

# 리스크 방어 및 예방과 킬체인 차단

Akamai Guardicore Segmentation으로 랜섬웨어의 영향 최소화



## 개요

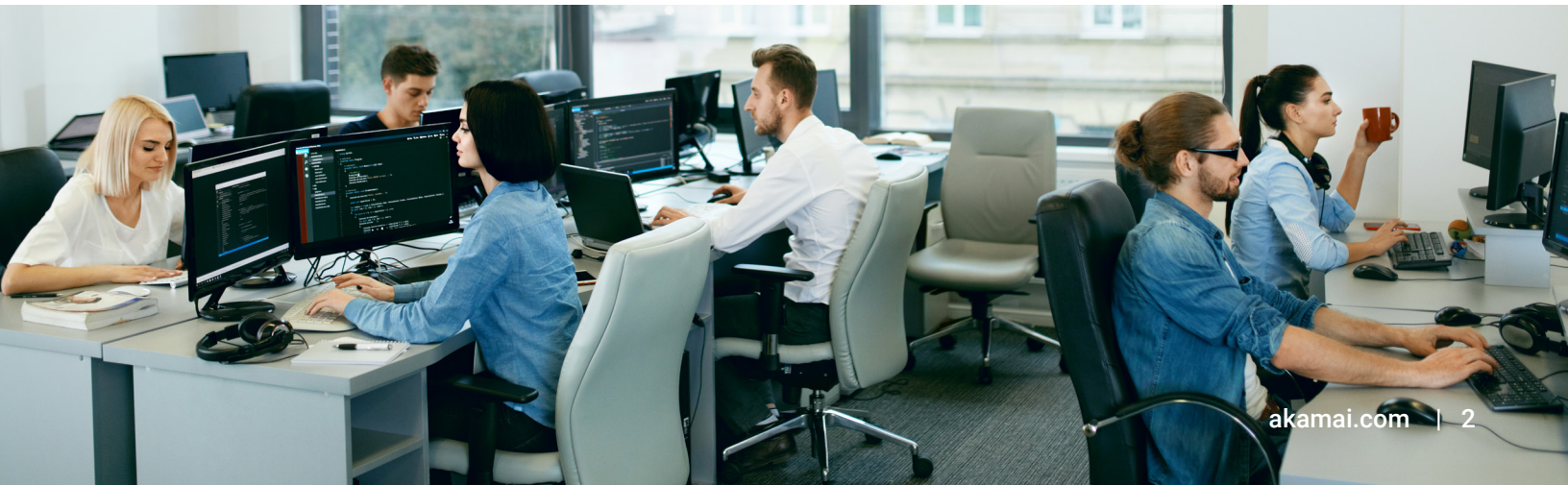
랜섬웨어는 한때 사이버 범죄자들이 암호화를 통해 파일 및 데이터 접속을 제한하기 위해 사용하는 멀웨어의 성가신 변종에 불과했지만, 지금은 훨씬 더 심각한 것으로 변했습니다. 영구적인 데이터 손실의 위협도 충격적이지만, 사이버 범죄자와 국가의 지원을 받는 해커들은 랜섬웨어를 이용해 대기업, 연방 정부, 글로벌 인프라, 헬스케어 기관에 침투해 마비시킬 정도로 정교해졌습니다.

2017년 Microsoft Windows의 취약점을 악용하여 전 세계 23만 대의 컴퓨터를 공격한 WannaCry 랜섬웨어로 랜섬웨어의 위협에 대한 경각심이 높아졌습니다. 그 이후 공격자들은 점점 더 정교해지고 공격도 더욱 확산했습니다. 여기에는 해커가 서비스를 판매하는 서비스형 랜섬웨어(RaaS)의 출현도 포함됩니다. [Akamai의 랜섬웨어 위협 보고서, H1 2022](#)는 2020년에 처음 탐지되었으며 러시아에 기반을 둔 것으로 보이는 악명 높은 RaaS 그룹 Conti의 공격 패턴을 평가했습니다. 이 분석은 측면 이동에 대비한 강력한 보호가 필요하고 이러한 보호가 랜섬웨어로부터 방어하는 데 중요한 역할을 할 수 있다는 것을 시사합니다. 또한 Conti 피해자의 압도적인 다수가 매출 규모가 천만~2억 5천 만 달러인 기업이라는 사실도 밝혀졌습니다.

**마이크로세그멘테이션은 정책에 의해 명시적으로 정의된 연결만 허용하여 네트워크의 암시적 신뢰를 줄임으로써 애플리케이션 전반에 머신 간 트래픽에 대해 최소한의 권한을 적용합니다.**

- Forrester, [제로 트러스트 마이크로세그멘테이션 모범 사례, 2022년 6월 27일](#)

낡은 기술, 경계 및 엔드포인트에만 초점을 맞춘 "충분히 우수한" 방어 전략, 교육 부족 및 잘못된 보안 관례, 알려진 "특효" 솔루션이 없는 상황 등이 종합적으로 원인이 되어 모든 규모의 기업이 리스크에 처해 있음을 분명히 알 수 있습니다. 사실, [Cybersecurity Ventures Who's Who In Ransomware: 2023 보고서](#)에 따르면 2031년까지 랜섬웨어가 2초에 한 번씩 기업, 소비자 또는 디바이스를 공격할 것으로 예상됩니다.



## 성패를 가르는 요소, 측면 이동

랜섬웨어 공격은 피싱 이메일, 네트워크 경계의 취약점, 무차별 대입 공격 등 최초의 보안 침해로부터 시작되며 공격자의 실제 의도와 무관하게 보안 체계를 무너뜨립니다. 일단 멀웨어가 디바이스나 애플리케이션에 침입하면 네트워크와 여러 엔드포인트에서 권한 확장 및 측면 이동을 통해 감염과 암호화 포인트를 극대화합니다. 공격자는 일반적으로 도메인 컨트롤러를 장악하고 인증정보를 감염시킨 후에 백업을 찾아 암호화해 운영자가 중단된 서비스를 복원하지 못하도록 합니다.

측면 이동은 공격 성공에 매우 중요합니다. 멀웨어가 도착 지점을 넘어서 확산할 수 없다면 무용지물이 됩니다. 따라서 측면 이동 방지가 필수적입니다. Akamai Guardicore Segmentation과 같은 솔루션의 가시성 및 세그멘테이션 기능을 사용하면 초기 유출을 방지하고 억제하는 정책을 신속하게 설정할 수 있습니다. 또한 측면 이동과 기타 의심스러운 행동에 대한 알림을 통해 멀웨어를 조기에 탐지하고 즉각적으로 대응할 수 있습니다.

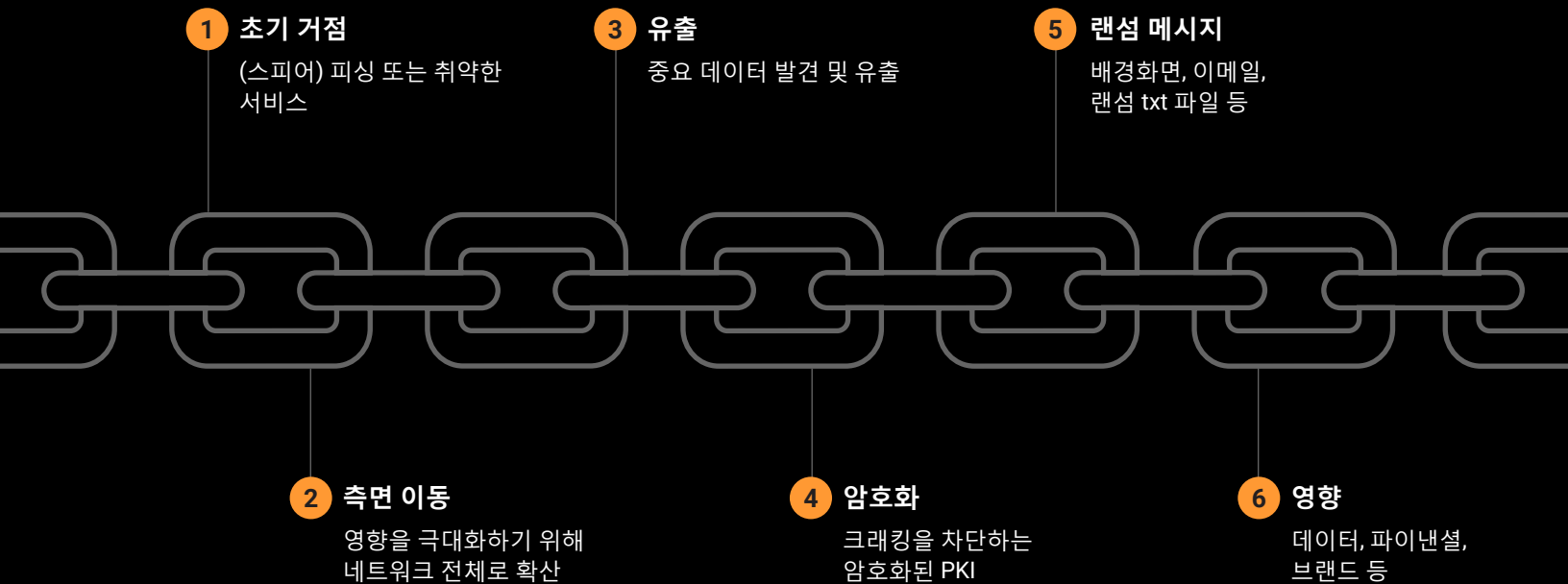


# 1부: 랜섬웨어 킬체인 차단 - 리스크 방어 및 예방

하나의 머신 또는 디바이스가 감염되었다고 랜섬웨어가 확산되지는 않습니다. 사이버 범죄자들은 랜섬웨어를 이용해 최대한 많은 네트워크상의 시스템을 암호화하여 랜섬을 갈취합니다.

랜섬웨어는 다면적인 공격이므로 멀티 레이어 방어를 구축하면 광범위한 피해, 데이터 손실, 다운타임을 방지할 수 있습니다. 첫 번째 방어 레이어는 초기 랜섬웨어 감염을 예방하는 것입니다.

## 랜섬웨어 킬체인



## 초기 감염 예방

모든 네트워크에서 첫 번째 취약 지점은 인터넷과 연결되는 지점입니다. 많은 랜섬웨어 공격이 스피어 피싱에 의존하지만 인터넷에 노출된 서비스 침해를 막아줄 수 있는 것은 없습니다.

Akamai Guardicore Segmentation의 가시성 기능을 통해 인터넷에 노출된 서비스를 모니터링하고 다음과 같은 정책을 통해 노출을 제한할 수 있습니다.

- 원격 접속 서비스(RDP, SSH, TeamViewer, AnyDesk, VPN)
- 잠재적으로 취약한 서비스(Apache, IIS, Nginx)
- 잠재적으로 취약한 머신(추가 인사이트 기능을 사용하여 패치되지 않은 운영 체제를 사용하는 머신 탐지)
- 원치 않게 노출된 서비스(데이터베이스, 도메인 컨트롤러, 내부 웹 또는 파일 서버)

## 세그멘테이션을 이용한 킬체인 차단

네트워크 침해를 100% 피할 수는 없습니다. 네트워크 침해는 스피어 피싱, 사람의 실수, 제대로 방어하지 못한 취약한 서비스의 실행 등으로 발생합니다. 따라서 적절한 리스크 방어 전략을 마련하는 것이 매우 중요합니다.

일단 머신이 침해되면 네트워크 내부에서 전파되는 것을 차단해야 하는데 다음과 같은 3가지 방법을 통해 가능합니다.

### 1. 애플리케이션 링펜싱을 통한 세그멘테이션

네트워크를 애플리케이션, 사용, 환경에 따라 운영 세그먼트로 분리하고 세그먼트와 세그먼트 사이 그리고 세그먼트 내부에서 불필요한 연결을 허용하지 않아야 합니다.

**이 때 다음과 같은 4가지 세그멘테이션 가이드라인을 고려해야 합니다.**

- 노트북·워크스테이션 사이의 모든 통신을 차단합니다.
- 도메인 관리자와 같은 "강력한" 도메인 사용자 권한을 실행하는 프로세스에서 보내는 통신을 차단합니다.
- 서버에서 프로세스를 실행할 수 있는 사용자를 제한합니다.
- 노트북 및 워크스테이션에서 데이터 센터 서버 및 클라우드 인스턴스로의 접속을 제한합니다.



Akamai Guardicore Segmentation은 랜섬웨어로부터 네트워크를 쉽게 보호할 수 있도록 지원합니다. 사전 구축된 템플릿을 사용하면 다음과 같이 간단한 세 단계로 정책을 설정하여 공격을 방어할 수 있습니다.

1. 중요한 애플리케이션 링펜싱, 랜섬웨어 방어 정책 생성, Active Directory 보안 등의 원하는 **목표를 선택하세요.**
2. 링펜스하려는 이커머스 애플리케이션 자산, 데이터 센터의 모든 Active Directory 워크로드, 랜섬웨어 확산으로부터 보호해야 하는 엔드포인트 등 **보호해야 하는 관련 자산을 확인하세요.** 대부분의 경우 이 단계는 Akamai의 AI 레이블링을 통해 자동으로 진행됩니다.
3. **정책을 만들어 자산을 보호하세요.** Akamai Guardicore Segmentation의 AI는 환경의 실제 트래픽을 기반으로 정책을 자동으로 제안 및 추천하며 수백 개의 네트워크에서 애플리케이션의 통신 패턴을 학습합니다.

|  |  |   |   |
|--|--|---|---|
| <p>Ra</p> <p>Create Ransomware Response - File Share Restrictions</p> <p>#ransomware #template</p> | <p>Ra</p> <p>Create Ransomware Recovery and Response Policies</p> <p>#ransomware #template</p> | <p>Ma</p> <p>Create Malware Response - Lateral Movement Mitigation Policies</p> <p>#malware #template</p> | <p>Apply Zero Trust Application Security on application</p> <p>#diy #zero trust</p> |
| <p>Application Tier-Segmentation by whitelisting flows bet...</p> <p>#diy</p>                      | <p>Ringfence an Application by whitelisting inbound a...</p> <p>#diy</p>                       | <p>Whitelist Outbound Flows for an application</p> <p>#diy</p>  | <p>Control Privileged Access to environment from jumpboxes</p> <p>#diy</p>          |

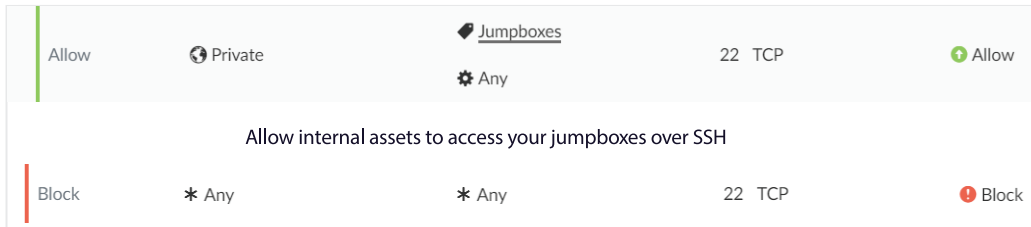
예: Akamai Guardicore Segmentation 템플릿



## 2. 프로토콜 제한 룰을 이용한 측면 이동 방지

특정 프로토콜 및 행동에 대한 일반적인 가이드라인이 있습니다. 일상적인 운영에 기본적으로 사용되는 프로토콜이 있기 때문에 일부를 신중하게 제한해야 합니다. Akamai Guardicore Segmentation을 사용하면 모든 트래픽을 시각화해 WinRM, SMB, RPC, RDP, SSH 등과 같은 리스크가 높은 프로토콜을 중심으로 환경에 가장 정확한 룰을 생성할 수 있습니다.

예를 들어 SSH는 원격 관리에 유용하며 sFTP와 같은 다른 프로토콜을 안전하게 만드는 데 사용되지만 공격자가 머신을 감염시키고 네트워크에 전파할 때 사용하는 툴이기도 합니다. 권한 있는 사용자를 위한 점프 박스를 생성해 네트워크 전체의 SSH를 최대한 제한할 수 있습니다.



Akamai Guardicore Segmentation에서 생성된 룰

## 3. 백업 및 중요 데이터 서비스 보호

랜섬웨어 공격은 피해를 극대화하기 위해 일반적으로 기업의 백업 서버를 표적으로 저장된 데이터를 암호화합니다. 이와 유사하게 데이터 서비스와 파일 서버가 랜섬웨어의 표적이 됩니다.

Akamai Guardicore Segmentation을 사용하면 백업 서버, 데이터베이스, 파일 서버에 대한 접속을 제한하고 네트워크 외부 및 접속이 필요하지 않은 네트워크 내부의 영역으로부터 접속을 제한할 수 있습니다. 중요한 백업 서버와의 통신을 최소화하기 위해 Akamai Guardicore Segmentation을 사용해 애플리케이션에 링펜스를 적용하고 애플리케이션에서 프로세스, 사용자 수준까지 통신을 차단할 수 있습니다. 데이터 서비스의 노출을 운영에 필요한 최소한의 수준으로 제한하면 해당 서비스에 대한 리스크 요소가 줄어들고 랜섬웨어 노출 및 전파 경로를 방어할 수 있습니다.

## 2부: 랜섬웨어 탐지 및 대응

랜섬웨어와 같은 사이버 위협에 대처하려면 사전 계획과 경계하는 태도가 필요합니다. 보안 침해에 신속하게 대응함으로써 네트워크 피해를 최소화할 수 있습니다. Akamai Guardicore Segmentation은 위협 탐지 및 대응을 모두 지원할 수 있는 기능을 갖추고 있습니다.

### Akamai Guardicore Segmentation을 통한 위협 탐지

인시던트에는 다음이 포함됩니다.

- **디셉션** - 의심스러운 측면 이동 시도를 탐지해 가로챈 다음 동적 허니팟으로 리디렉션해 행동을 모니터링하고 분석할 수 있습니다. 디셉션 인시던트는 매우 정확해서 악성 활동 및 사이버 범죄자의 다음 공격 단계에 대한 자세한 데이터를 제공합니다.
- **네트워크 스캔** - 사이버 범죄자들은 일단 네트워크 내부에 침투하면 인텔리전스를 수집합니다. 네트워크 스캔을 정찰 방법으로 사용해 다른 서버가 리스닝하는 열린 포트 또는 서비스를 탐지합니다. Akamai Guardicore Segmentation은 자동으로 네트워크 스캔을 탐지해 사용자에게 즉시 알립니다.
- **정책 기반 탐지** - 네트워크 및 프로세스 수준의 보안 정책을 통해 무단 통신 및 규정을 준수하지 않는 트래픽을 즉시 인식할 수 있습니다.

### Akamai Guardicore Segmentation, 인사이트 기능 발표

Akamai Guardicore Segmentation은 OSQuery에 기반한 추가 기능을 활용하여 개별 자산에 대한 가시성을 제공할 수 있습니다. 이 쿼리 프레임워크는 랜섬웨어의 가장 일반적인 사전 암호화 조치인 Volume Shadow Copy 탐지 같은 비정상적인 활동을 빠르게 탐지합니다. 또한 정상적인 Windows 프로세스인 svchost.exe에 멀웨어를 숨기는 일반적인 공동화 기법을 검색해 랜섬웨어 전달에 사용되는 트로이 목마를 탐지할 수도 있습니다.

### 관리형 위협 탐지

관리형 위협 탐지 서비스인 Akamai Hunt는 네트워크 내부의 비정상적인 행동을 사용자에게 알려줍니다. 이 작업은 수신 및 발신 인터넷 연결과 관련 GeolIP 분석, 전파를 나타낼 수 있는 네트워크 프레전스(Presence)가 증가하는 새로운 실행 파일 검색, 인접 카운트(Neighbor-Count) 비정상 활동(Anomaly)을 통해 측면 이동의 징후를 발견하는 자산 연결 분석 등과 같은 기법을 통해 이루어집니다.

### 즉각적인 대응

네트워크 내부에서 랜섬웨어와 같은 위협을 탐지하면 프로세스 및 사용자 수준에서 정책을 적용하고 방어 조치를 신속하게 배포함으로써 악성 활동을 적극적으로 거부하고 발생하지 않도록 분리합니다.





### 증가하는 감염 가시성

감염의 초기 단서나 지표(IOC)를 이용해 통신 패턴, 프로세스, 사용된 포트, 감염된 자산 등과 같은 추가 지표를 찾기 시작할 수 있습니다. Akamai Guardicore Segmentation을 사용해 이 지표가 포함된 모든 자산(C2와 통신하는 모든 자산, 고유 포트로 통신하는 모든 자산 또는 악성 프로세스를 실행하는 모든 자산)을 찾는 데 도움을 줄 수 있습니다. 또한 환경의 비주얼 맵 내에서 감염된 머신들이 갖고 있는 유사성이나 전파 흔적을 찾을 수 있습니다.

## 3부: 감염 제거 및 복구

일단 감염된 모든 머신과 IOC의 목록을 확보하면 감염 제거를 시작할 수 있습니다. 머신을 **격리**, **모니터링**, **복구**라는 세 가지 라벨 그룹으로 나눕니다.

### 격리

- 멀웨어에 **감염**된 자산
- 멀웨어를 제거할 때까지 해당 자산을 **격리**

### 모니터링

- **감염**여부가 불확실한 자산
- 멀웨어 **제거**를 확인할 때까지 **모니터링**

### 복구

- **감염되지 않은** 것으로 확인되어 **정상 운영**할 수 있는 자산

## 복구를 위한 세그멘테이션 가이드라인

3개의 라벨 그룹을 설정한 후 다음과 같은 4개의 통신 계층을 생성해 네트워크를 분할하는 정책을 추가할 수 있습니다.

- **격리**된 머신으로부터의 모든 수신 및 발신 통신을 **차단**합니다.
- **모니터링**되는 머신의 원격 관리 프로토콜 통신을 **차단**합니다.
- 머신을 **복구**하기 위해 모든 원격 관리 프로토콜 통신에 대한 **알림**을 제공합니다.
- 라벨 그룹 간의 모든 통신을 **차단**합니다.

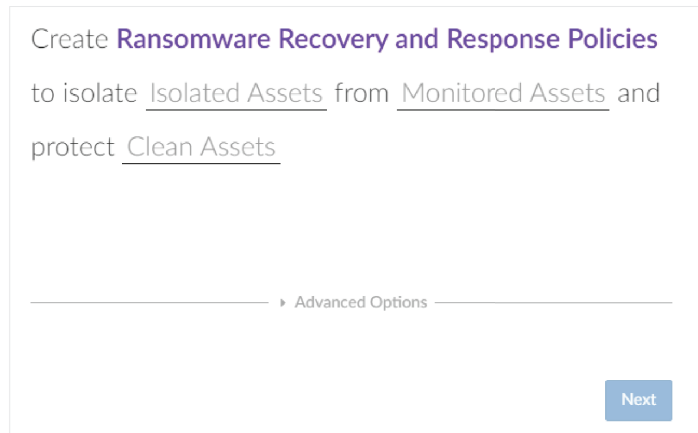
|                |                  |                  |                           |
|----------------|------------------|------------------|---------------------------|
| Override Alert | * Any            | <u>Clean</u>     | 5985, 5986 ... TCP   UDP  |
| Override Block | <u>Monitored</u> | <u>Clean</u>     | Any TCP   UDP             |
| Override Block | <u>Clean</u>     | <u>Monitored</u> | Any TCP   UDP             |
| Override Block | <u>Monitored</u> | * Any            | 5985, 5986 ... TCP   UDP  |
| Override Block | * Any            | <u>Isolated</u>  | Any TCP   UDP<br>Any ICMP |
| Override Block | <u>Isolated</u>  | * Any            | Any TCP   UDP<br>Any ICMP |

Akamai Guardicore Segmentation의 차단 및 알림 룰

## 랜섬웨어 복구 및 응답 템플릿

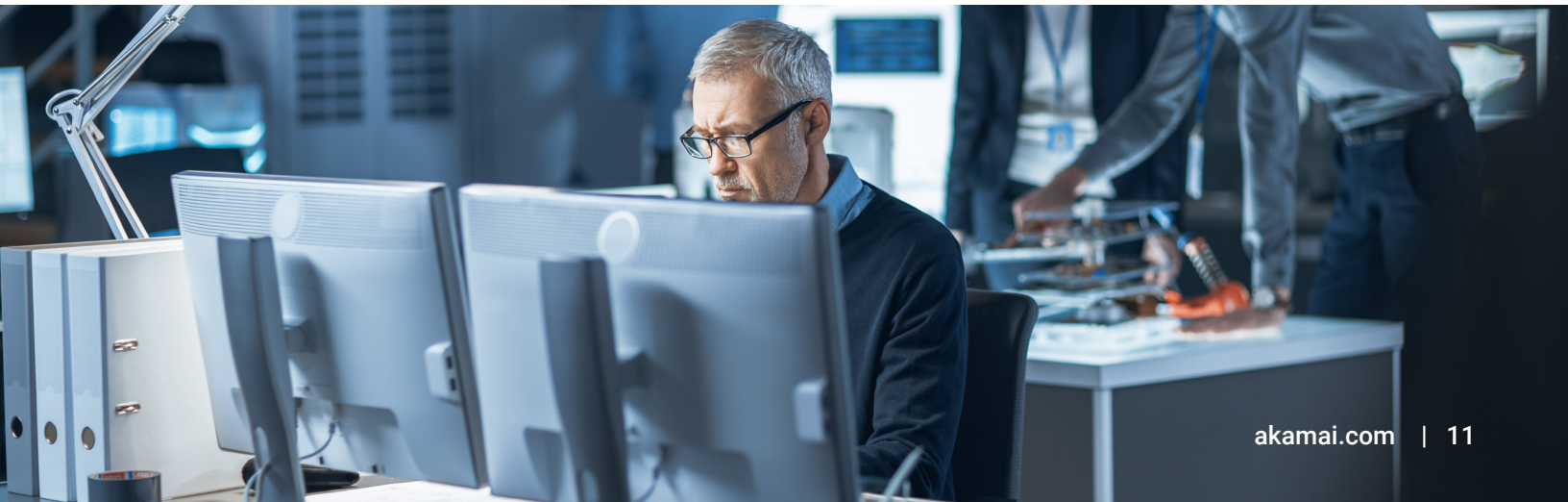
Akamai Guardicore Segmentation에 포함된 랜섬웨어 복구 및 응답 정책 템플릿은 격리, 모니터링, 복구 라벨의 접속을 제한하기 위해 사용하기 쉽고 미리 만들어진 정책을 제공합니다.

이 템플릿을 사용하면 격리된 머신으로부터의 (재)감염 리스크에 대한 우려 없이 복구된 머신의 운영 연속성을 쉽게 유지할 수 있습니다.



## 결론






레거시 방화벽이나 경계 전용 방어를 계속 사용하고 있다면 랜섬웨어가 네트워크 전체에 확산하여 중요한 애플리케이션과 인프라가 락다운되는 상황을 막을 수 없습니다. 실제로 유출은 피할 수 없으며 이에 대비해야 하는 것이 현실입니다. Akamai Guardicore Segmentation은 동서 데이터 센터 트래픽의 위협을 탐지하고 랜섬웨어가 가장 중요한 자산을 암호화하고 랜섬웨어에 의존하는 측면 이동을 차단하도록 지원합니다.







## Akamai Guardicore Segmentation을 이용해 랜섬웨어의 영향을 방어하는 5단계

-  IT 환경에서 실행되는 모든 애플리케이션과 자산을 탐지해 **준비**
-  일반적인 랜섬웨어 전파 기법을 차단하는 룰을 만들어 **예방**
-  세그먼트화된 애플리케이션 및 백업에 대한 접속 권한을 얻으려는 모든 시도에 대한 알림을 수신하여 **탐지**
-  공격 탐지 시 위협 차단 및 격리 조치를 시작하여 **문제 해결**
-  단계별 복구 전략을 지원하는 시각화 기능으로 **복구**

네트워크에서 랜섬웨어의 측면 이동을 막으세요.  
믿기 어려우신가요? 직접 확인해 보십시오. [akamai.com/guardicore](https://akamai.com/guardicore)



Akamai는 서비스를 구축하고 제공하는 위치에 상관없이 보안 기능을 내장함으로써 고객 경험, 인력, 시스템 및 데이터를 보호합니다. Akamai 플랫폼은 글로벌 위협에 대한 가시성을 바탕으로 제로 트러스트 지원, 랜섬웨어 차단, 앱 및 API 보안 또는 DDoS 공격 차단을 목표로 보안 체계를 조정하고 발전시켜 지속적으로 안심하고 혁신하고 확장하며 가능성을 현실로 구현할 수 있습니다. Akamai의 보안, 컴퓨팅, 전송 솔루션에 대한 자세한 정보는 [akamai.com](https://akamai.com) 및 [akamai.com/blog](https://akamai.com/blog)를 방문하거나 [Twitter](#) 및 [LinkedIn](#)에서 Akamai Technologies를 팔로우하세요. 2023년 05월 발행.