Network Blackbox

Avant-garde Network Detection and Response

사고 기록 **전체를 분석**하는 항공기 **블랙박스**처럼
네트워크 트래픽 전체를 **손실 없이 수집**해서
사이버 보안 위협을 **탐지**하고 **분석**합니다

Quad Miners

100% FULL 패킷 캡쳐

최대 40G 망에서 | 단 하나의 데이터 유실 없이 | 그대로 저장

40Gbps
Connectivity

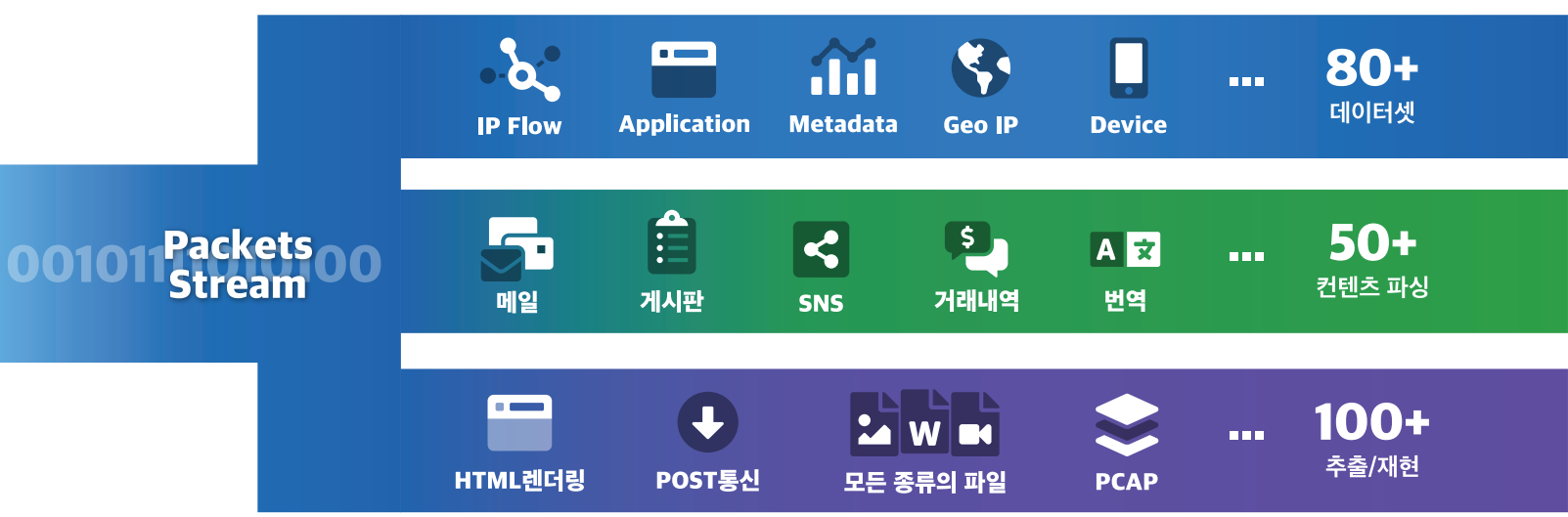
100%
Zero Packet Loss

Payload
대용량 저장 공간 (최대 15PB)

패킷을 미러링하므로 네트워크 망에 어떠한 영향도 없으며, 별도의 에이전트를 설치하지 않습니다.

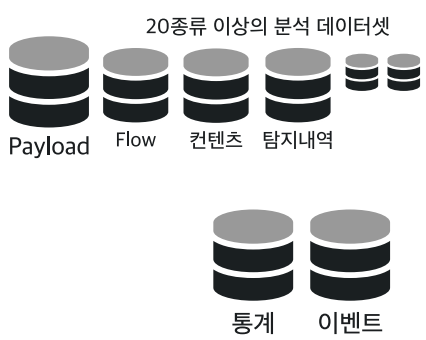
네트워크 패킷 실시간 재조합

단순하게 패킷 저장만 하는 것이 아니라, Application 계층(L7)까지 재조합하여 네트워크에서 벌어지는 행위를 가시화합니다.



이 외에도 바이러스 검사, 이상 행위 탐지 등의 다양한 후처리를 하고 있습니다

심층적인 네트워크 트래픽 분석



Flow 뿐만 아니라
80종류 이상의 조건으로 상관 분석

임계치 기반 분석 및
다수의 장비에서 수집한 이벤트 분석

고도로 정제된 데이터베이스를 통해 사이버 위협을 분석하고, 단순 로그가 아닌 실제 패킷까지 확인할 수 있습니다

실시간 지능형 위협 탐지

최신 위협탐지 룰을 통해

25000+
Cyber Threat Hunting

실시간으로 이상 징후 탐지

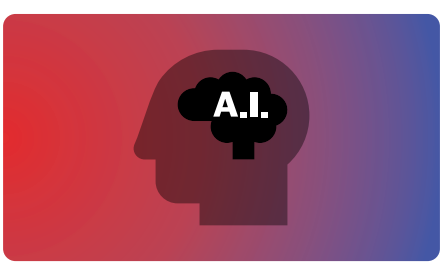
Realtime
Anomaly Detection

고도화된 위협 대응
시그니처 기반 공격 탐지
행위 기반 공격 탐지
C&C, 악성코드, 웜 탐지
시나리오 기반 공격 탐지

탐지된 내역을 다각도로 분석하여 악성 여부에 대한 명확한 가시성을 제공합니다

유연하고 확장 가능한 아키텍처

머신러닝 기반 위협탐지 연동

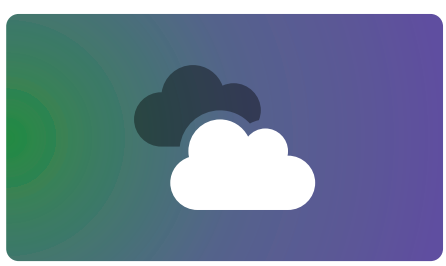


은행, 증권사에서 네트워크 블랙박스가 추출한
네트워크 트래픽 데이터와 컨텐츠 데이터를
머신러닝 기반 위협탐지 솔루션을 연동하여
Fraud Detection을 하고 있습니다.

서드파티 보안솔루션 연동

많은 기업들이 SIEM, APT 대응 솔루션 등을 도입하여 사용하고 있습니다.
단순 로그 밖에 없었던 기존 솔루션에 네트워크 블랙박스를 연동하여
해당 장비의 탐지 내역의 정오탐 확인은 물론, 첨부된 파일을 복원하여 다운로드하고,
실제 패킷을 열어 다각도로 분석하는 등 네트워크 포렌직 장비로 활용하고 있습니다.

클라우드 서비스 READY



전세계에서 주목하고 있는 솔루션

APAC CIO Outlook TOP 10
CYBER SECURITY

Gartner

APAC CIO Outlook에서 2019년 사이버 보안 부문 Top 10에 선정하였으며 가트너와 전략 파트너쉽을 맺고 있습니다

GOOD Software
GS인증 1등급

특허 출원 내역

고성능 패킷 스트림 저장 시스템 및 이를 이용한 고성능 패킷 스트림 저장 방법 (10-2019-0073260)
패턴 기반 색인 처리 시스템 및 이를 이용한 패턴 기반 색인 처리 방법 (10-2019-0073261)
시나리오 중심 실시간 공격 감지 시스템 및 이를 이용한 시나리오 중심 실시간 공격 감지 방법 (10-2019-0073262)
네트워크 포렌식 시스템 및 이를 이용한 네트워크 포렌식 방법 (PCT-KR2019-008860)

조달 등록 내역

통신소프트웨어, 쿼드마이너, 넷블랙 2.0, 네트워크분석솔루션 (43232902-23613516)

CYBER SECURITY EDITION

APAC CIO Outlook

JULY -08- 2019

APACCIOOUTLOOK.COM

Top10 Cyber Security Solution Providers -2019

In the wake of the growing sophistication of cybersecurity threats and risks, coupled with the unprecedented volume of attacks and increasingly stricter regulatory mandates, there is a pressing need to be in-line with the emerging trends and solutions of the cybersecurity space more than ever. The rapidly growing number of IoT endpoints is outpacing innovation in the security space. Enterprises need to come to grips with this trend and assert some control over the use of unmanaged devices and establish clear protocols for managed devices. As every industry adapts to new and emerging threats, a zero trust cloud security model will be considered an enterprise standard— the model eliminates the idea that internal employees are trustworthy individuals who mean no harm and will continuously evaluate an individual's behavior and actions to identify and eliminate potential threats.

The introduction of a two-factor authentication system for all cloud services will act as a first-line-of-defense mechanism and an endpoint process monitoring tool. Many security and risk management companies are rolling out cybersecurity management platforms that harness the power of automation. The implementation of machine learning into an advanced logging and analytics process will enable us to take in data from multiple of different sources—assisting in co-relating the information, detecting threats, automating generation and distributions of security protocols.

This edition of APAC CIO Outlook brings you the "Top 10 Cyber Security Solution Providers - 2019." This list gives you some of the most prominent organizations in the industry that have excelled with their solution portfolio in the cybersecurity space. This list is aimed at bridging the gap between businesses and solution providers that are transforming business processes through their insights and technological prowess.

Company:

Quad Miners

Key Person:

Bumjoong (Ven) Park
CEO & Co-Founder

Description:

Provides a next-generation security solution based on network detection and response that stores and analyzes full-packet traffic in real time

Website:

quadminers.com

APAC CIO Outlook
CYBER SECURITY
SOLUTION PROVIDERS –2019

Quad Miners

The Rising Rookie in Network Security

During a security incident investigation, the network engineer of a company notices that certain devices are being crippled by some suspicious traffic. Try as he might, the engineer couldn't troubleshoot what exactly was transpiring on the network. Despite having an abundance of security tools, the company was capturing an incomplete record of network activity making it next to impossible to quickly investigate the issue and determine the root cause.

The above scenario is probably a common occurrence across many organizations today. Currently, when security incidents occur due to an attack by a cracker or an information leak from personnel within the organization, significant clues and data to analyze them are missed. This is because most existing security and network monitoring solutions in the market show only part of the alerts, issue description, and log analysis, preventing a thorough understanding of network behavior or an incident. If only the company in the example above was using Network Blackbox by Quad Miners they could have resolved and eliminated the threat in no time. A truly next-gen network security solution, the Network Blackbox can process large amounts of bandwidth and collect and analyze full-packet traffic in real-time, which makes it easier to track all attacks in a network environment.

The rising rookie in network security solutions, Quad Miners' Network Blackbox applies Suricata rules to detect events and user-defined rules to analyze full-packets. Behind this “futuristic iteration of network security” are a group of four visionaries (the Quad) that go back 15 years. Having met each other in their college's network security lab, overtime the experts put together their skills at packet mining to redefine the

Bumjoong(Ven) Park,
CEO & Co-Founder

world of network security forever. “While Quad Miners was founded in 2017, the research and development behind the Network Blackbox began as early as 2014, signifying the kind of dedication, passion, and groundwork that went behind Quad Miners,” says Bumjoong (Ven) Park, CEO and co-founder of Quad Miners.

To delve a little more into the Network Blackbox, the solution can process large amounts of traffic per second and recognize up to 400 applications. It can easily integrate with various third-party solutions, APIs, Java Database Connectivity (JDBC), security information and event management (SIEM) tools, APT Sandbox, and more. The solution also comes in-built with specific rules and policies to detect abnormal behavior within internal users that are sending consistent emails to the same location.

In the event of a breach, another unique feature in Network Blackbox, which comes to the rescue is the ability to restore a user’s screen so that the security team can check where and what website a user was on without the use of forensic. Moreover, keeping in mind that the global security market is increasingly leveraging big data and machine learning where the data integration of the contents of a packet emerges as a necessity, Quad Miners offers full packet data integration. “To analyze and save packets quickly, we also design and develop our own database,” mentions Park.

What speaks for itself about Quad Miners’ superior value proposition is their list of esteemed clientele that comprises industry bigwigs such as Samsung Display, the Shinhan Bank, Starbucks Korea, Gyeonggi Provincial Government, Korea Airports Corporation, and much more. To give a deeper understanding of their solution, Park recalls a case in point where a reputable global company was facing serious security problems as sensitive information was being leaked out by personnel within the company. The company used a combination of webmail, in-house messenger, data loss prevention strategies, and forensic solution yet failed to fully identify the leaks. However, enter Network Blackbox and the single solution was equivalent to four, saving full-packet traffic into distributed database nodes in a scaled-out fashion. Quad Miners' state-of-the-art database was able to store three months of full-packet traffic and using it the client could fully analyze traffic in real-time and take rapid actions against security issues.

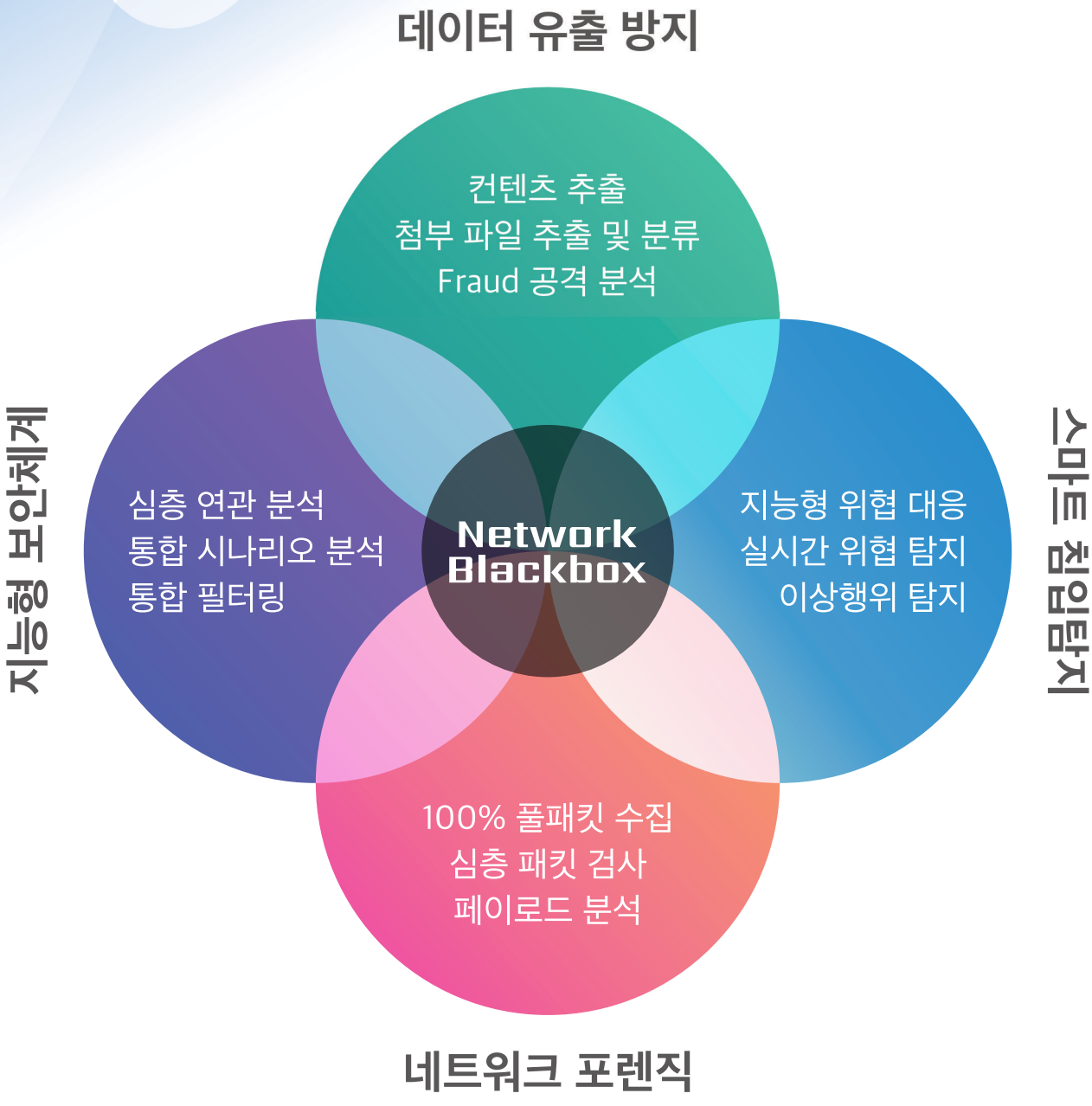
Another engaging customer success story is that of a large-sized financial company. They were trying to detect fraudulent activities using a SIEM system but received an incomplete picture of network activity. With Network Blackbox, the client was able to establish a next-generation fraud detection system, collect full-packet traffic, and analyze transactions based on the traffic. In case of a breach or detection of suspicious activity, the client could drill down to the network packets to pinpoint precisely what took place, eliminating guesswork, and taking remedial action much faster. “The implementation was such a hit that other domestic clients and overseas branches of the company are now considering Network Blackbox,” states Park.

> Network Blackbox can process large amounts of bandwidth and collect and analyze full-packet traffic in real time

Quad Miners’ client success rate is growing with each passing year and they have their eyes on even bigger milestones. The company is looking at further expanding its footprint in Singapore and Japan. Innovation will continue to be the name of the game for the company as is evident from the cloud-based beta version of Network Blackbox, which they are currently working on. “We believe this will be the world's first cloud-based full-packet inspection technology that will integrate various network security solutions into one,” mentions Park.

All in all, on combining Quad Miners’ journey so far with their future endeavors in progress, it can be said beyond any doubt that the pictogram of a shovel in their logo and what it stands for is clearly an apt representation of the company: patience, effort, and digging deep into the security landscape. ACO

모든 패킷을 저장하고 재현할 수 있기 때문에
모든 종류의 사이버 보안 위협을
탐지하고 대응할 수 있습니다



sales@quadminers.com | +82-2-548-1124 Quad Miners