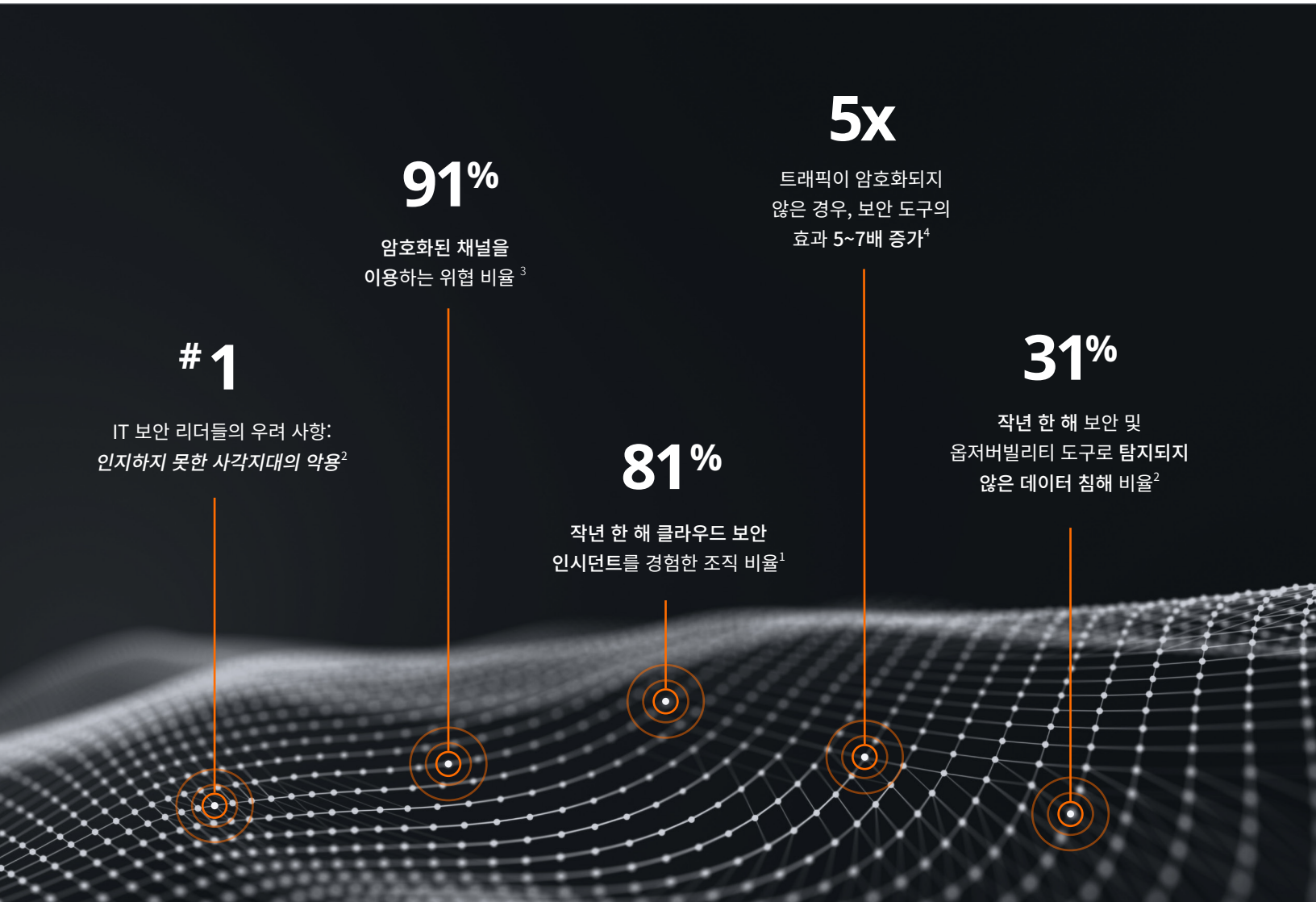
# Precryption™을 통한 대규모 사각지대 제거

Gigamon Precryption 기술은 측면 트래픽이 암호화되기 전 분석해 가상, 클라우드, 컨테이너를 포함한 전체 보안 스택에 평문에 대한 가시성을 제공합니다. 따라서 복호화가 필요하지 않습니다.



Gigamon Precryption™ 기술은 통신이 암호화되기 전 분석하여 전통적으로 복호화에 수반되는 비용 및 복잡성 없이 전체 보안 스택에 평문에 대한 가시성을 제공할 수 있도록 가상, 클라우드 및 컨테이너화된 애플리케이션의 보안을 재정의합니다.

**정보 보안 관련 어려움**

1. 클라우드 도입 증가
2. 개발팀의 촉박한 일정
3. 숨겨진 위협 활동

오늘날 암호화된 통신은 거의 모든 최신 하이브리드 클라우드 인프라 전반에서 사용되며 전통적인 감청 기술로부터 민감 데이터를 보호합니다. 위협 행위자들은 민감 데이터에 접근하기 위해 새롭고 보다 정교한 침투 방식을 통해 주요 시스템을 손상시킵니다. 이들은 이제 동일한 암호화 통신 채널을 사용해 특히 측면 이동, 민감 데이터 액세스 및 유출과 같은 활동을 은폐하고 있습니다. 기존 시판 솔루션으로는 가상 워크로드 간에 측면으로 이동하는 트래픽이 암호화되기 전에 평문에 대한 가시성을 확보하는 것이 거의 불가능합니다. 따라서 숨겨진 위협 활동의 탐지 역시 매우 어려워지고 암호화된 측면 통신은 대규모 보안 사각지대로 남아 있게 됩니다.

## 숨겨진 위협 활동을 탐지하는 Precryption 기술

Precryption 기술은 오늘날 하이브리드 클라우드 인프라에 존재하는 최대 사각지대, 즉 TLS 1.3과 같은 최신 암호화 방식을 통해 난독화되는 위협 행위자의 측면 이동 문제에 대한 직접적인 해결책을 제시하는 혁신적인 솔루션입니다. Precryption은 많은 비용이 소요되는 복호화나 진행을 방해하는 복잡한 키 수집 및 관리 없이 가상 통신이 암호화되기 전 효율적이고 마찰이 없는 폼 팩터를 이용한 분석을 바탕으로 평문에 대한 가시성을 제공합니다.

## Precryption 기술의 작동 방식

Precryption 기술은 기본 Linux 기능을 활용해 OpenSSL 등의 암호화 라이브러리와 애플리케이션과 간 통신을 태핑 또는 복사합니다.


Precryption은 이러한 방식으로 암호화 전 또는 복호화 후에 네트워크 트래픽을 평문 형식으로 수집합니다. Precryption의 기능은 메시지의 실제 암호화나 네트워크 전송을 방해하지 않습니다. 또한 프록시, 재전송, 복호화 및 암호화의 반복(break-and-inspect)이 필요하지 않습니다. 대신 이 평문 사본은 Gigamon 딥 옵저버빌리티 파이프라인으로 전달되어 추가적인 최적화, 변환, 복제를 거치거나 다양한 도구로 전송됩니다.

Precryption 기술은 GigaVUE® Universal Cloud Tap(UCT)에 기반하며 온프레미스 및 가상 플랫폼을 포함한 하이브리드 및 멀티 클라우드 환경 전반에서 작동합니다.

또한 Precryption 기술과 UCT의 결합은 애플리케이션과 독립적으로 실행되고 애플리케이션 개발 수명주기에 통합될 필요가 없다는 추가적인 이점을 제공합니다.

## 주요 사용 사례

**사이버 범죄 완화:** 클라우드 내부의 측면 이동은 특히 사이버 범죄 공격에서 명백한 사각지대를 발생시킵니다. 일단 경계 보안을 통과한 후에는 암호화된 패킷에 대한 모니터링이 이루어지지 않으므로 위협 행위자는 다양한 트릭 및 기술을 활용해 탐지를 회피할 수 있습니다.

**TLS 1.3 규정 준수:** 오늘날 일부 조직은 TLS 1.3이 확실히 필요함에도 불구하고 암호화된 트래픽에 대한 가시성이 부족하다는 이유로 도입을 미루고 있습니다. 별도의 복호화 솔루션을 관리하는 것에 안주하는 조직도 있습니다.

**제로 트러스트:** 효과적인 제로 트러스트 아키텍처는 패킷을 확인하고 네트워크 리소스 간 모든 상호작용을 조사하며 정책을 적용하는 능력에 달려 있습니다.

**네트워크 유래 인텔리전스:** SIEM과 같은 보안 도구는 위협 탐지 능력의 개선을 위해 메타데이터 변환 및 보강에 의존하는 경우가 많습니다.

## Precryption을 선택해야 하는 이유

Precryption 기술이 적용된 GigaVUE Universal Cloud Tap은 최신 하이브리드 클라우드 인프라에 존재하는 사각지대를 제거하여 가상, 클라우드 및 컨테이너 플랫폼에 대한 동서(East-West) 가시성을 제공하는 마찰 없는 가벼운 솔루션입니다. 이제 IT 조직은 복호화 키를 관리 및 유지할 필요 없이 TLS 1.3을 포함한 모든 암호화 유형에 대해 명확한 가시성을 확보할 수 있으므로 규정 준수를 관리하고 프라이빗 통신의 기밀을 유지하고 제로 트러스트의 기본 토대를 설계하며 보안 도구의 효과를 5배 이상 개선하는 것이 가능합니다.

### 주요 기능

- **최신 암호화 방식**(TLS 1.3, mTLS, TLS 1.2 및 Perfect Forward Secrecy)**을 통해 통신이 암호화되기 전 분석해 평문에 대한 가시성을 제공**
- **기존 암호화 방식**(TLS 1.2 및 이전 버전)**을 통해 통신이 암호화되기 전 분석해 평문에 대한 가시성을 제공**
- 컨테이너 워크로드 내부에서 에이전트를 실행할 필요 없는 **비침입 방식의 트래픽 액세스**
- 전통적인 트래픽 복호화에 수반되는 **고비용 리소스 소비 제거**
- 전통적인 트래픽 복호화에서 **요구되는 키 관리 제거**
- 암호 유형, 강도 또는 버전에 따른 **성능 영향 부재**
- 온프레미스, 가상, 컨테이너 플랫폼을 포함한 **하이브리드 및 멀티 클라우드 환경 전반에 걸친 지원**
- 보안 도구에 평문 형식으로 수집한 위협 활동 정보를 전달하여 네트워크 전반에서 **프라이빗 통신의 기밀 유지**
- **Gigamon 딥 옵저버빌리티 파이프라인과의 통합**을 바탕으로 완벽한 최적화, 변환 및 브로커 기능 제공

### 주요 이점

- 방화벽을 통과할 수 없는 트래픽을 포함한 암호화된 동서(측면) 및 남북(North-South) 통신의 **사각지대 제거**
- 개발팀의 속도를 높이는 독립적인 접근 방식에 기반한 **애플리케이션 통신 모니터링**
- 암호화 유형과 무관하게 모든 통신에 대한 **보안 도구의 가시성 확장**
- 가상 환경 전반에 걸친 **최대한의 트래픽 태핑 효율성 달성**
- 암호화되지 않은 데이터 사용을 통해 **5~7배 강화**된 보안 도구 성능 활용
- 딥 옵저버빌리티에 기반한 **제로 트러스트 아키텍처 지원**
- 복호화된 트래픽 관리와 관련된 **개인정보 보호** 및 규정 준수 유지

## 관련 어려움: 자세히 살펴보기

오늘날 IT 조직은 해당 조직의 책임 하에 있는 시스템 및 데이터의 보안 유지와 관련해 가상 및 클라우드 도입 증가, 개발팀의 촉박한 일정, 숨겨진 위협 활동이라는 3가지 중대한 어려움을 마주하고 있습니다.

### 1. 가상 및 클라우드 도입 증가

**81%의 조직이 작년 한 해 클라우드 보안 인시던트를 경험했습니다.[1]**

온프레미스, 프라이빗/퍼블릭 클라우드, VM 또는 컨테이너 등 가상화된 시스템으로의 전환은 계속해서 증가 추세에 있으며 감소 징후는 거의 관찰되지 않고 있습니다. 효율적인 운영을 목표로 설계된 이러한 최신 아키텍처는 경계 기반 보안 아키텍처보다 빠른 진화 속도를 보여주었습니다. 한편 측면 이동은 탐지가 매우 어렵습니다. 이에 일부 조직은 암호화된 통신의 하이브리드 클라우드 인프라 내 이동을 허용함으로써 계산된 위험을 감수하거나 방화벽 추가 배포를 통해 가상 아키텍처를 확장하여 효율성을 희생합니다. 오늘날과 같이 대부분의 기업이 다수의 가상 플랫폼을 보유하고 있는 상황에서 어려움과 위험은 더욱 커집니다.

### 2. 개발팀의 촉박한 일정

**83%의 조직이 IT팀과 보안팀의 공동책임주의를 도입했습니다.[2]**

소프트웨어 개발팀의 주된 목표는 매출 증대에 기여하거나 조직에 시간 및 비용 절감 효과를 제공하는 애플리케이션을 개발하는 것입니다. 마감 기한에 대한 지속적인 압박이 이어지는 가운데 데브옵스(DevOps)팀은 핵심 기능에 집중합니다. 이들은 보안과 관련해 일정 수준의 관심을 기울이고 있지만 대체로 침입 방지에 대한 전문적인 지식을 보유하고 있지 않으며 발생 가능한 취약성에 대해서도 잘 알지 못합니다. 또한 보안 에이전트로 인해 테스트가 지연되고 소프트웨어 개발 수명주기에 관련 작업 및 시간이 추가될 수 있기 때문에 소프트웨어 및 시스템에 이를 배포하는 것을 꺼릴 수도 있습니다.

각 보안 조직은 이 문제에 대해 다양한 접근 방식을 취하고 있습니다. 일부는 규정 준수를 위해 엄격한 관행을 바탕으로 모든 코드에 에이전트 설치를 의무화하거나 개발팀에 보안 담당자를 포함시킵니다. 반면 철저한 보안 감독이 없는 빠른 개발 외에는 선택지가 없는 경우도 있습니다. 하지만 대부분의 조직이 개발팀에게 일정 수준 이상의 보안 책임을 요구합니다.

### 3. 숨겨진 위협 활동

**91%의 위협이 암호화된 채널을 이용합니다.[3]**

암호화된 통신은 일부 위협에 대한 방지 효과가 있지만 다른 위협을 불러올 수도 있습니다. 일반적으로 위협 행위자는 시스템에 액세스한 후 가장 먼저 로그를 삭제, 비활성화 및/또는 수정합니다. 이후 명령 및 제어 서버 호출, 권한 상승, 측면 이동, 데이터 무단 복사를 통해 최종적으로 데이터 유출을 시행합니다. 이 모든 과정에서 암호화된 통신이 이용됩니다.

**트래픽이 암호화된 경우, 보안 도구의 효과가 5~7배 감소합니다.**

일반적인 암호화 방식은 2개 범주로 나눌 수 있습니다.

- **최신 암호화:** PFS(Perfect Forward Secrecy)를 사용해 감청되는 통신에 대한 복호화 및 암호화의 반복을 막습니다. 감청한 암호화 키는 수명이 짧고 대역 외 복호화에는 활용이 불가능합니다. 최신 암호화 방식에는 TLS 1.3, mTLS 및 PFS를 선택적으로 활성화한 TLS 1.2의 일부 배포 버전이 포함됩니다. Gigamon은 오늘날 네트워크 트래픽의 약 30~40%가 최신 암호화 방식을 사용하고 있으며 앞으로도 증가 추세를 보일 것으로 예상합니다.
- **기존 암호화:** PFS를 사용하지 않으며 감청한 키를 이용한 복호화가 가능합니다. TLS 1.2의 일부 배포 버전과 TLS 및 SSL(Secure Sockets Layer)의 이전 버전이 포함됩니다.

통신이 암호화된 경우에도 네트워크 모니터링이 가능한 다양한 보안 도구가 있습니다. 기존 암호화 방식의 경우, 보안 도구는 일반적으로 이러한 트래픽의 복호화를 직접 시도합니다. 하지만 계산에 많은 비용이 소요될 뿐만 아니라 성능에도 상당한 영향을 미치는 작업이기 때문에 처리에 훨씬 더 많은 "장비"가 필요합니다. 또한 기본 키 라이브러리의 지속적인 업데이트가 요구되며 키 관리에도 많은 시간과 복잡성이 동반됩니다. 하지만 이러한 단점에도 불구하고 여전히 기존 암호화 방식에 밀려 최신 암호화 방식은 소외되고 있습니다.

최신 암호화 방식을 사용하는 경우, 통신을 "중간에" 복호화하는 것이 불가능하기 때문에 보안 도구는 다른 접근 방식을 취해야 합니다. 따라서 패킷 헤더, 패킷 크기, 패킷 주파수 및 기타 서명을 머신러닝 알고리즘에 입력하여 특정 통신의 위험을 평가합니다. 이는 아무것도 하지 않는 것보다는 낫지만 확실한 결과를 가져다 주진 못합니다. 일부 조직은 기존 암호화 방식만 모니터링하거나 경계 보안에 의존하거나 애플리케이션에서 최신 암호화 방식을 금지합니다. 하지만 이와 같은 조치는 이상적인 보안 태세를 갖추는 데 도움이 되지 않습니다.

1,000명 이상의 IT 및 보안 리더를 대상으로 실시한 최근 설문조사 결과, 보안 및 옵저버빌리티 도구로 탐지되지 않은 데이터 침해 비율이 31%에 이르는 것으로 나타났습니다.

**이제 보다 개선된 솔루션이 필요합니다.**

## Precryption 솔루션: 자세히 살펴보기

Precryption 기술이 새롭게 결합된 GigaVUE Universal Cloud Tap(UCT)은 암호화된 가상 및 컨테이너 통신의 사각지대를 제거하여 IT 및 보안 리더가 잃어버린 제어권을 다시 돌려줍니다.


GigaVUE UCT는 가상 환경에서 가장 효율적인 통신 미러링 방법을 제공하도록 설계된 기본 Linux eBPF 기술을 활용하는 최신 가상 탭입니다. UCT는 암호화되지 않은 데이터를 수집한 다음 이를 Gigamon 딥 옵저버빌리티 파이프라인에 효율적으로 전송합니다. 파이프라인에서 추가적인 최적화, 변환, 필터링 및 브로커링을 거쳐 궁극적으로 올바른 물리/가상 도구에 올바른 데이터가 전달됩니다.

GigaVUE UCT를 기반으로 구축된 Gigamon Precryption 기술은 Linux 및 OpenSSL과 같은 암호화 라이브러리와의 원활한 통합을 바탕으로 네트워크 전반에서 암호화가 이루어지기 전 또는 일부 애플리케이션의 경우 네트워크 전반에서 복호화가 이루어진 후에 가상 및 컨테이너 통신을 수집합니다.

- ✓ 네트워크 통신에 대한 영향 없이 그대로 보존되며 네트워크 전반에서 암호화 상태를 유지합니다.
- ✓ 많은 비용이 소요되는 복호화 계산을 수행하지 않습니다. 따라서 Precryption 기술은 최신 및 기존 암호화 방식 모두와 호환되며 암호 유형, 강도 또는 버전에 따른 영향을 받지 않습니다.
- ✓ 애플리케이션 키의 노출 및 번거로운 관리, 인위적인 가상 경로가 필요하지 않습니다.
- ✓ Precryption 기술의 실행은 모니터링되는 애플리케이션과 독립적으로 이루어지므로 애플리케이션 리소스 및 수명주기 관리에 영향을 미치지 않으며 애플리케이션 내부 결함도 야기하지 않습니다.

## Gigamon Precryption 기술 작동 방식: 싱글 노드(그림 1)

1. 앱이 메시지를 암호화해야 하는 경우, OpenSSL과 같은 암호화 라이브러리를 사용해 실제 암호화를 실시합니다.
2. Precryption 기술이 적용된 GigaVUE Universal Cloud Tap(UCT)이 네트워크상에서 암호화되기 전에 해당 메시지의 사본을 수집합니다.
3. 암호화된 메시지는 암호화에 대한 수정 없이 수신 앱으로 전송됩니다. 프록시, 재암호화 및 재전송이 필요하지 않습니다.
4. GigaVUE UCT가 필요에 따라 패킷 헤더를 생성하고 터널에 캡슐화한 다음 딥 옵저버빌리티 파이프라인의 GigaVUE V 시리즈로 전송합니다. Gigamon은 추가적인 복호화 없이 데이터 최적화 및 변환을 거쳐 도구에 전달합니다.

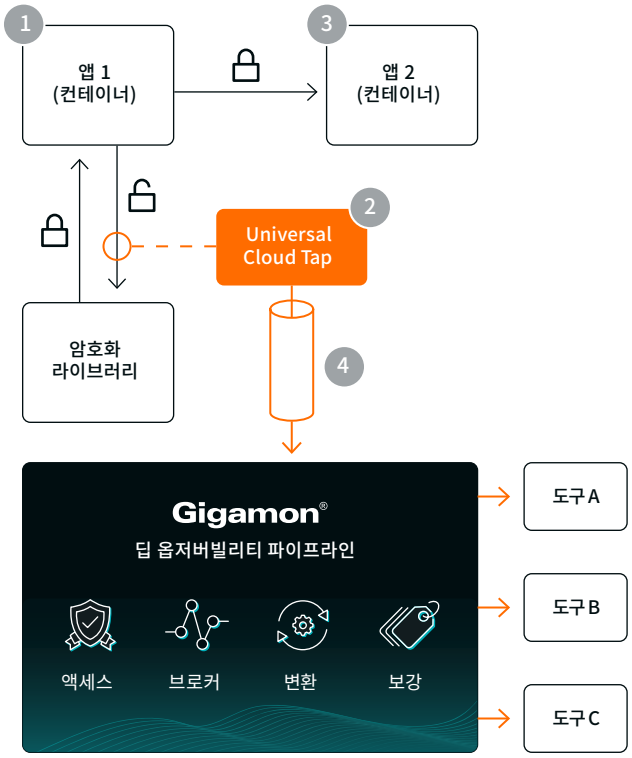



그림 1

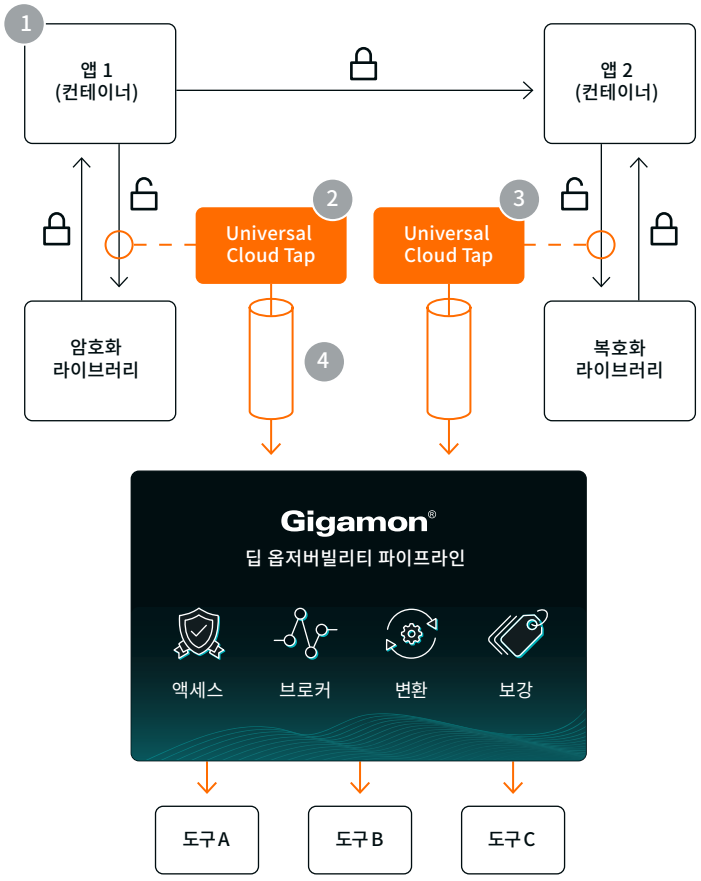



그림 2

## Gigamon Precryption 기술 작동 방식: 멀티 노드(그림 2)

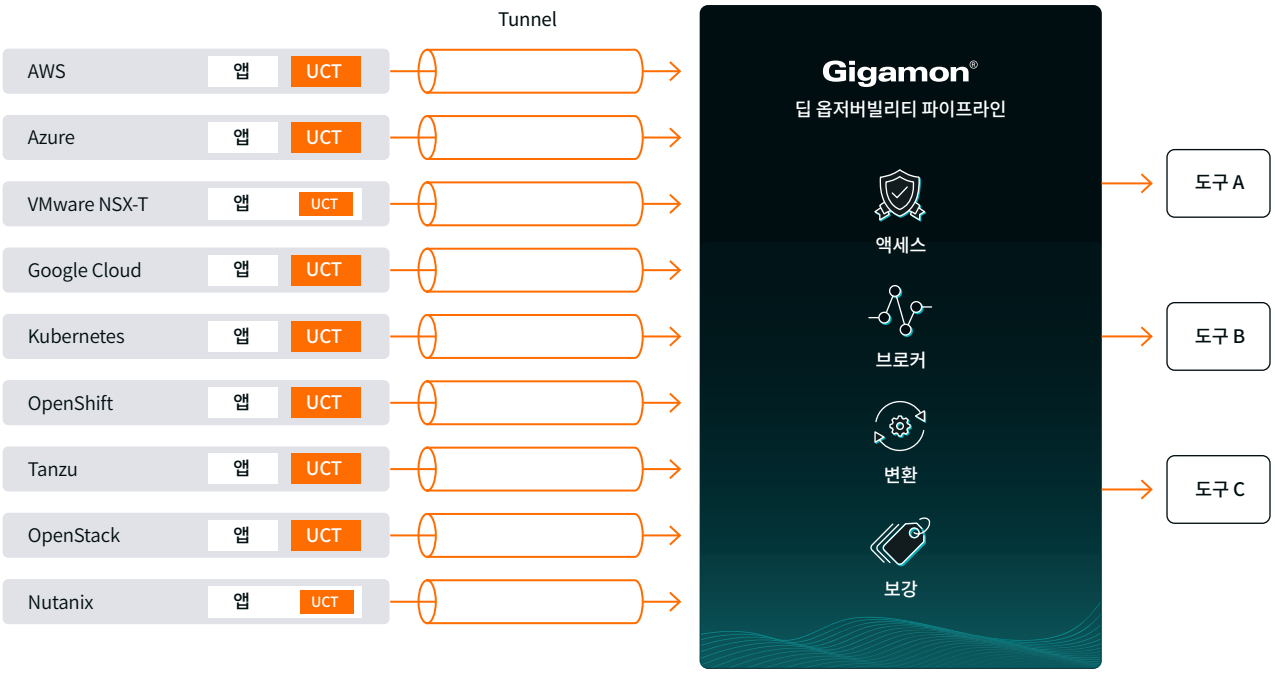
1. 앱이 메시지를 암호화해야 하는 경우, OpenSSL과 같은 암호화 라이브러리를 사용해 실제 암호화를 실시합니다.
2. Precryption 기술이 적용된 GigaVUE Universal Cloud Tap(UCT)가 네트워크상에서 암호화되기 전에 해당 메시지의 사본을 수집합니다.
3. Precryption 기술이 적용된 GigaVUE UCT가 복호화 후 서버 엔드에서 해당 메시지의 사본을 수집할 수도 있습니다(선택 사항).
4. GigaVUE UCT가 필요에 따라 패킷 헤더를 생성하고 터널에 캡슐화한 다음 딥 옵저버빌리티 파이프라인의 V 시리즈로 전송합니다. 추가적인 복호화 없이 최적화 및 변환을 거쳐 도구에 전달됩니다.

## 멀티 클라우드 및 대규모 환경 지원

✓ Precryption 기술과 결합한 GigaVUE UCT는 VMware, AWS, Microsoft Azure, OpenStack, Google Cloud, Nutanix 등 다양한 가상 및 클라우드 플랫폼에서 작동하며 단일 글로벌 관리 인터페이스를 통해 공통 데이터 파이프라인에 전송 가능합니다.

✓ Kubernetes 내 자동 배포가 지원되므로 손쉬운 확장이 가능합니다.

✓ 모든 클라우드 환경 전반의 단일 공유 라이선스 풀 및 무제한 인스턴스가 지원됩니다.




## 애플리케이션과 독립적으로 실행되는 GigaVUE UCT

"에이전트"라는 용어는 상황에 따라 그 의미가 달라질 수 있습니다. 일반 에이전트 대비 UCT의 이점은 다음 표를 참조하십시오.

| 일반 에이전트 | GigaVUE UCT |
|---|---|
| X 애플리케이션 공간/팟 내부에서 실행 | ✓ 독립된 팟 내 독립적인 사용자 공간 |
| X 애플리케이션 리소스 사용량에 영향을 미침 | ✓ 독립적인 노드 리소스 |
| X 버전 업그레이드 조정 필요 | ✓ 독립적인 업그레이드 |
| X 앱과 함께 테스트 필요 | ✓ 독립적인 수명주기 관리 |
| X 앱 레이턴시 유발 | ✓ 독립적인 수집 |
| X 불안정성 또는 장애 발생 시 중단 유발 가능 | ✓ 독립적인 장애 도메인 |

## 네트워크 유래 인텔리전스를 통해 촉박한 개발 일정 속에서도 보안 태세 개선

암호화되지 않은 데이터 추출이 발생하는 경우, Gigamon 딥 옵저버빌리티 파이프라인은 원본(raw) 통신 데이터를 플로우 수준의 메타데이터 레코드로 변환하여 오탐 감소 및 포트 스푸핑과 같은 범죄 활동 식별에 도움을 주는 한편 선제적인 실시간 모니터링을 통해 사후적 성격을 지닌 포렌식보다 빠르게 위협을 탐지할 수 있습니다. 이러한 네트워크 유래 인텔리전스는 로그 수정 대상에 해당하지 않으며 IoT 및 기타 에이전트리스 디바이스와 호환됩니다. 또한 섹옵스(SecOps) 및 데브옵스팀이 사용하는 옵저버빌리티 도구에 전송됩니다.

민감도가 높은 환경에서 UCT는 딥 옵저버빌리티 파이프라인으로 전송되는 미러링된 통신에 대해 선택적인 재암호화를 실시할 수 있을 뿐만 아니라 도구에 전달하기 전에 신용카드 또는 개인식별정보(PII)와 같은 민감 데이터를 숨길 수도 있습니다.

사용 사례

# Precryption 기술을 이용한 사이버 범죄 탐지

랜섬웨어 공격으로도 불리는 사이버 범죄 공격은 일반적으로 위협 행위자가 피싱 또는 기타 자격증명 수집 기술을 이용해 네트워크 외부에 위치한 직원 노트북에 액세스하면서 시작됩니다. 안타깝게도 엔드포인트 보안은 이러한 공격의 탐지 또는 차단에 실패하는 경우가 있습니다.

네트워크 침입에 성공한 위협 행위자에게는 로그 삭제, 권한 상승 및 호스트, 애플리케이션, 워크로드와 같은 보다 흥미로운 기타 네트워크 리소스 및 민감 데이터 검색이 가능한 정교한 기술 등 이용 가능한 다양한 리소스가 주어집니다. 충분한 시간과 공격 벡터만 있다면 이들은 다른 네트워크 리소스에도 침투할 수 있습니다. 우리는 이 기술을 측면 이동이라고 부릅니다.

최종적으로 위협 행위자는 데이터 노출 및 통신 감청이 이루어지는 보다 흥미로운 애플리케이션에 침투합니다. 이들은 제어 가능한 네트워크 내부 장소로 데이터를 천천히 빼돌립니다. 이러한 데이터 추출은 성능에 영향을 주거나 경보가 발생하는 일이 없도록 신중하게 수행됩니다. 충분한 데이터를 확보하고 준비를 마치면 마지막으로 고속 및 대규모 데이터 유출 이벤트를 통해 훔친 데이터를 외부로 내보낸 다음 그 대가로 조직에 돈을 요구합니다.

**이 시나리오에서 위협 행위자의 주요 활동 유형을 4가지로 구분할 수 있습니다.**

1. 엔드포인트 보안 우회를 위한 초기 피싱 또는 자격증명 수집
2. 네트워크 내 측면 이동
3. 민감 데이터를 지정된 위치로 천천히 추출
4. 고속 데이터 유출 이벤트

Gigamon Precryption 기술은 평문에 대한 가시성을 바탕으로 보안 도구가 이러한 활동을 감지하는 데 다음과 같은 도움을 줍니다.

| | **Precryption이 없을 때 보안 도구로 탐지 가능한 항목** | **Precryption이 있을 때 보안 도구로 탐지 가능한 항목** |
|---|---|---|
| **초기 피싱** | 직원 정규 활동 | 직원 정규 활동 |
| **측면 이동** | 양성 노이즈 | 알려진 공격이 배포 및 서버에 성공적으로 침투 |
| **데이터 유출** | 양성 노이즈 | VIP 데이터에 대한 액세스 및 승인되지 않은 채널을 통한 전송 |
| **데이터 유출** | 대규모 데이터 전송 | 도난 항목에 대한 상세 분석 |

**사이버 범죄 시나리오에 대한 보다 자세한 해결 방법은 인포그래픽을 다운로드하세요.**

## 결론

암호화된 트래픽 및 메타데이터에 대한 가시성은 하이브리드 클라우드 보안, 모니터링 및 문제 해결에 상당한 도움을 줍니다. Gigamon 딥 옵저버빌리티 파이프라인은 온프레미스 및 퍼블릭 클라우드 모두에서 가상 및 컨테이너 트래픽의 모니터링과 관련된 최신 보안 문제를 직접적으로 해결하는 솔루션입니다. GigaVUE UCT는 강력한 플랫폼 지원 및 단일 관리 인터페이스를 바탕으로 클라우드 도입 증가로 인한 문제를 처리합니다. Gigamon의 네트워크 유래 인텔리전스는 데브옵스, 클라우드옵스(CloudOps) 및 섹옵스팀이 사용하는 보안 도구를 위한 품질 메타데이터를 공급합니다. 또한 Gigamon Precryption 기술은 최신 암호화 방식을 이용해 복잡하게 숨겨진 클라우드 내 활동을 모니터링하는 한편 정교하고 간편한 방식으로 보안 태세를 개선하고 공격을 차단합니다.

## Gigamon 소개

Gigamon은 실행 가능한 네트워크 유래 인텔리전스를 바탕으로 옵저버빌리티 도구의 기능을 극대화하는 딥 옵저버빌리티 파이프라인을 제공합니다. 이 강력한 조합은 IT 조직의 보안 및 규정 준수 거버넌스 보장, 성능 병목 현상의 근본 원인에 대한 신속한 분석 및 하이브리드/멀티 클라우드 IT 인프라 관리에 수반되는 운영 간접비 절감을 지원합니다. Gigamon은 이를 통해 오늘날의 기업들이 클라우드의 혁신 잠재력을 완벽히 구현할 수 있도록 합니다. Gigamon은 Fortune 100대 기업의 80% 이상, 10대 모바일 네트워크 공급업체 중 9개, 수백 개 이상의 정부 및 교육 기관을 포함한 전 세계 4,000여 고객에게 서비스를 제공하고 있습니다. 보다 자세한 정보는 gigamon.com에서 확인할 수 있습니다.


1. Shelley Boose. 81% of Companies Have Had a Cloud Security Incident in the Last Year. Venafi, September 28, 2022. https://venafi.com/ blog/81-companies-have-had-had-cloud-security-incident-last-year-venafi-research.
2. 2023 Hybrid Cloud Security Survey: Perception vs. Reality. Gigamon, 2023. https://www.gigamon.com/content/dam/gated/wp-gigamon- survey-hybrid-cloud-security-2023.pdf.
3. Internet Security Report – Q2 2021. Watchguard, 2021. https://www.watchguard.com/wgrd-resource-center/security-report-q2-2021.
4. Deepen Desai. Encrypted Attacks Rise 314%: New ThreatLabz State of Encrypted Attacks Report. Zscaler, October 28, 2021. https://www. zscaler.com/blogs/security-research/encrypted-attacks-rise-314.



Gigamon®

**전 세계 본사**
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com




**09.23_01**