Precryption™을 통해 가장 큰 사각지대 없애기

기가몬 Precryption 기술은 가상, 클라우드, 컨테이너를 포함한 전체 보안 스택에 대한 측면 트래픽의 평문 가시성을 제공하며 복호화가 필요하지 않습니다.

#1

IT 보안 리더의 우려 사항:
미처 인지하지 못한 사각지대의 악용[2]

91%

암호화된 채널 사용
으로 야기된 위협[3]

81%

작년 한 해 클라우드 보안 사고를 경험한 조직[1]

5배

트래픽이 암호화되지 않은 경우 보안 도구의 효과
5~7배 증가[4]

31%

작년 한 해 보안 및 옵저버빌리티 도구로 **탐지되지 않은 데이터 침해**[2]

기가몬 Precryption™ 기술은 가상, 클라우드 및 컨테이너화된 애플리케이션에 대한 보안을 재정의하여 기존에 투입되던 비용 및 복호화 복잡성 없이 전체 보안 스택에 대해 암호화된 통신의 평문을 가시적으로 파악할 수 있도록 합니다.

정보 보안 과제

1. 클라우드 채택 증가
2. 개발 팀의 촉박한 일정
3. 숨겨진 위협 활동

암호화된 통신은 오늘날 최신 하이브리드 클라우드 인프라 전반에 걸쳐 거의 모든 곳에 사용되며, 기존의 가로채기 기법으로부터 민감한 데이터를 보호합니다. 위협 행위자는 새롭고 더욱 정교한 접근 방식에 대응하여 침투하고 주요 시스템을 해킹하여 민감한 데이터에 액세스합니다. 이제 이러한 침입자는 암호화된 동일한 통신 채널을 사용하여 자신의 활동, 특히 측면 이동, 민감한 데이터에 대한 액세스 및 데이터 유출을 숨깁니다. 시중에 나와 있는 기존 솔루션으로는 가상 워크로드 간에 측면으로 이동하는 암호화된 트래픽에 대한 평문을 가시적으로 파악하는 것이 거의 불가능하기 때문에 숨겨진 위협 활동을 탐지하는 것이 매우 어렵습니다. 따라서 암호화된 측면 통신은 가장 큰 보안 사각지대로 남게 됩니다.

숨겨진 위협 활동을 탐지하는 Precryption 기술

Precryption 기술은 오늘날 하이브리드 클라우드 인프라의 가장 큰 사각지대인, TLS 1.3을 포함한 최신 암호화 형태를 통해 난독화되는 위협 행위자의 측면 이동을 직접 해결하는 혁신적인 솔루션입니다. Precryption는 비용이 많이 드는 복호화나 키 수집 및 관리로 인한 어려움 없이 효율적이고 마찰이 없는 폼 팩터에서 암호화된 가상 통신에 대한 평문 가시성을 제공합니다.

Precryption 기술의 작동 방식

Precryption 기술은 네이티브 Linux 기능을 활용하여 애플리케이션과 암호화 라이브러리(예: OpenSSL) 간의 통신을 태핑하거나 복사합니다.

이러한 방식으로 Precryption은 네트워크 트래픽이 암호화되기 전 또는 복호화된 후에 네트워크 트래픽을 평문으로 캡처합니다. Precryption 기능은 메시지의 실제 암호화나 네트워크를 통한 메시지의 전송을 방해하지 않습니다. 또한 프록시, 재전송, 중단 및 검사가 필요 없습니다. 대신 이 평문 복사본은 추가적인 최적화, 변환, 복제 및 여러 도구로의 전송을 위해 기가몬 딥 옵저버빌리티 파이프라인으로 전달됩니다.

Precryption 기술은 GigaVUE® UCT(Universal Cloud Tap)를 기반으로 구축되었으며 온프레미스 및 가상 플랫폼을 포함하여 하이브리드 및 멀티 클라우드 환경에서 작동합니다.

그 외에도 Precryption 기술이 적용된 UCT는 애플리케이션과 독립적으로 실행되어 애플리케이션 개발 수명주기에 포함될 필요가 없다는 이점이 있습니다.

주요 사용 사례

사이버 범죄 방지: 클라우드의 측면 이동은 사이버 범죄 공격에 특히 취약한 사각지대입니다. 일단 경계 보안을 통과하면 암호화된 패킷이 모니터링되지 않으므로 위협 행위자는 모든 종류의 수법과 기술을 사용하여 탐지를 피할 수 있습니다.

TLS 1.3 규정 준수: TLS 1.3의 도입이 필요함에도 불구하고 일부 조직은 오늘날 암호화된 트래픽에 대한 가시성 부족을 이유로 TLS 1.3의 채택을 미루고 있습니다. 몇몇 조직은 별도의 복호화 솔루션을 관리하는 방식에 의존하고 있습니다.

제로 트러스트: 효과적인 제로 트러스트 아키텍처의 핵심 기반은 패킷을 확인하고, 네트워크상의 리소스 간 모든 상호 작용을 검사하고, 정책을 적용하는 기능입니다.

네트워크 기반 인텔리전스: SIEM과 같은 보안 도구는 위협을 더 잘 탐지하기 위해 메타데이터 변환 및 강화에 의존하는 경우가 많습니다.

기가몬 Precryption을 선택해야 하는 이유

Precryption 기술이 탑재된 GigaVUE Universal Cloud Tap은 최신 하이브리드 클라우드 인프라에 존재하는 사각지대를 제거하여 가상, 클라우드 및 컨테이너 플랫폼에 대한 동서(East-West) 가시성을 제공하는 마찰이 없는 경량 솔루션입니다. 복호화 키를 관리 및 유지하지 않아도 TLS 1.3을 포함한 모든 암호화 유형에 대한 명확한 가시성을 제공합니다. 이제 IT 조직은 규정 준수를 관리하고, 사설 통신을 비공개로 유지하고, 제로 트러스트에 필요한 기반을 설계하고, 보안 도구 효율성을 5배 이상 높일 수 있습니다.

주요 기능

- **첨단 암호화**(TLS 1.3, mTLS 및 Perfect Forward Secrecy를 사용한 TLS 1.2)**를 사용하는 통신에 대한 평문 가시성 제공**
- **레거시 암호화**(TLS 1.2 및 이전 버전)**를 사용하는 통신에 대한 평문 가시성 제공**
- 컨테이너 워크로드 내부에서 에이전트를 실행할 필요가 없는 **비침입 방식의 트래픽 액세스**
- 기존 트래픽 복호화와 관련하여 **비용이 많이 드는 리소스를 사용할 필요 없음**
- 기존 트래픽 복호화처럼 **키를 관리할 필요 없음**
- 암호 유형, 강도 또는 버전에 따라 **성능에 미치는 영향 없음**
- 온프레미스, 가상, 컨테이너 플랫폼을 포함하여 **하이브리드 및 다중 클라우드 환경 전반에 걸쳐 지원**
- 보안 도구에 평문으로 된 위협 활동을 전달하여 네트워크 전반에서 **사설 통신을 비공개로 유지**
- **기가몬 딥 옵저버빌리티 파이프라인과 통합**되어 완벽한 전체 최적화, 변환 및 중개 기능 제공

핵심 이점

- 방화벽을 통과할 수 없는 트래픽을 포함하여 암호화된 동-서(측면) 및 남-북 통신의 **사각지대 제거**
- 개발 팀의 속도를 향상하는 독립적인 접근 방식으로 **애플리케이션 통신 모니터링**
- 암호화 유형에 관계없이 모든 통신에 대한 **보안 도구의 가시성 확장**
- 가상 환경 전반에서 **트래픽 태핑 효율성 극대화**
- 암호화되지 않은 데이터를 사용하여 보안 도구의 **성능 5~7배 향상**
- 딥 옵저버빌리티를 기반으로 한 **제로 트러스트 아키텍처 지원**
- 복호화된 트래픽 관리와 관련된 **개인정보 보호** 및 규정 준수 유지

직면 과제: 자세히 살펴보기

오늘날 IT 조직은 각자 책임지고 있는 시스템과 데이터를 보호하는 데 가상 및 클라우드 채택 증가, 개발 팀의 빠듯한 일정, 숨겨진 위협 활동이라는 중대한 세 가지 과제에 직면해 있습니다.

1. 가상 및 클라우드 채택 증가

작년 한 해에 81%의 조직이 클라우드 보안 사고를 경험[1]

온프레미스, 사설 또는 공용 클라우드, VM 또는 컨테이너 등 가상화된 시스템을 향한 이러한 움직임은 계속 증가하고 있으며 둔화될 조짐은 거의 보이지 않습니다. 이러한 최신 아키텍처는 운영 효율성을 높이도록 설계되었으며 경계 기반 보안 아키텍처보다 매우 빠르게 발전하고 있습니다. 측면 이동은 탐지하기가 매우 어렵습니다. 일부 조직에서는 암호화된 통신이 하이브리드 클라우드 인프라 전반에서 이동하도록 허용해 계산된 위험을 감수하며, 다른 일부 조직에서는 보안에 적절한 효율성이 저하되는 것을 감수하고 추가 방화벽을 배포하여 가상 아키텍처 강화를 시도합니다. 또한 다수의 기업이 여러 가상 플랫폼을 보유하고 있는 경우 직면 과제와 위험이 배가됩니다.

2. 개발 팀의 촉박한 일정

83%의 조직에서 IT 팀과 보안 팀 간의 공동 책임을 도입[2]

소프트웨어 개발 팀의 주요한 목표는 매출 성장에 기여하거나 조직의 시간과 비용을 절약할 수 있는 애플리케이션을 개발하는 것입니다. 기한을 맞추기 위해 계속해서 서두르면서 DevOps 팀은 핵심 기능에 집중합니다. DevOps 팀은 어느 정도 보안을 고려할 수는 있지만 일반적으로 침입 방지 분야의 전문가는 아니기 때문에 발생할 수 있는 취약점을 간과할 수 있습니다. 또한 보안 에이전트로 인해 테스트가 지연되고 소프트웨어 개발 수명주기에 작업과 소요 시간이 늘어날 수 있기 때문에 소프트웨어 및 시스템에 보안 에이전트를 배포하는 것을 꺼릴 수 있습니다.

보안 조직은 이 문제에 다양한 방식으로 접근합니다. 일부 조직은 규정 준수를 위한 엄격한 관행을 적용해 에이전트를 모든 코드에 적용하고, 몇몇 조직에서는 보안 인력을 개발 팀에 포함시키는 반면, 엄격한 보안 감독 없이 개발 팀에 빠듯한 일정에 맞춰 빠르게 업무를 수행하도록 할 수밖에 없는 조직도 있습니다. 그러나 대다수 조직에서는 적어도 일정 수준의 보안 책임을 개발 팀에 부여합니다.

3. 숨겨진 위협 활동

위협의 91%는 암호화된 채널 사용으로 야기됨[3]

암호화된 통신은 일부 위협을 방지하는 데 유용하지만 이로 인해 다른 위협이 발생할 수도 있습니다. 일반적으로 위협 행위자는 시스템에 액세스한 후 가장 먼저 로그를 삭제, 비활성화 및/또는 수정합니다. 그런 다음 명령 및 제어 서버에 대한 호출, 권한 상승, 측면 이동, 데이터의 비밀 복사를 수행하여 궁극적으로 데이터를 유출하며, 이는 모두 암호화된 통신을 사용하여 이루어집니다.

암호화된 트래픽의 경우 보안 도구의 효율성이 5~7배 저하될 있음[4]

일반적인 암호화 방법은 다음 두 가지 범주로 나눌 수 있습니다.

- **최신 암호화:** PFS(Perfect Forward Secrecy)를 사용하여 가로챈 통신에 대한 중단 및 검사 복호화를 방지합니다. 이는 가로챈 암호화 키는 수명이 짧고 대역 외 복호화에 쓸모가 없기 때문입니다. 최신 암호화에는 TLS 1.3, mTLS 및 PFS가 선택적으로 활성화된 일부 TLS 1.2 배포가 포함됩니다. 기가몬은 오늘날 네트워크 트래픽의 약 30~40%가 최신 암호화를 사용하고 있으며 이 비율은 계속해서 증가할 것으로 추정합니다.

- **레거시 암호화:** PFS를 사용하지 않으며 가로챈 키로 복호화할 수 있습니다. 여기에는 TLS 1.2의 일부 배포와 TLS 및 SSL(Secure Sockets Layer)의 이전 버전이 포함됩니다.

암호화된 통신을 사용하는 네트워크를 모니터링할 수 있는 보안 도구가 있습니다. 레거시 암호화의 경우 이러한 보안 도구는 일반적으로 직접 트래픽 복호화를 시도합니다. 이는 계산 비용이 많이 들고 성능에 상당한 영향을 미치므로 처리 요구 사항을 해결하기 위해 훨씬 더 많은 '박스'가 필요합니다. 또한 기본적인 키 라이브러리를 지속적으로 업데이트해야 하며 키 관리도 복잡하며 많은 시간이 소요됩니다. 그러나 이 모든 단점에도 불구하고 여전히 레거시 암호화만 다루고 있으며 최신 암호화는 간과되고 있습니다.

최신 암호화의 경우 이러한 도구는 다른 접근 방식을 취해야 하는데, 이는 통신을 '중간에' 복호화할 수 없기 때문입니다. 따라서 패킷 헤더, 패킷 크기, 패킷 빈도 및 기타 서명을 기계 학습 알고리즘에 공급하여 해당 통신의 위험을 평가합니다. 아무런 조치를 취하지 않는 것보다는 낫지만 결과는 미비합니다. 일부 조직에서는 레거시 암호화만 모니터링하고 경계 보안을 신뢰하거나, 애플리케이션에서 최신 암호화를 금지하고 있는데, 이는 모두 이상적인 보안 조치는 아닙니다.

1,000명이 넘는 IT 및 보안 리더를 대상으로 한 최근 설문 조사에서 응답자들은 데이터 침해의 31%가 보안 및 옵저버빌리티 도구로 감지되지 않았다고 답했습니다.

더 나은 솔루션이 필요합니다.

Precryption 솔루션: 자세히 살펴보기

이제 Precryption 기술이 탑재된 GigaVUE Universal Cloud Tap(UCT)은 암호화된 가상 및 컨테이너 통신의 사각지대를 없애 IT 및 보안 리더가 다시 통제력을 확보할 수 있도록 합니다.

GigaVUE UCT는 가상 환경에서 통신을 미러링하는 가장 효율적인 방법으로 설계된 네이티브 Linux eBPF 기술을 활용하는 최신 가상 탭입니다. UCT는 암호화되지 않은 데이터를 획득하여 기가몬 딥 옵저버빌리티 파이프라인에 효율적으로 전달합니다. 여기에서 추가적인 최적화, 변환, 필터링 및 중개가 이루어져 궁극적으로 물리적이든 가상이든 도구 유형에 구애받지 않고 올바른 도구에 올바른 데이터를 전달합니다.

기가몬 Precryption 기술은 GigaVUE UCT를 기반으로 하며 Linux 및 OpenSSL과 같은 암호화 라이브러리와 원활하게 통합되어 네트워크 전반에서 암호화되기 전에 가상 및 컨테이너 통신을 획득하며, 일부 애플리케이션의 경우 네트워크 전반에서 복호화된 통신을 획득합니다.

- ✓ 네트워크 통신이 훼손되지 않고 보존되며 네트워크 전반에서 암호화된 상태로 유지됩니다.
- ✓ 비용이 많이 드는 복호화 계산이 필요하지 않습니다. 따라서 Precryption 기술은 최신 및 레거시 암호화와 함께 작동하며 암호 유형, 강도 또는 버전의 영향을 받지 않습니다.
- ✓ 애플리케이션 키가 노출되지 않고 번거롭게 애플리케이션 키를 관리하지 않아도 되며, 부자연스러운 가상 경로도 필요하지 않습니다.
- ✓ Precryption 기술은 모니터링되는 애플리케이션과 독립적으로 실행되므로 애플리케이션의 리소스 및 수명주기 관리에 영향을 미치지 않고 애플리케이션 내에 오류를 일으키지 않습니다.

기가몬 Precryption 기술의 작동 방식: 단일 노드(그림 1)

1. 앱에서 메시지를 암호화해야 하는 경우 OpenSSL과 같은 암호화 라이브러리를 사용하여 실제 암호화를 수행합니다.

2. Precryption 기술이 적용된 GigaVUE Universal Cloud Tap(UTC)가 메시지가 네트워크에서 암호화되기 전에 해당 메시지의 복사본을 확보합니다.

3. 암호화된 메시지가 암호화 수정 없이 수신 앱으로 전송됩니다. 프록시, 재암호화 및 재전송이 필요하지 않습니다.

4. GigaVUE UCT는 필요에 따라 패킷 헤더를 생성하여 터널에 압축한 다음 딥 옵저버빌리티 파이프라인의 GigaVUE V 시리즈로 전달합니다. 기가몬은 추가적인 복호화 없이 데이터를 더욱 최적화하고 변환하여 도구에 전달합니다.

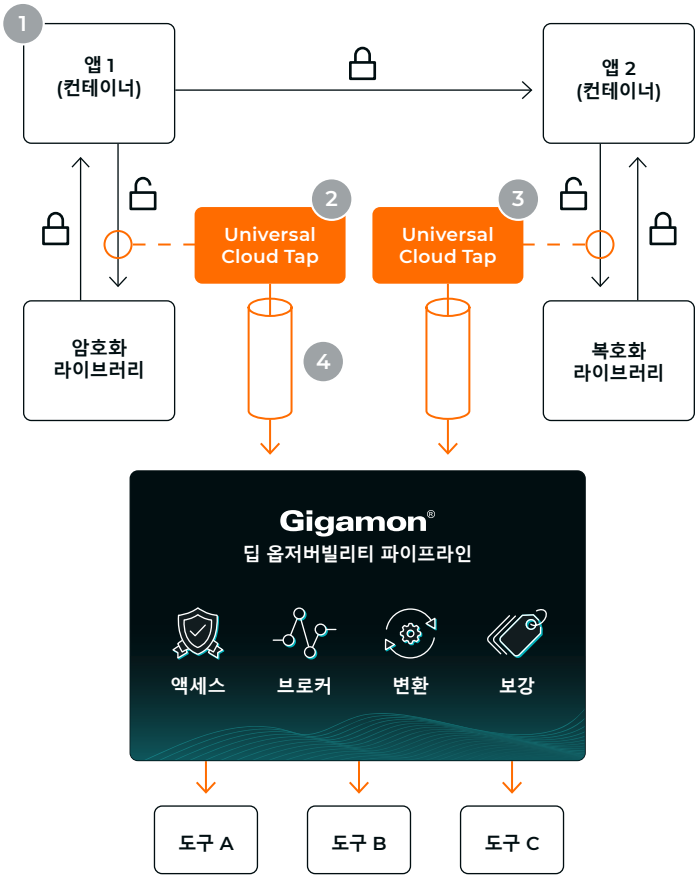

그림 2

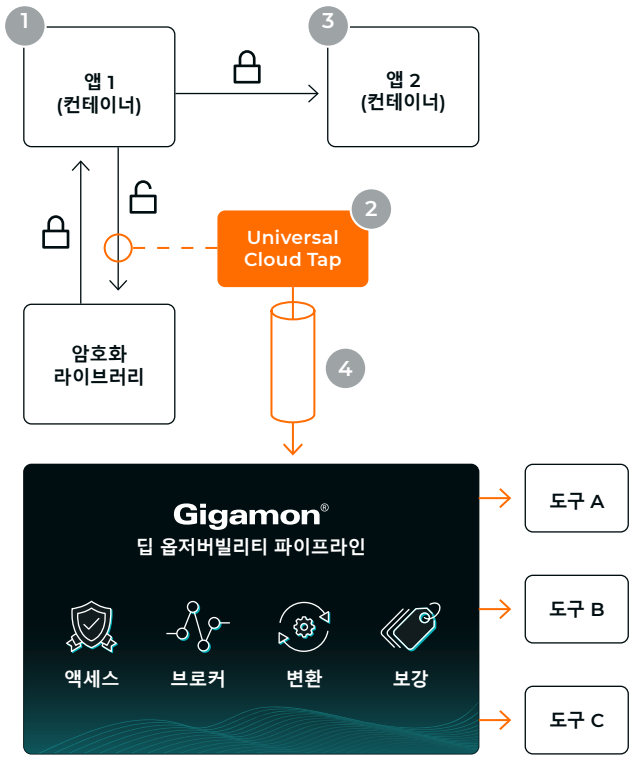

그림 1

기가몬 Precryption 기술의 작동 방식: 다중 노드(그림 2)

1. 앱에서 메시지를 암호화해야 하는 경우 OpenSSL과 같은 암호화 라이브러리를 사용하여 실제 암호화를 수행합니다.

2. Precryption이 적용된 GigaVUE Universal Cloud Tap (UCT)가 메시지가 네트워크에서 암호화되기 전에 해당 메시지의 복사본을 확보합니다.

3. 경우에 따라 Precryption이 적용된 GigaVUE UCT는 복호화 후 서버 엔드에서 메시지 복사본을 확보할 수도 있습니다.

4. GigaVUE UCT는 필요에 따라 패킷 헤더를 생성하여 터널에 압축한 다음 딥 옵저버빌리티 파이프라인의 V 시리즈로 전달합니다. 여기서 추가적인 복호화 없이 패킷 헤더가 더욱 강화되고 변환되어 도구에 전달됩니다.

다중 클라우드 및 대규모 환경에서 작동

Precryption 기술이 적용된 GigaVUE UCT는 VMware, AWS, Microsoft Azure, 오픈스택, Google Cloud, Nutanix 등을 포함하여 여러 가상 및 클라우드 플랫폼 전반에 걸쳐 작동하며, 단일 글로벌 관리 인터페이스를 통해 공통 데이터 파이프라인에 적용됩니다.

- ✓ 확장 편의성을 위해 Kubernetes 내 자동 배포 지원
- ✓ 모든 클라우드 환경에 걸친 하나의 공유 라이선스 풀, 무제한 인스턴스

애플리케이션과 독립적으로 실행되는 GigaVUE UCT

'에이전트'라는 용어는 맥락에 따라 그 의미가 달라질 수 있습니다. 일반 에이전트 대비 UCT의 이점을 확인하려면 다음 표를 참조하십시오.

일반 에이전트	GigaVUE UCT
X 애플리케이션 공간/파드 내부에서 실행	✓ 독립 파드 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 지연이 발생할 수 있음	✓ 독립적인 캡처
X 불안정성 또는 장애 발생 시 중단될 수 있음	✓ 독립적인 장애 도메인

네트워크 기반 인텔리전스를 추가하여 개발 일정이 촉박한 상황에서도 보안 태세를 향상

암호화되지 않은 데이터가 추출되면 기가몬 딥 옵저버빌리티 파이프라인을 추가로 활용하여 원시 통신 데이터를 플로우 수준의 메타데이터 레코드로 변환하여 긍정 오류를 줄이고, 포트 스푸핑과 같은 악의적인 활동을 식별하고, 대응적 포렌식이 대신 선제적인 실시간 모니터링을 통해 위협 탐지를 가속화할 수 있습니다. 이 네트워크 기반 인텔리전스는 로그 수정 대상이 아니며 IoT 및 기타 에이전트리스 장치에서 작동하며 SecOps 팀 및 DevOps 팀에서 사용하는 옵저버빌리티 도구에 반영됩니다.

매우 민감한 환경에서 UCT는 딥 옵저버빌리티 파이프라인으로 전달되는 미러링된 통신을 선택적으로 다시 암호화할 수 있을 뿐만 아니라 도구에 전달하기 전에 신용 카드나 개인 식별 정보(PII)와 같은 민감한 데이터를 마스킹할 수도 있습니다.

사용 사례

Precryption 기술을 사용하여 사이버 범죄 탐지

랜섬웨어 공격이라고도 하는 사이버 범죄 공격은 일반적으로 위협 행위자가 피싱이나 기타 자격 증명 수집 기술을 통해 네트워크 외부에 있는 직원의 노트북에 액세스하는 것으로 시작됩니다. 엔드포인트 보안이 이러한 상황을 감지하거나 예방할 수 있으면 좋지만 안타깝게도 놓치는 경우가 있습니다.

일단 네트워크 내부에 침입하면 위협 행위자는 로그를 삭제하고, 권한을 상승시키고, 호스트, 애플리케이션, 워크로드와 같이 더 민감한 데이터를 포함한 보다 흥미로운 기타 네트워크 리소스를 찾을 수 있는 정교한 기술 등의 다양한 리소스를 이용할 수 있습니다. 충분한 시간과 공격 벡터가 주어지면 위협 행위자는 다른 네트워크 리소스에 침투할 수 있게 됩니다. 이 기술을 측면 이동이라고 합니다.

궁극적으로 위협 행위자는 더욱 흥미로운 애플리케이션에 침투합니다. 이렇게 되면 데이터가 노출되어 위협 행위자의 감시를 받게 됩니다. 위협 행위자는 자신이 제어하는 네트워크 내의 드롭 위치로 데이터를 천천히 빼돌릴 것입니다. 이러한 데이터 빼돌리기 작업은 성능에 영향을 주거나 경보를 유발하지 않도록 주도면밀하게 수행됩니다. 위협 행위자가 충분한 데이터를 획득하고 준비를 마치면 마지막으로 신속하게 대규모 데이터 유출을 감행해 훔친 데이터를 외부로 내보낸 다음 조직으로부터 돈을 갈취합니다.

이 시나리오에서 위협 행위자가 수행한 네 가지 주요 활동 유형은 다음과 같습니다.

1. 엔드포인트 보안을 우회하기 위한 초기 피싱 또는 자격 증명 수집
2. 네트워크 내 측면 이동
3. 중요한 데이터를 드롭 위치로 천천히 유출
4. 신속하게 데이터 유출 감행

아래 내용을 살펴보고 기가몬 Precryption 기술을 통해 평문 가시성을 확보하여 도구가 이러한 활동을 탐지하도록 돕는 방법을 확인하세요.

	Precryption를 사용하지 않는 경우 보안 도구가 탐지할 수 있는 항목	**Precryption를 사용하는 경우 보안 도구가 탐지할 수 있는 항목**
초기 피싱	일상적인 직원 활동	일상적인 직원 활동
측면 이동	양성 노이즈	알려진 공격이 전개되어 서버에 성공적으로 침투
데이터 빼돌리기	양성 노이즈	승인되지 않은 채널을 통해 VIP 데이터가 액세스되고 전송됨
데이터 유출	대규모 데이터 전송	도난 항목 상세 분석

사이버 범죄 시나리오에 대한 자세한 내용을 알아보려면 인포그래픽을 다운로드하세요.

결론

암호화된 트래픽과 메타데이터에 대한 가시성을 확보하면 하이브리드 클라우드 보안, 모니터링 및 문제 해결이 크게 향상됩니다. 기가몬 딥 옵저버빌리티 파이프라인은 온프레미스 및 공용 클라우드 모두에서 가상 및 컨테이너 트래픽을 모니터링하기 위한 최신 보안 문제를 직접 해결합니다. GigaVUE UCT는 강력한 플랫폼 지원과 단일 관리 인터페이스를 통해 클라우드 도입 증가로 인한 문제를 해결합니다. 기가몬 네트워크 기반 인텔리전스는 DevOps 팀, CloudOps 팀 및 SecOps 팀을 위한 보안 도구에 양질의 메타데이터를 제공합니다. 또한 기가몬 Precryption 기술은 최신 암호화 방식을 이용해 클라우드에서 숨겨진 활동을 모니터링하는 방법에 대한 매우 까다로운 문제를 해결하고, 이를 위해 보안 태세를 강화하고 악의적인 행위자의 공격을 차단하도록 고안된 정교하고 간편한 방식을 사용합니다.

기가몬 정보

기가몬은 실행 가능한 네트워크 기반 인텔리전스를 활용하는 딥 옵저버빌리티 파이프라인을 제공하여 옵저버빌리티 도구의 기능을 확장합니다. 이러한 강력한 도구를 함께 사용하면 IT 조직이 보안 및 규정 준수 거버넌스를 보장하고, 성능 병목 현상의 근본 원인 분석 속도를 높이며, 하이브리드 및 다중 클라우드 IT 인프라의 관리와 관련된 운영 오버헤드를 낮출 수 있습니다. 결과: 오늘날의 기업은 클라우드의 잠재력을 최대한 발휘한다는 약속을 실현할 수 있습니다. 기가몬은 Fortune 100대 기업의 80% 이상, 10대 모바일 네트워크 제공업체 중 9곳, 전 세계 수백 개의 정부 및 교육 기관을 비롯하여 전 세계 4,000곳 이상의 고객사에 서비스를 제공하고 있습니다. 자세히 알아보려면 gigamon.com을 방문하세요.

1. Shelley Boose. 81% of Companies Have Had a Cloud Security Incident in the Last Year(작년 한 해 81%의 기업이 클라우드 보안 사고를 경험). Venafi, 2022년 9월 28일. 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(2023 하이브리드 클라우드 보안 설문 조사: 인식과 현실의 비교). 기가몬, 2023. https://www.gigamon.com/content/dam/gated/wp-gigamon-survey-hybrid-cloud-security-2023.pdf.
3. Internet Security Report – Q2 2021(인터넷 보안 보고서 - 2021년 2분기). 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(암호화된 공격 314% 증가: ThreatLabz의 새로운 암호화된 공격 상태 보고서). Zscaler, 2021년 10월 28일. 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