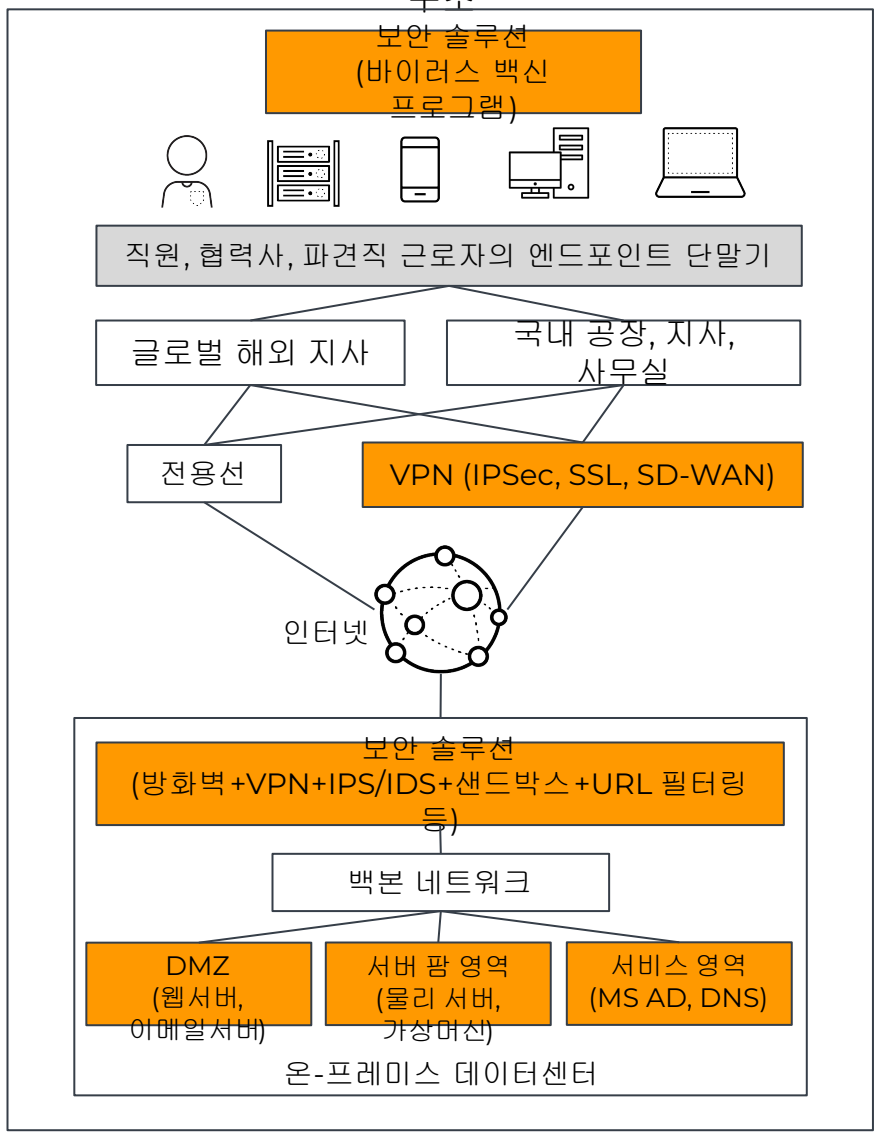
NGFW + EDR_XDR을 활용한 랜섬웨어 탐지 차단 솔루션

팔로알토 네트웍스
코리아

paloalto NETWORKS

2024년 최신 국내/외 랜섬웨어 보안 침해 사고가 발생한 주요 기술적인 원인은 아래와 같습니다.

(그림) 일반적인 국내 중견 기업의 IT 인프라의 논리적인 구조



바이러스 백신 프로그램의 한계 : 일반적인 엔드포인트 백신(이하 EPP, Endpoint Protection Platform 혹은 '안티바이러스')은 최신 랜섬웨어를 적시에 탐지하지 못하며 그 주된 이유는, 아래와 같이 전통적인 감지 기법과 오늘날 랜섬웨어 공격자들이 사용하는 고도화된 회피 기법 간의 격차가 지속적으로 발생하기 때문입니다.

-시그니처 기반 탐지의 한계, 정적 분석 우회 기법 악용 (패킹 및 난독화, 파일리스 공격), 비정상 행위 기반 탐지 기술 부족, 최신 고급 회피 기법 악용 (안티-디버깅, 안티-샌드박스, 맞춤형 랜섬웨어 제작 기술), 이메일/URL 기반 유입 미탐지, DNS tunneling 기법, 암호화된 악성코드 송수신(SSL/TLS 트래픽), OS / App 취약점 익스플로잇.

인터넷에 노출되어 있는 VPN 장비의 취약점을 악용한 랜섬웨어 공격 사례 증가 : 2024년 랜섬웨어 보안 침해사고의 시작점이 되고 있는 중요한 네트워크 접속 포인트 입니다. 공격자들은 IPSec 및 SSL VPN 솔루션/제품의 공개된 보안 허점을 통해 네트워크에 무단으로 침입하여 랜섬웨어를 배포하고 있습니다. 특히, 해외 공장을 운영 중인 제조업 고객의 경우, VPN 장비를 통해서 유입되는 랜섬웨어 / 악성코드 탐지 및 조치 대응을 하지 못하고 있는 상황이 매우 많았습니다.

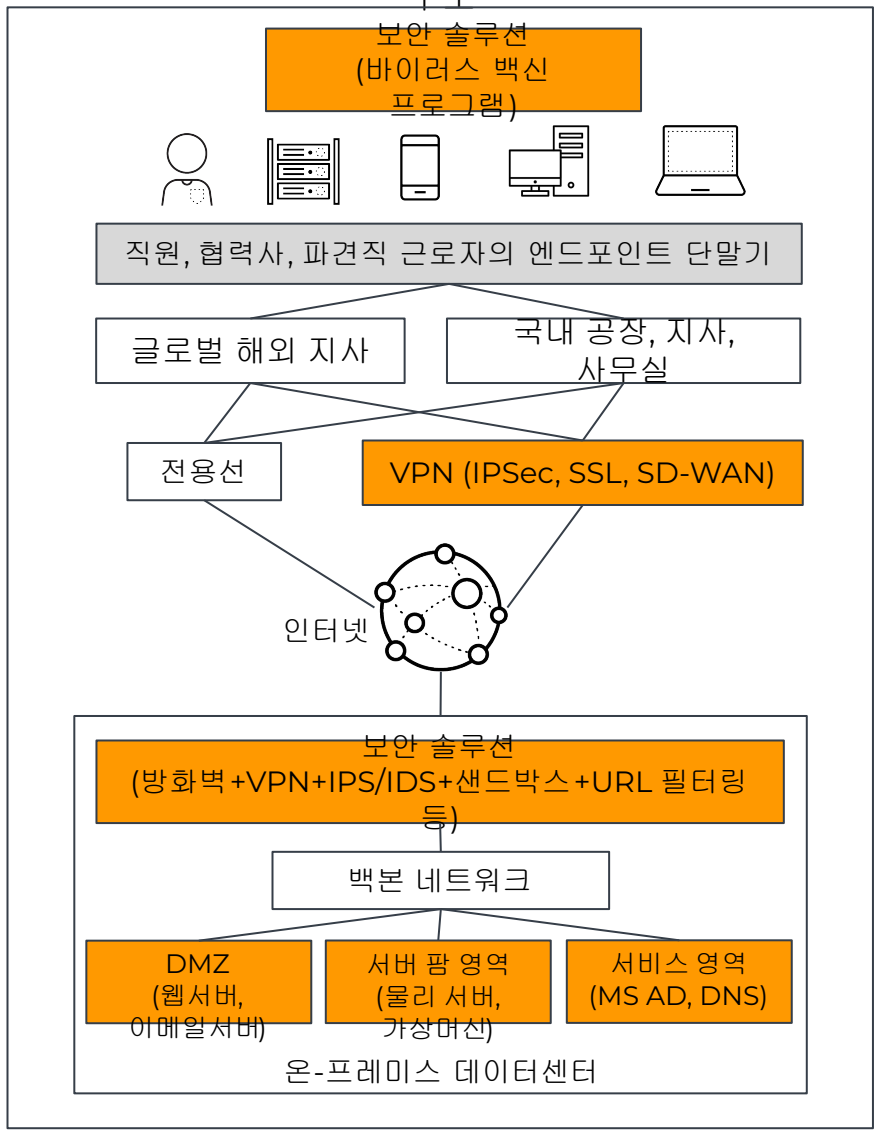
-F사/C사/S사 VPN 장비 취약점 악용 사례, 한국원자력연구원 해킹 사건, I사 SSL VPN 취약점 공격 사례.

통신 트래픽의 Payload(페이로드) 검사 기술이 없는 보안 장비를 우회한 랜섬웨어 유입 피해 사례 증가 : 일반적인 국내 중견 기업에서 운영 중인 대부분의 보안 장비 (방화벽, IPS/IDS, NAC, URL 필터링 장비, 샌드박스 등)는 통신 트래픽 패킷(Packet)의 페이로드 (Payload) 부분을 검사하는 기능이 없는 상태로 운영되고 있습니다. 이러한 보안 장비의 한계를 악용한 랜섬웨어 침해 사고가 증가하고 있습니다. 특히, 인터넷 사용에 필수인 DNS 서비스 (UDP 포트번호 53)를 악용한 DNS 터널링(tunneling) 기반 C2 멀웨어 트래픽 침입 사례가 급증 하였습니다.

-WannaCry 랜섬웨어 공격(2017), Log4j 취약점 악용 사례(2021), 교육 기관/병원 의료/제조업 공장 대상의 랜섬웨어 피해 사례 (2024).

2024년 국내 랜섬웨어 보안 침해 사고 해결 및 2차 공격 방지를 위해서, 팔로알토 네트웍스가 지원한 사례 (1/2).

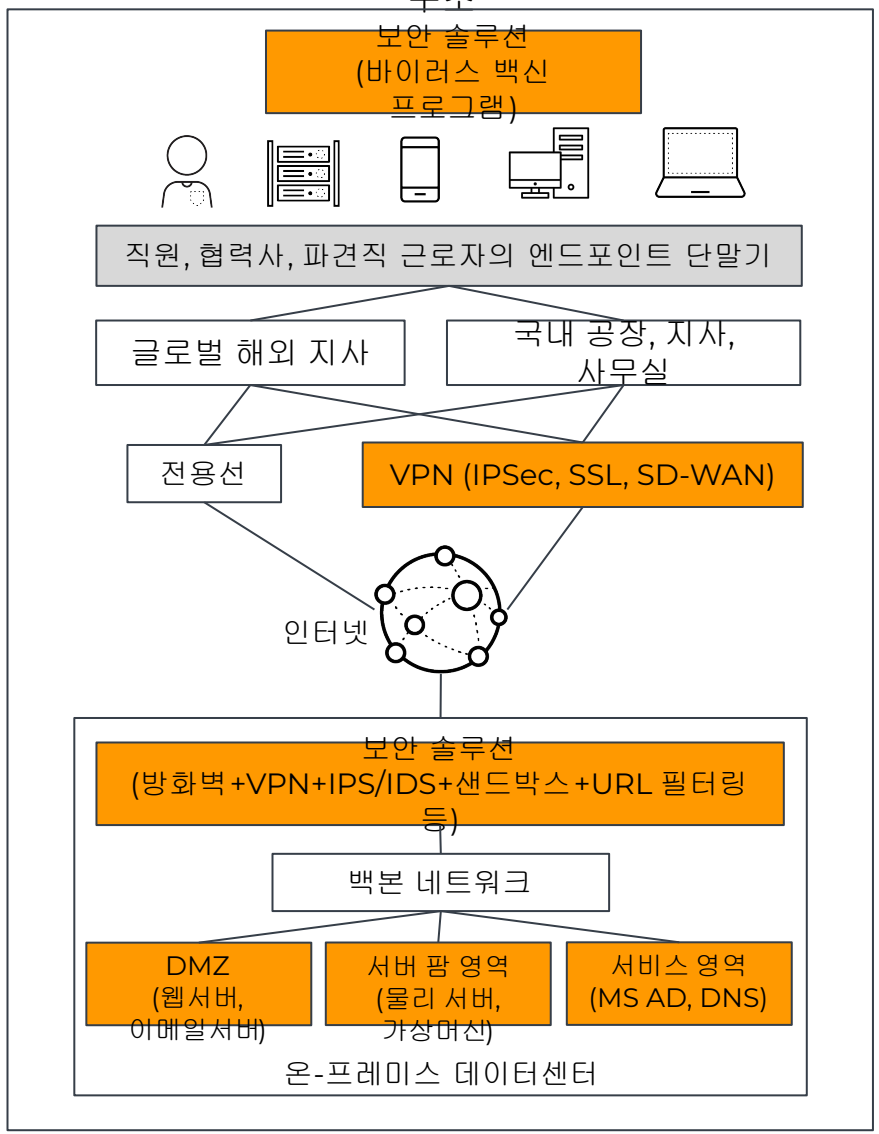
(그림) 일반적인 국내 중견 기업의 IT 인프라의 논리적인 구조



구분	도입 전		도입 후 (팔로알토 네트웍스 NGFW+EDR/XDR)
-사용자 엔드포인트 단말기 -서버	백신 (EPP)	A사, K사, T사	-시그니처 기반의 EPP는 최신 사이버 공격 기술 랜섬웨어 및 악성코드 탐지 및 차단 한계가 존재함. -랜섬웨어 및 악성코드의 비정상 행위 탐지 및 차단을 위한 EDR/XDR 에이전트 적용하여 효과적으로 조치 대응함.
	UEBA	없음	
	EDR (USB 매체 제어) / XDR	K사	
네트워크	방화벽	L4 방화벽	-L4 방화벽 기술 한계 상, 랜섬웨어, 악성코드 탐지 및 차단이 불가능. -서비스 중단 없는 Virtual-Wire mode-NGFW 적용함.
	IPS	국산	
	악성 URL 접속 방지, C2 탐지 방어	국산	
	DNS 트래픽 보안 (DNS 터널링 공격 탐지 방어)	C사	
	ATP (랜섬웨어, 악성코드 탐지 차단) 보안	F사	투입될 Virtual-Wire-mode-NGFW에 랜섬웨어 검출용 클라우드 기반의 샌드박스 적용함.
	OT / IOT 보안	없음	기술지원 종료된 Windows XP/7 등에 대한 C2통신 차단을 위해서 NGFW 적용함.
	SD-WAN (IPSec VPN)	C사	VPN은 전송 구간 암호화 기술이기 때문에, 터널 복호화 이후 트래픽에 대한 랜섬웨어/악성코드 탐지 및 차단 기능 없음. → 랜섬웨어/악성코드 탐지 및 차단용도의 NGFW 적용함. → 중장기 대책 : Prisma SASE 도입 계획 (RDP, SSH 원격 보안 지원)
	SSL VPN	S사, C사	
	SASE (ZTNA)	없음	중/장기 도입 계획.
공장	방화벽	L4 방화벽	-L4 방화벽 기술 한계 상, 랜섬웨어, 악성코드 탐지 및 차단이 불가능. -서비스 중단 없는 Virtual-Wire mode-NGFW 적용함.

2024년 국내 랜섬웨어 보안 침해 사고 해결 및 2차 공격 방지를 위해서, 팔로알토 네트웍스가 지원한 사례 (2/2).

(그림) 일반적인 국내 중견 기업의 IT 인프라의 논리적인 구조



구분	도입 전		도입 후 (팔로알토 네트웍스 NGFW+EDR/XDR)
애플리케이션 서비스	이메일 서비스	M사	-최신 사이버 보안 피싱 및 랜섬웨어 다운로드, C2 사이트 접속 차단을 위한 SaaS 보안.
	웹 서비스/Groupware	HTTP기반	
	데이터베이스	O사	
	온-프레미스 ERP	S사, O사	
	인터넷에 오픈된 디지털 자산 보안 해킹 위협 탐지 방어 (예: 웹 사이트 서비스)	없음	인터넷에 오픈된 Domain 및 공인 IP 주소 서비스 (SSL VPN, RDP, SSH, Telnet 등) 스캐닝을 통해서, 알려진 Vulnerability, Exploit 24X7 상시 모니터링 및 조치 체계 구축.
사용자 ID	Active Directory Domain Controller 서버	SSO 도입 계획	직원 ID에 기반한 NGFW 방화벽 보안 접속 정책 마련 제안 (방화벽 정책, VPN 접속 정책 등)
	IDP(MFA)	없음	외부에서 VPN 접속 시, 2FA 사용 권고.
퍼블릭 클라우드 워크로드 보호	ERP, SAP	없음	-클라우드 워크로드 보안 정책 컨설팅 및 랜섬웨어/악성코드 업로드-다운로드 탐지 및 차단 기술 적용 지원.
보안 운영 센터 (SOC)	SIEM	없음	-네트워크 보안 장비, EDR/XDR에서 발생하는 보안 이벤트 실시간 SIEM+SOAR+TI (Threat Intelligence)+ASM(Attack Surface Management) 구축을 위한 Cortex 제안.
	SOAR 보안 업무 조치 자동화	없음	

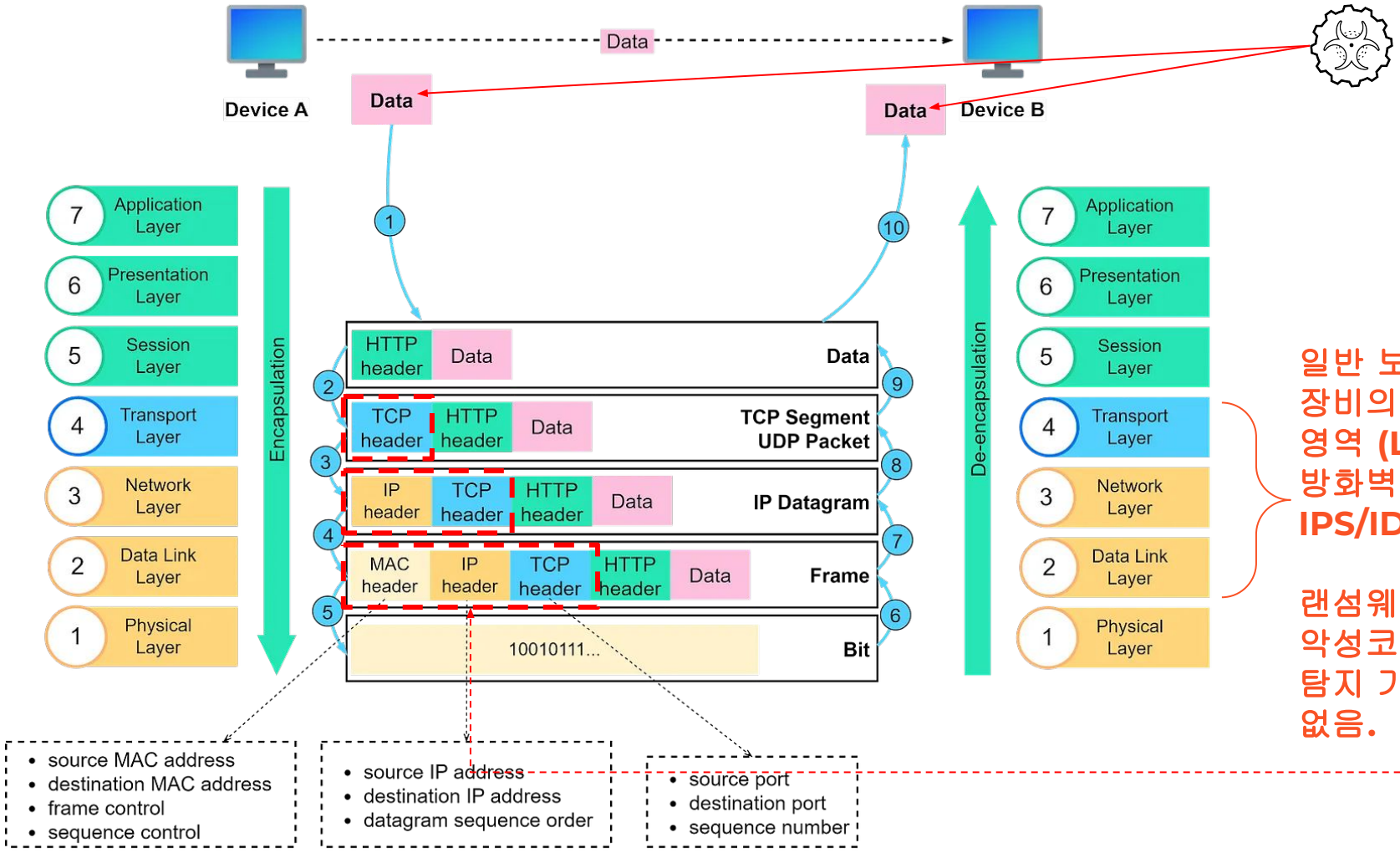
EPP (백신), EDR, XDR 비교 *(팔로알토 네트웍스는 EDR/XDR 벤더)*

기능 구분	EPP	**EDR**	**XDR**
핵심 기능	방지 (시그니처 기반 악성 파일 탐지)	엔드포인트에서의 감지 및 대응	다중 보안 계층에 걸친 탐지 및 대응
범위	엔드포인트	엔드포인트	엔드포인트, 네트워크, 클라우드, 이메일 등
위협 커버 범위	알려진 맬웨어, 랜섬웨어, 피싱	파일리스 맬웨어, 제로데이와 같은 고급 위협	다중 벡터 공격, 내부 위협, 정교한 공격
대응 능력	제한적 (격리, 차단)	강력함 (격리, 치료, 법의학적 분석)	강력함 (다양한 환경에서 자동 응답)
가시성 제공 범위	엔드포인트로 제한됨	자세한 엔드포인트 가시성	조직 전반의 통합된 가시성 (엔드포인트, 네트워크, 클라우드)
탐지-대응 조치 자동화 지원	기본 수준	사고 대응을 위한 일부 자동화	높은 수준의 자동화 및 AI 기반 분석
추천하는 유스케이스	기본 위협 예방	엔드포인트에서의 고급 위협 탐지 및 대응	조직의 전체 보안 스택에 걸친 포괄적인 위협 탐지 및 대응

paloalto NETWORKS

랜섬웨어 및 악성 코드는, **Data Payload** 를 통해서 통신 합니다.

본 슬라이드 목적:
"여러가지 보안 제품이 있었는데, 왜 랜섬웨어를 탐지 못했는가?" 에 대한 이해를 돕기 위함.



일반 보안 장비의 검사 영역 **(L4 방화벽, IPS/IDS 등)**

랜섬웨어, 악성코드 탐지 기능 없음.

차세대 방화벽 NGFW (L7 방화벽) 검사 영역.

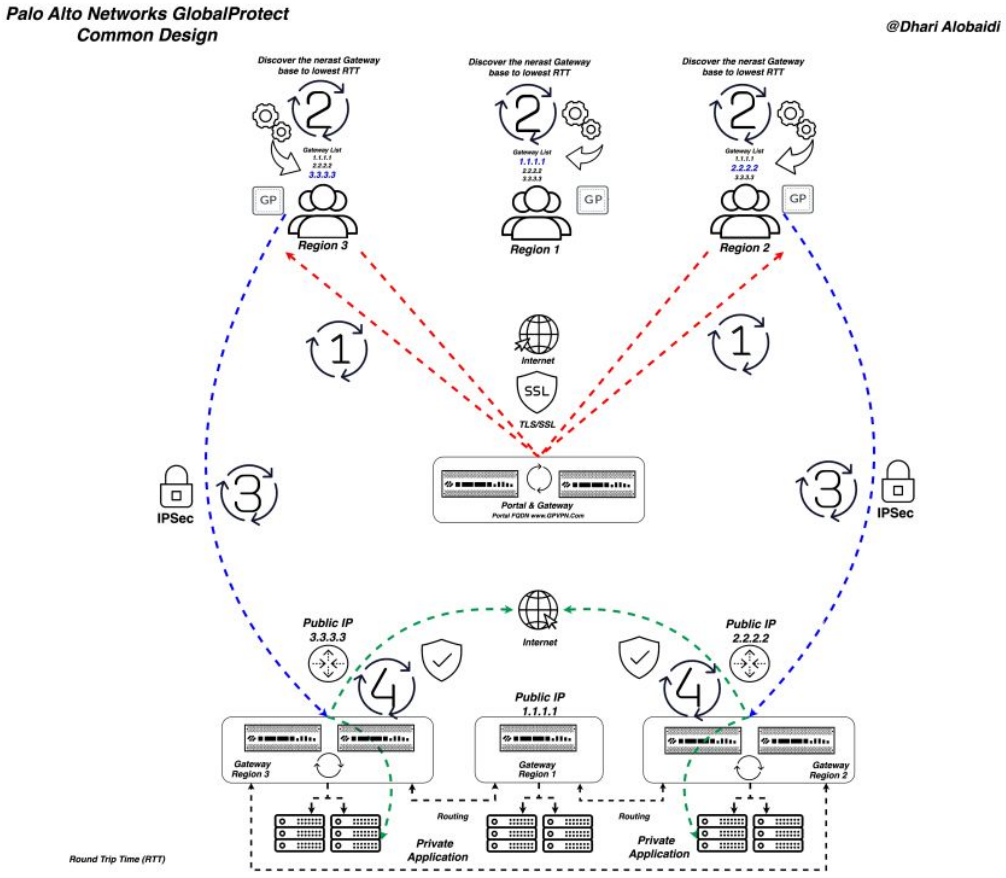
랜섬웨어, 악성코드 탐지, 제거 기능 있음.

*주의 사항 : 차세대 방화벽 특징

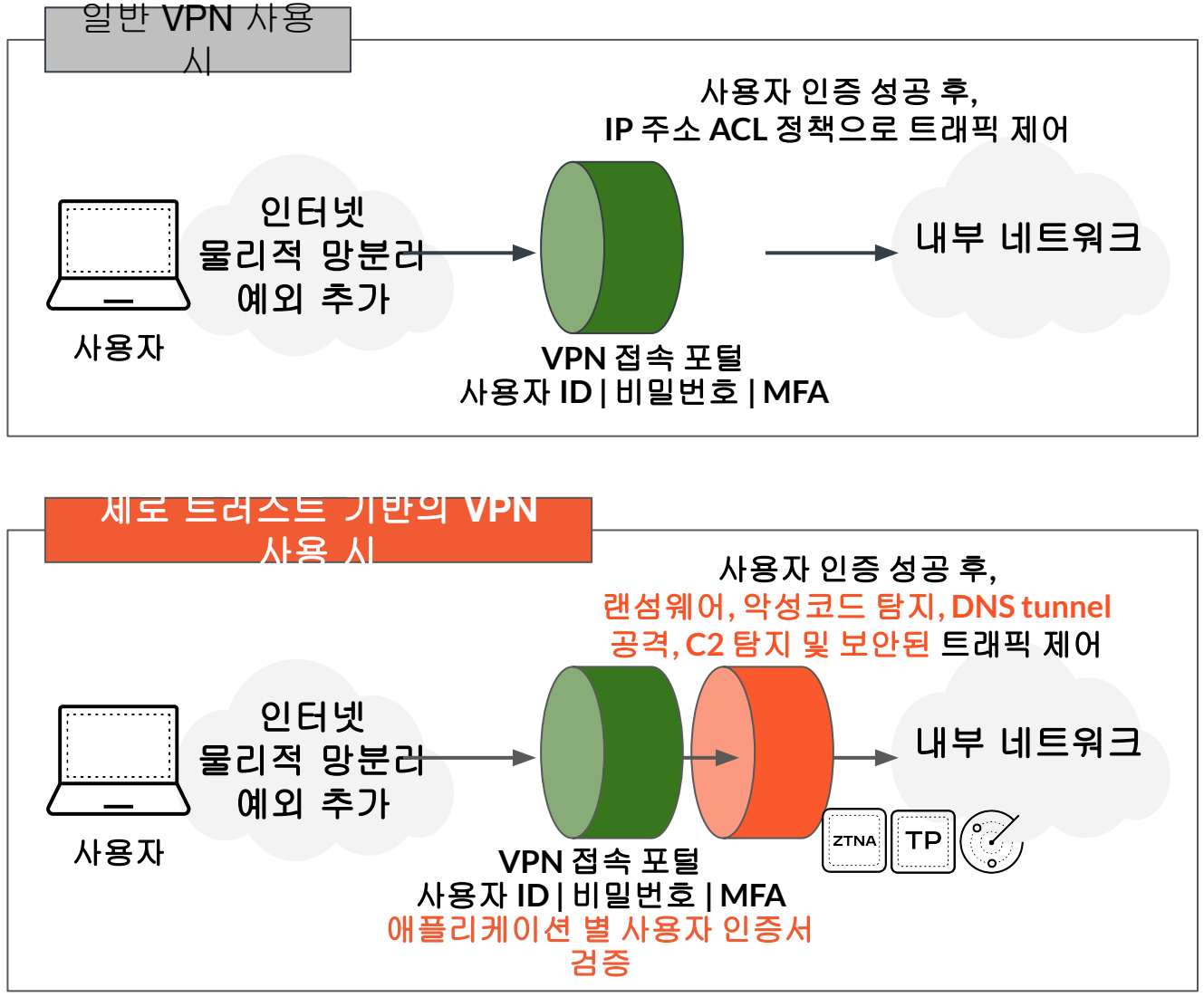
- 랜섬웨어, 악성코드 탐지/제거를 위한 라이선스 필요함.
- 이러한 라이센스가 없으면 **L4** 방화벽과 동일함.
- 라이센스 유효기간 지나면, 신규 공격 탐지 불가능함 (예: 제로-데이 어택).

제로 트러스트 기반의 VPN 구축 도입 필요성.

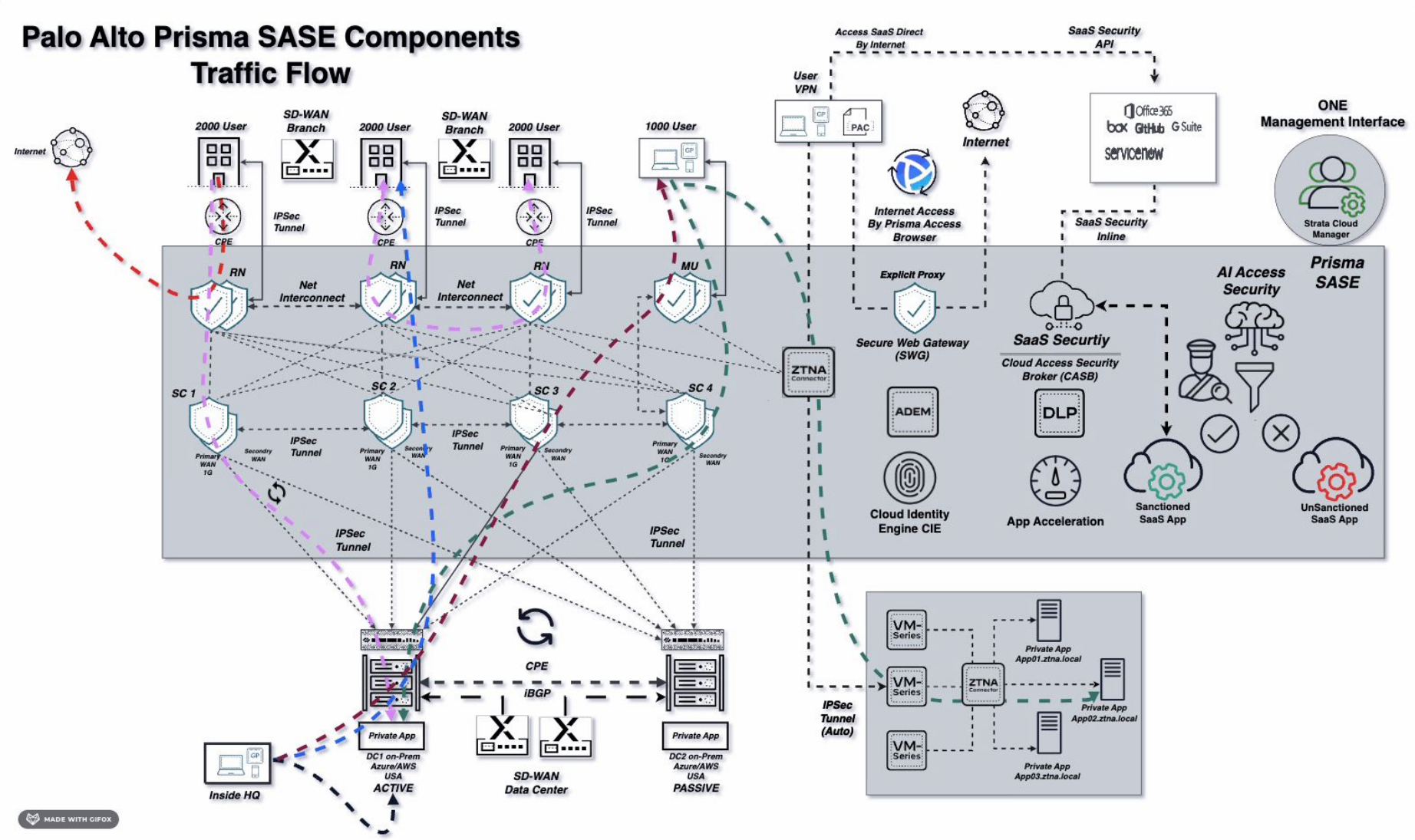
원격 접속 + 랜섬웨어/악성 코드 탐지 + 사용자 ID 연동



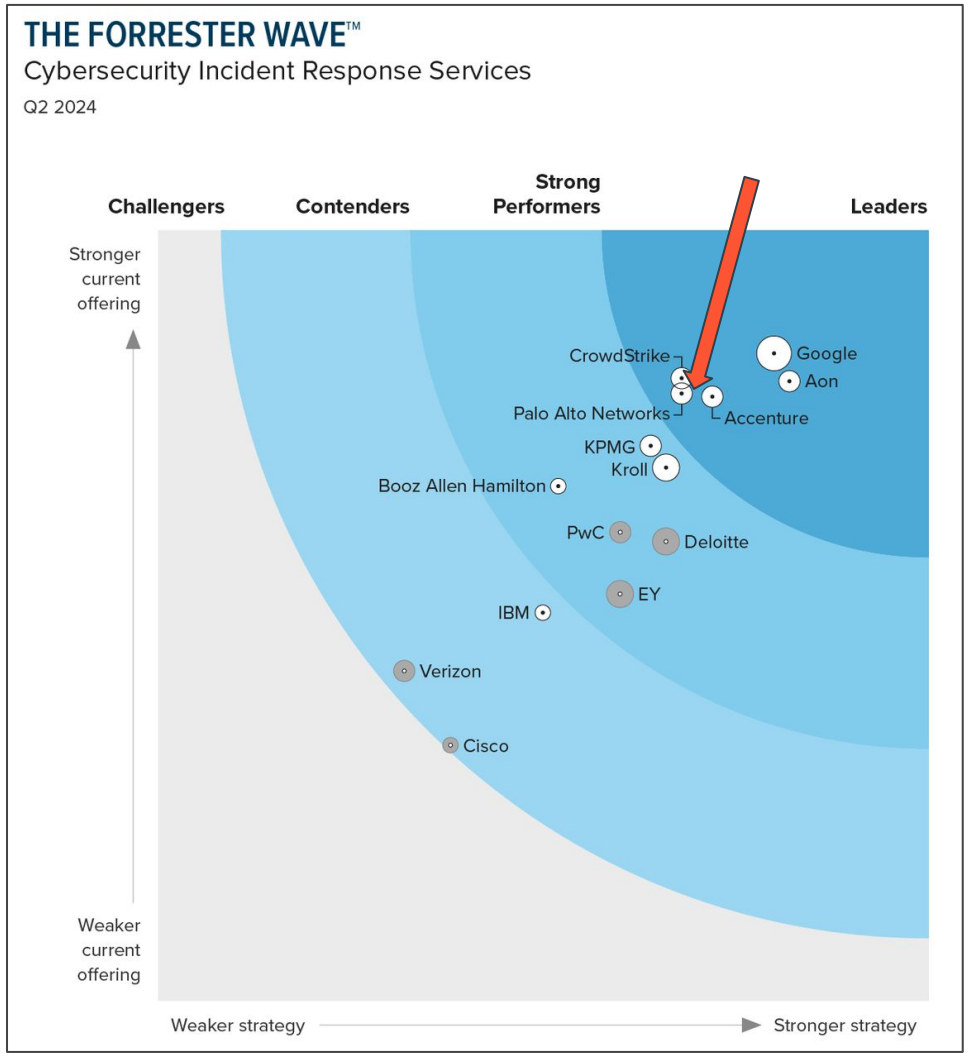
(1) 포털을 통한 TLS/SSL 설정
(2) RTT 기반 자동 게이트웨이 검색
(3) 가장 가까운 게이트웨이로 IPsec 터널 설정
(4) 리소스에 대한 보안 액세스



전통적인 VPN (SD-WAN, IPSec / SSL VPN) 한계 극복을 위한, 제로 트러스트 기반의 글로벌 고객 SASE 도입 아키텍처 및 트래픽 플로우



미국 컨설팅 시장 평가, 포레스터 웨이브™ : **사이버 침해 사고 대응 IR** 서비스 벤더 중, 리더 그룹으로 선정된 팔로 알토 네트웍스 Unit 42 (유닛 42)



"[유닛 42]는 지난 2년간 최고의 리더십 인재를 영입하고 글로벌 입지를 구축했으며, 자체 제품과 서비스를 보완하기 위해 파트너 네트워크를 확장하여 대형 IR 회사 및 대형 컨설팅 업체와 경쟁할 수 있게 되었습니다."

- **Unit 42 Named a Leader** 포레스터 웨이브™에서 리더로 선정: 사이버 보안 사고 대응 서비스, 2024년 2분기 기준
- 혁신, 기술, 위협 인텔리전스, 클라우드 환경에서의 IR, IR 리더십 및 팀 구조 등 9개 기준에서 최고 점수를 획득했습니다.
- **중요 차별점 : 한국에 진출한 벤더 중, 보안만 지원하는 기술/영업/마케팅 인력 규모**
  - **팔로 알토 네트웍스 코리아 : 60명-70명**
  - **경쟁사 : 1~5명**