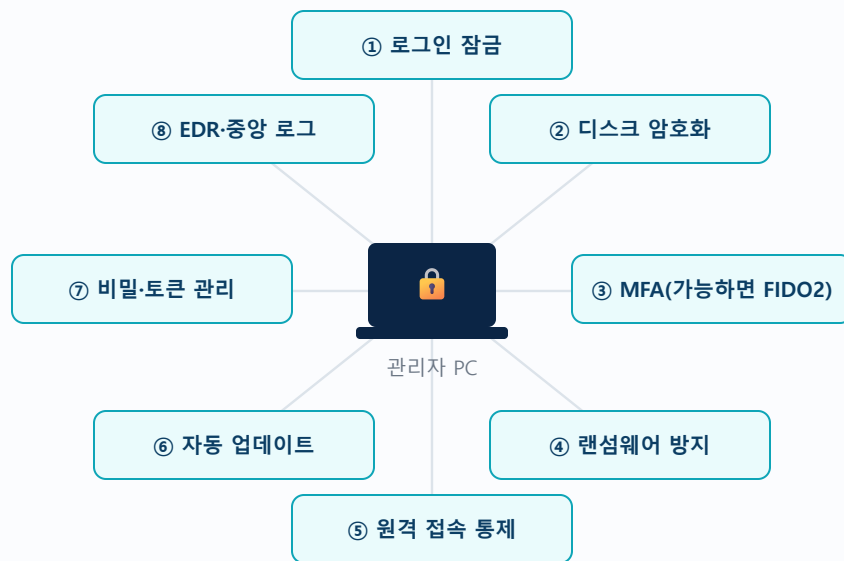
SaaS·클라우드 — 패스키·WebAuthn과 조건부 접근을 적용하고 전역 관리자 역할을 최소화합니다. 감사 로그 보존, OAuth 앱 권한 검토, SaaS 데이터의 별도 백업과 복구 테스트를 운영합니다. 클라우드 제공자의 고가용성과 고객 데이터 복구 책임은 같은 개념이 아닙니다.

사고 대응·재구축 — 법무·개인정보·경영진·보험·고객 통지 담당을 사전에 정합니다. 복구는 깨끗한 환경 재구축 → 자격 증명 전면 교체 → 최초 침투 원인과 지속성 제거 → 백업 무결성 검사 → 단계적 재연결 순으로 진행하며, 데이터 유출·공개 협박 대응은 암호화 복구와 별도 트랙으로 관리합니다.

[보너스] 관리자 PC 보안 강화 체크리스트

서버·백업망을 아무리 잘 지켜도, 그 모든 설정을 관리하는 담당자의 PC 한 대가 뚫리면 전부 무너질 수 있습니다. 관리자 개인 컴퓨터부터 점검하는 8가지 체크리스트입니다.

지금까지 서버·네트워크·백업 관점의 방어선을 다뤘다면, 마지막으로 짚어야 할 건 이 모든 설정을 실제로 만지는 사람의 컴퓨터입니다. 관리자 PC 한 대가 악성코드에 감염되면, 거기 저장된 원격 접속 정보·비밀번호·API 키가 그대로 공격자 손에 넘어가고, 지금까지 쌓아 올린 방어선이 안에서부터 뚫릴 수 있습니다.



서버는 지켜도 이 PC 한 대가 뚫리면 안에서부터 무너집니다

관리자 PC 8대 보안 체크포인트 인포그래픽

✓ 관리자 PC 보안 체크리스트

- **로그인 잠금** — Windows 로그인에 암호/PIN이 걸려 있고, 화면보호기가 5분 이내 자동 잠금으로 설정돼 있는지 확인하세요.
- **디스크 암호화** — 노트북이나 PC의 시스템 드라이브에 운영체제가 지원하는 디스크 암호화가 적용돼 있는지 확인하세요. 분실·도난 시 데이터 자체가 보호됩니다.
- **MFA** — **가능하면 FIDO2/passkey** — 업무에 쓰는 클라우드·이메일·개발자 콘솔 계정에 전부 다중 인증이 켜져 있는지 확인하세요. 문자 OTP도 없는 것보다는 낫지만, 피싱 저항성이 있는 FIDO2·패스키가 마지막 방어선으로 더 안전합니다.
- **랜섬웨어 방지 기능** — Windows Defender의 "제어된 폴더 접근"(랜섬웨어 방지) 기능을 켜고, 업무 폴더를 보호 대상에 추가하세요.
- **원격 접속 통제** — 원격 데스크톱(RDP)을 쓰지 않는다면 꺼두고, 쓴다면 반드시 사설망(VPN)을 통해서만 접근되도록 제한하세요.
- **자동 업데이트** — Windows·주요 소프트웨어의 자동 업데이트가 켜져 있는지 확인하세요. 알려진 취약점은 패치만으로 막을 수 있습니다.
- **비밀·토큰 관리** — 장기 API 키 대신 단기 토큰과 비밀 저장소를 사용하고, 가능한 경우 자동 순환하세요. 유출이 의심되면 정해진 날짜를 기다리지 말고 즉시 폐기·재발급합니다.
- **EDR·중앙 로그** — 작업 관리자를 가끔 보는 방식에 의존하지 말고 EDR 경보, 프로세스·예약 작업·자동 실행 등 지속성 지점, 인증·관리 행위를 중앙에서 지속적으로 모니터링하세요.

서버는 방화벽과 EDR로 지키면서 정작 그 서버를 관리하는 사람의 노트북은 무방비인 경우가 뜻밖에 많습니다. 8가지 중 지금 안 되어 있는 항목이 있다면, 오늘 하나씩만 켜보시길 권합니다.

마치며

관리자 계정 보호에서 시작해 외부 통로 차단, 서버 경화, 네트워크 분리, 백업 전략, 골든타임 대응, 그리고 자가진단까지 다뤘습니다. 각 통제는 운영체제·하드웨어·애플리케이션 호환성과 조직의 위험 수준을 확인한 뒤 시험군부터 단계적으로 적용해야 합니다.

다만 어떤 단일 통제도 관리자 권한 탈취 이후의 모든 공격 경로를 차단하지는 못합니다. 그래서 마지막 질문은 늘 같은 곳으로 돌아옵니다 — **운영 계정이 침해돼도 복구 사본에 이르는 경로와 권한을 충분히 분리했는가.**



이 가이드가 도움이 되셨다면

비슷한 고민을 하는 동료, IT 커뮤니티, 사내 보안 교육 자료로 자유롭게 공유해 주세요. 기업 IT 담당자 및 사이버보안 담당자일수록 이런 정보가 늦게 닿는 경우가 많습니다. 공유한 번이 누군가의 회사를 지킬 수 있습니다.

무료 배포

출처 표기 시 재배포 자유

상업적 재판매 금지

이 가이드를 만든 회사 소개



D-FORTRESS

Zero Trust Backup

이 가이드는 (주)락게이트코어가 무료로 제작·배포합니다. 앞선 7개 장의 조치와는 별개로, 회사가 만드는 하드웨어 백업 보안 제품 D-FORTRESS를 참고용으로 한 페이지 소개합니다.

6장에서 다룬 3-2-1-1-0 백업과 불변 스토리지는 대부분 소프트웨어·설정으로 구현됩니다. 다만 소프트웨어 기반 통제는 결국 관리자 권한이라는 하나의 지점으로 수렴하고, 그 권한이 탈취되면 보존 잠금 설정 자체도 함께 뚫릴 위험이 남습니다. D-FORTRESS는 이 지점을 하드웨어로 끊어내는 접근입니다. 이중 데이터 다이오드(Dual Data Diode)로 운영망과 백업 금고 사이의 통신 회로 자체를 물리적으로 분리해, 데이터는 들어갈 수 있어도 반대 방향으로 어떤 명령도 통과할 수 없게 만듭니다.

관리자 계정이 탈취돼 "백업 삭제" 명령이 내려와도, 백업을 보관하는 서버(RX)에는 애초에 외부 명령을 수신할 수 있는 물리적 역방향 채널이 없어 삭제나 암호화 자체가 원천적으로 불가능합니다. 설령 랜섬웨어 악성코드가 백업 서버로 넘어오더라도 이를 실행시킬 양방향 통신 세션이 형성되지 않아 무해한 데이터 덩어리로만 보관됩니다. 또한, 기존 단방향 통신의 한계였던 패킷 유실 문제는 별도로 물리 분리된 '재전송 요청 전용 회로'를 통해 해결하여, 대용량 데이터도 지연 없이 10Gbps급 초고속 무손실로 동기화 및 즉각 복구(Zero RTO)가 가능합니다.

뚫는 것을 막는 대신, 들어올 길 자체를 없앴습니다

디포트리스는 외부에서 해커가 침입할 양방향(TCP/IP) 침입 경로 **자체를 물리적으로 제거**한 데이터 금고입니다.

해커가 최고관리자 권한을 탈취해도 **백업 데이터 파괴(삭제 및 암호화) 자체가 불가능**합니다. (관리자도 데이터를 네트워크 상에서 삭제/변경 불가)



1

이중 데이터 다이오드

외부에서 해커가 접속해 들어오는 침입 경로를 **물리적으로 단절**합니다.

2

네트워크 스텔스 + 프로토콜 브레이크

네트워크에서 탐지되지 않아 해커가 침입할 수 없고, 양방향 세션이 끊겨 악성 코드를 실행시킬 수 없습니다.

3

제로 트러스트 스토리지 기능

해커뿐만 아니라 관리자도 네트워크를 통해서는 데이터를 **수정·삭제**할 수 없습니다.

기존에 구축한 백업 시스템을 교체할 필요는 없습니다. 백업망 최후단에 추가로 배치해 그 뒤를 물리적으로 봉인하는 방식이라 네트워크 구성 변경이나 서비스 중단 없이 도입됩니다. 표준 TCP/IP 환경, Windows·Linux·macOS·Unix, 파일 서버·DB 서버·VMware 가상화까지 폭넓게 연동되며, ISMS-P·금융보안원의 백업망 분리·오프라인 소산 백업 요건 대응에도 활용됩니다. 소규모 사업장용 Basic부터 금융권·대규모 데이터센터용 Enterprise까지 라인업이 나뉘어 있고, 장비 구매(구축형)와 월 구독형 중 선택할 수 있습니다.

D-FORTRESS 3대 핵심 가치

세 겹의 방어로 구축하는 기업의 최종 방어선



물리적 망분리 (Physical Air-Gap)

하드웨어 수준의 일방향 격리를 통해 공격 표면(Attack Surface)을 원천적으로 제거합니다.



데이터 무결성 (Data Integrity)

제로 트러스트 아키텍처 기반으로, 최고 관리자도 백업 데이터의 임의 수정 및 삭제가 불가능합니다.



비즈니스 연속성 (Zero RTO)

사고 발생 즉시 사전에 무결성이 검증된 데이터를 복구하여 비즈니스 다운타임을 최소화합니다.

이 가이드와 D-FORTRESS에 대해 더 알고 싶다면 dfortress.kr에서 확인하실 수 있습니다.



D-FORTRESS

Zero Trust Backup

ROCKGATE
CORE

(rockgatecore.com / dfortress.kr)

랜섬웨어 예방 가이드

제작·배포: (주)락게이트코어

초판: 2026년 8월 · 개정판: 2026년 9월

본 전자책은 정보 공유 목적의 무료 배포용이며, 출처 표기 시 자유롭게 재배포하실 수 있습니다.