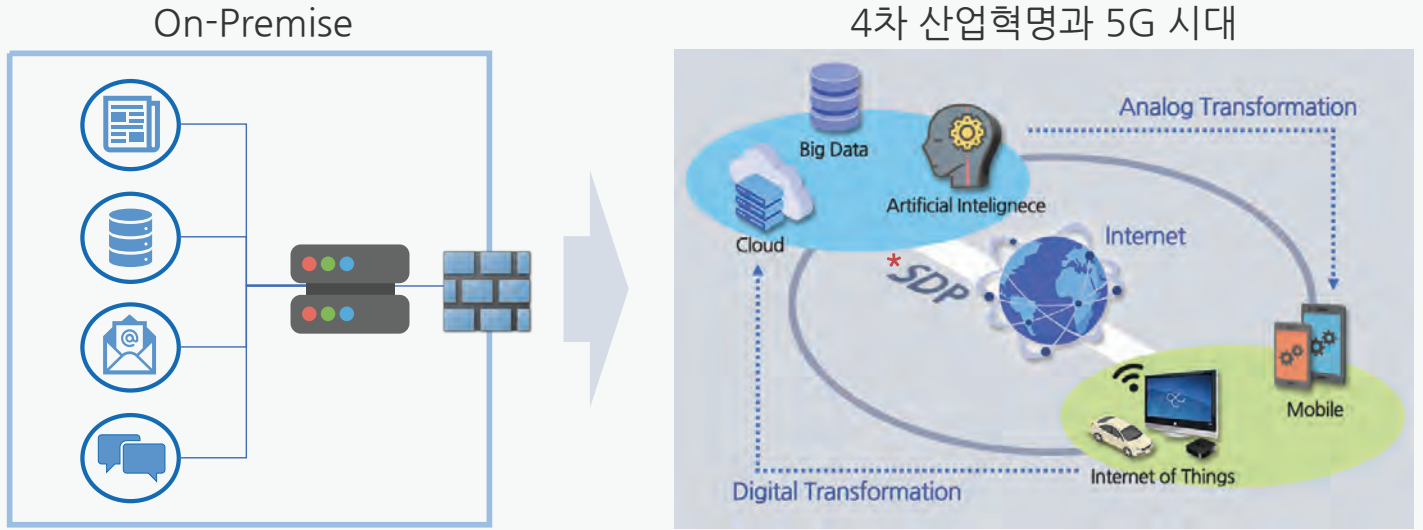


장소에 구애 받지 않고 언제 어디서나 사내 업무를...

4차 산업혁명과 5G 시대를 맞아 BigData와 AI를 이용한 초지능·초연결 사회로 급속히 바뀌고 있으며, 이에 따라 기업의 전산망은 폐쇄적인 사내(On-Premise) 전산체계에서 개방적인 클라우드(Cloud) 체계로 전환되고 있습니다. 이에 대한 성패는 Zero-Trust 보안에 있습니다.



*SDP : Software Defined Perimeter

02 현 상황

정보의 주요 매개체인 Endpoint(PC, Notebook, Mobile, IoT)의 관리,통제 및 보안방법이 전세계적으로 새롭게 변화, 강화되고 있음 (Endpoint Security)

- 단순 관리에서 정책에 의한 통제 (NAC)
- 사내업무(On-Premise) 체계에서 클라우드 체계
- 한정 지역 내 사용에서 전세계 어느 곳에서도 사용

네트워크 보안중심에서 개인인증 보안중심으로 전환하는 추세

네트워크 중심적 보안

↓

사용자 중심적 보안

클라우드로 확장된 보안경계를 위해 전통적 보안시스템에서 새로운 사이버보안 패러다임 출현

Network : VPN, FW, IPS, IDS
Threat : DDoS, APT
Endpoint : NAC, 망분리

↓

Zero-Trust



04 개선 방안



선 인증과 다단계 접근통제를 통해 허가된 사용자/단말만 망 접속을 허용하는 **신뢰 연결(Trust Connectivity) 방식**

Trust Connectivity

Multi-Factor 인증 ➡ Verify ➡ Connect



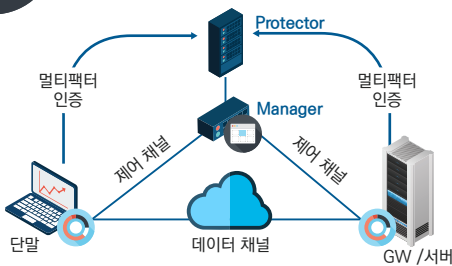
접속 및 연결되는 모든 대상을 **매니저로 관리·제어**함으로써 효율적·신뢰적인 **통합관리 기능**



MLsoft
+
ETRI



관리·제어 망과 데이터 망을 종단간 **신뢰 터널로 분리적으로 운용**



보호할 도메인에 **Black/Dark 네트워크**를 구성하여 공격자에게 노출되지 않는 **강건한 구조의 DDoS 방지 설계**로 자원 소모를 방지



1 VPN 보안 문제

클라우드로 확장된 비즈니스 환경에서는 보안의 경계를 효과적으로 확보하기 어렵습니다. 기존 VPN을 이용한 작업자의 원격접속은 지정된 리소스 외에도 광범위한 네트워크에 접속이 가능하여 보안 취약점이 발생합니다.

2 제로 트러스트 네트워크

사용자 및 기기가 인증되고 권한이 부여될 때까지 중요 응용프로그램 및 서비스가 노출 또는, 접속되지 않도록 하여 네트워크 보안 위험을 줄여줍니다.

3 사용자 중심 네트워크

IP, 세그먼트가 아닌 사용자 중심으로 네트워크를 구성하여 액세스 권한을 부여합니다.

4 접근성

귀찮은 관리 요구 사항 (방화벽, IPS 등)이나 하드웨어 비용을 들이지 않고도 간단한 로그인으로 사용자가 필요로 하는 서비스에 효율적으로 연결할 수 있습니다.

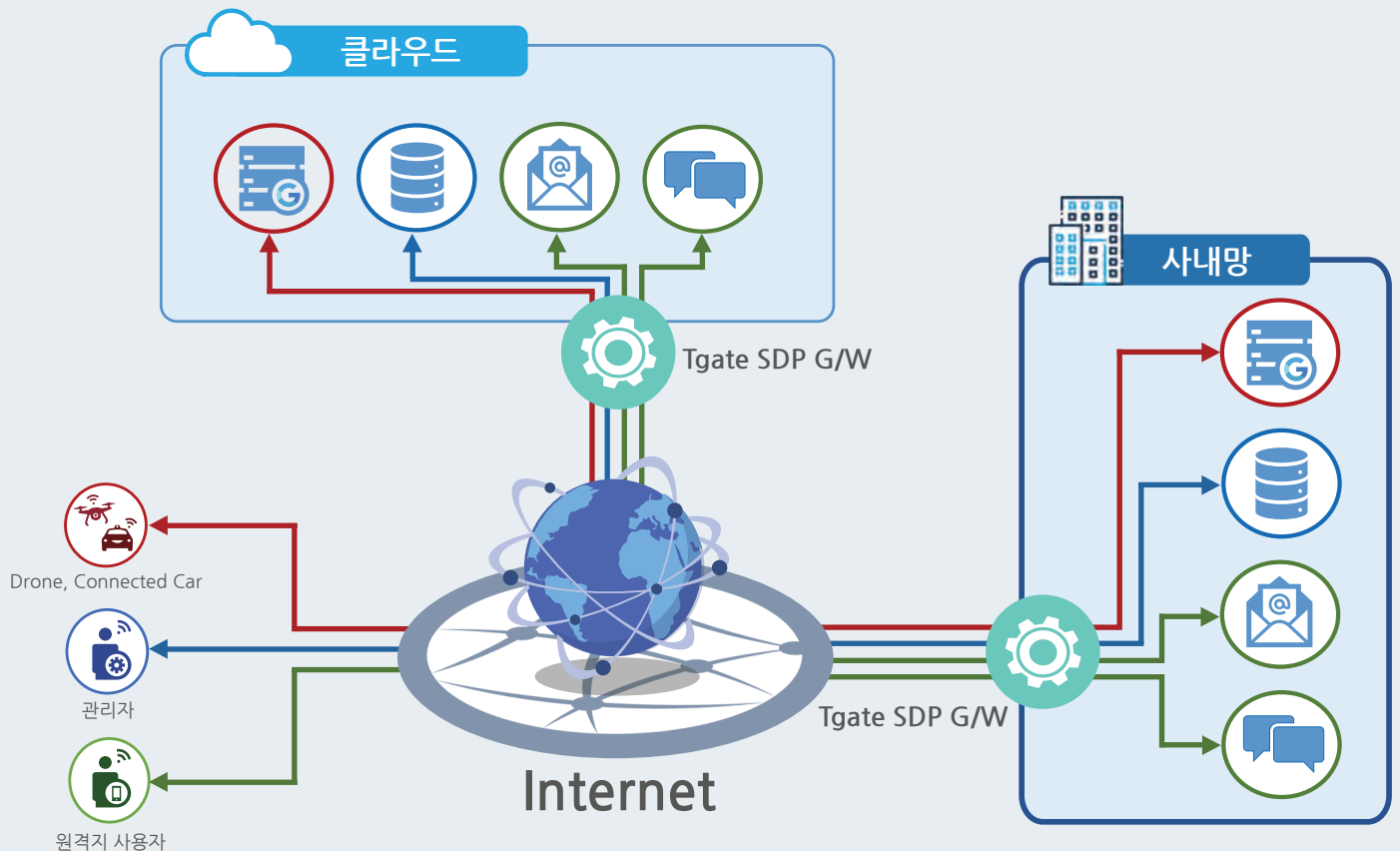
5 확장성

사용자 수나 액세스해야 하는 애플리케이션 수가 증가 또는 감소함에 따라 클라우드에서 유연하게 확장할 수 있습니다.

6 비용

복잡한 IT 환경에 쉽게 배치할 수 있고, 비싼 장비를 구입하거나 추가로 임대할 필요 없이 필요할 때 보안 기능을 손쉽게 확장 할 수 있습니다.

06 SDP 개념도





User centric security
네트워크 중심적 보안에서 사용자 중심적 보안

SDP + NAC
SDP와 NAC(Network Access Control) 가 결합한 세계 최초의 보급형 SDP

Availability
On-Premise와 Cloud 환경하에서 모두 사용가능

Easy SDK
SDK 제공으로 쉬운 Agent 개발과 AppBinding 제공

Flexible
SW 방식의 다양한 보안 네트워크 구성 가능

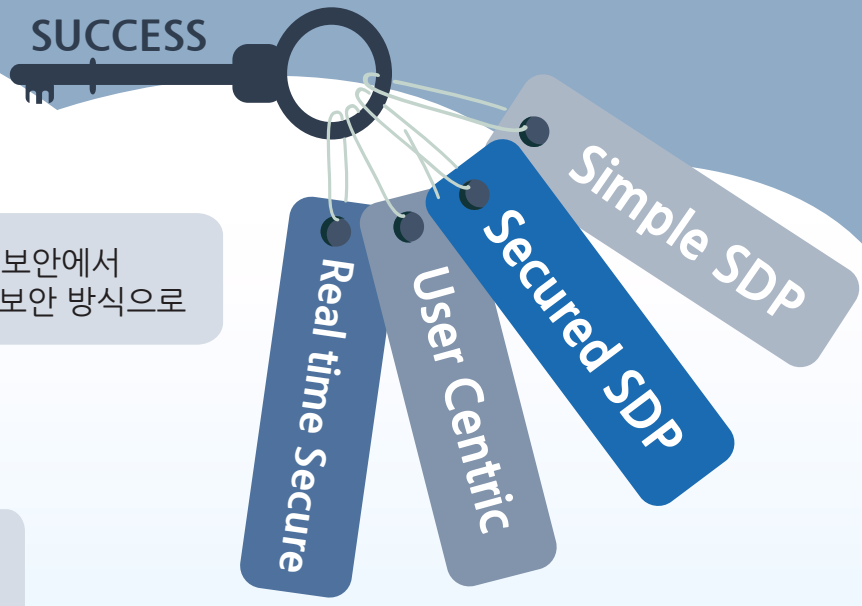
08 기대효과

1 폐쇄적인 망분리 보안에서 개방적인 SDP 보안으로

2 VPN 방식의 선접속 후인증 보안에서 SDP 방식의 선인증 후접속 보안 방식으로

3 네트워크 중심적 보안에서 사용자 중심적 보안으로

4 개별적 보안에서 통합적 실시간 보안으로



01 무엇이 SDP인가?

- ☑ SDP는 클라우드, 빅데이터, AI를 위한 필수 보안 서비스
- ☑ PC 및 모바일, 각종 IoT 장비의 네트워크 보안 강화
- ☑ 인터넷상에서 서비스연결 대상을 숨김으로써 공격 노출 영역 최소화
- ☑ 인터넷 환경에서 가지는 전통적 네트워크 보안시스템의 한계 극복
- ☑ 네트워크 중심에서 사용자 중심으로 네트워크 구성

02 누가 SDP를 필요로 하는가?

- ☑ 클라우드 및 폐쇄망 인터넷 네트워크를 통해서 접속한 BYOD 사용자
- 군, 정부, 금융, 기업, 병원, 물류, 중소기업 등
- ☑ 모빌리티 산업 - 커넥티드 카, 드론
- ☑ VPN 사용자 - 차기 보안을 위한 대체
- ☑ 가정용 IoT 보안을 위한 사용자 - AP장치, 셋탑박스, IoT 카메라 등

03 왜 Tgate SDP인가?

- ☑ 사용자(ID) 중심의 정책에 의해 운영되며 관리 및 통제가 용이
- ☑ AD 또는 LDAP 유무 관계없이 동작하는 단순 하지만 완벽한 IAM
- ☑ 이중 보안 컨트롤러와 다중 인증 지원
- ☑ App-Binding 지원
- ☑ SDK를 통한 전용서비스 접속 통제 지원
- ☑ 간편한 구현 및 합리적인 가격

SDP 기술, NAC 기술, IP관리 기술, PC제어 기술을 모두 보유한
Cyber Security 전문 기업