Genians

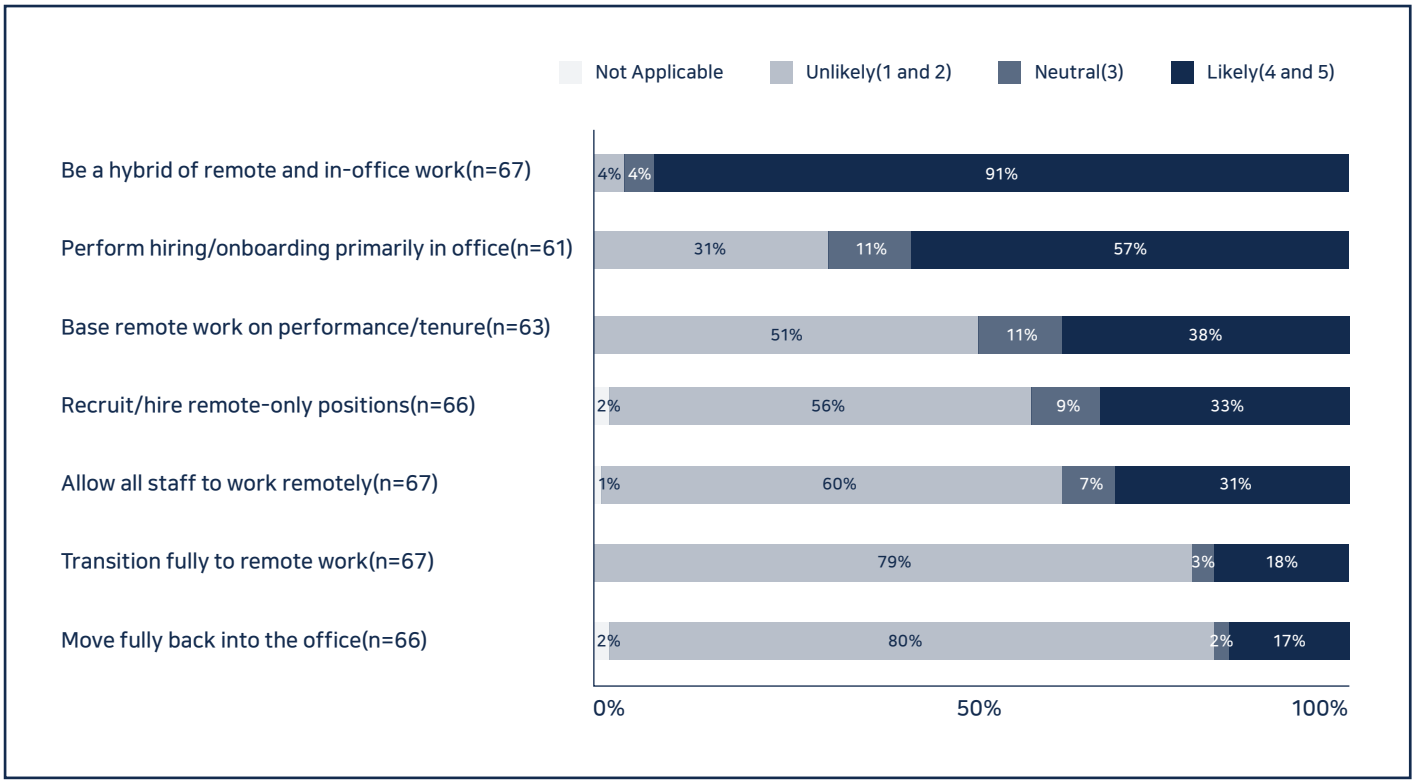
Genian ZTNA (Zero Trust Network Access) 제로트러스트 보안의 완성

WHITE PAPER

1. Introduction(포스트 코로나 그리고 해결과제)

코로나(Covid-19) 긴 터널의 끝이 보입니다. 코로나는 모든 분야에 영향을 주었으며 다양한 변화를 촉발시켰습니다. 기업의 IT 담당자는 급작스런 업무환경의 변화를 수용하면서 동시에 업무 연속성과 보안을 유지해야 했습니다. 그 결과 재택근무와 클라우드, SaaS(Software as a Service)와 사투를 벌여야 했습니다. 그러나 이러한 노력으로 우리는 유례없이 빠른 디지털 전환(DX, Digital Convergence)을 경험했습니다.

그러나 아직 끝나지 않았습니다. 코로나가 종식되어도 변화된 환경은 유지될 것 입니다. 하이브리드 근무(사무실 + 재택근무)는 대중화 되었고 클라우드와 SaaS의 활용은 사실상 표준이 되어가고 있습니다. 기업들은 디지털 전환을 통해 과거의 한계를 빠르게 극복하고 있습니다. 변화에 맞추어 규제나 제도 역시 개선되고 있습니다. 전환은 앞으로도 더욱 가속화 될 것 입니다.



[Hybrid Work Becoming Pervasive, Gartner]

이제 우리는 변화된 환경을 안전하고 견고하게 유지해야 합니다. 미래 보안에 대한 고민이 필요합니다. 불행히도 과거의 보안모델은 도전을 받고 있고 더 이상 효과적이지 않습니다. 변화된 환경에 맞추어 새로운 보안 모델이 필요 합니다.

2. 새로운 접근통제

** 클라우드를 보호하기 위해 다양한 보안기술이 필요합니다. 전문가들은 공통적으로 3가지를 언급하고 있습니다. 인증과 식별, 데이터 보호(암호화 등) 그리고 접근통제 입니다. 본 백서에서는 이 중, 접근통제에 관해서만 언급합니다.*

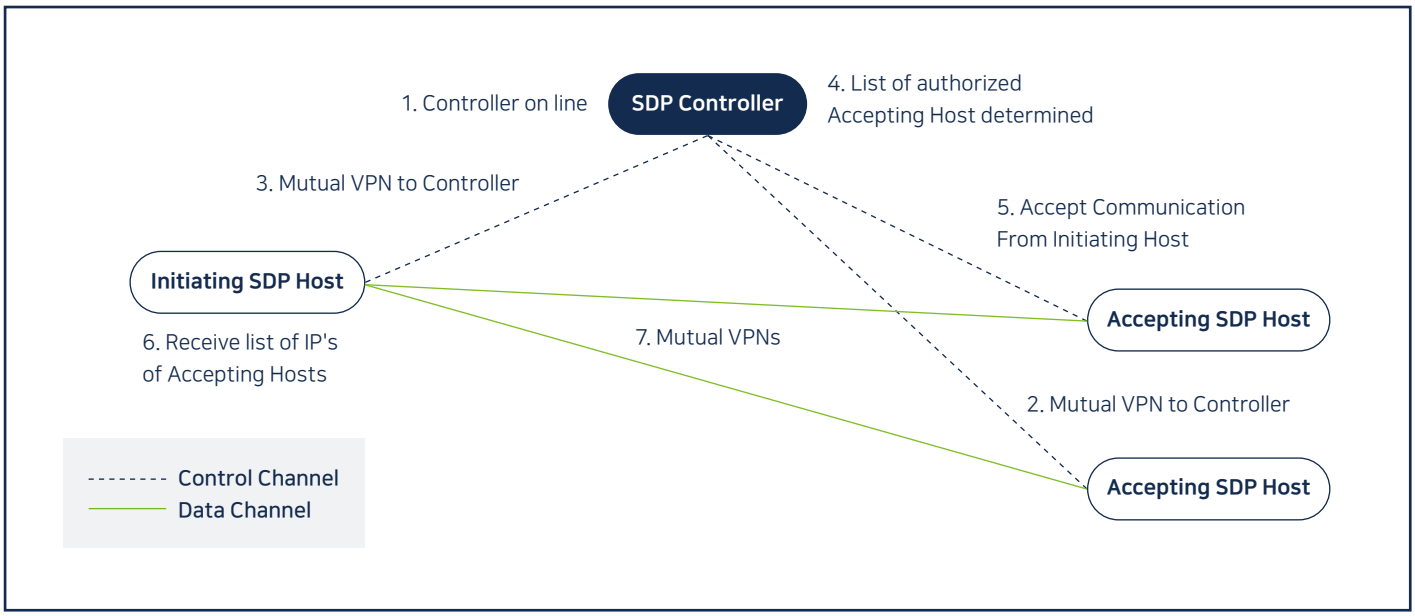
새로운 환경으로 인해 기존의 보안 모델이 도전을 받고 있습니다. 대표적으로 '신뢰(Trust) 기반의 경계선(Perimeter) 모델'을 들 수 있습니다. 이것은 내부(신뢰)와 외부(비신뢰)를 나누고 경계를 강화하는 (Castle and Moat) 네트워크 보안 모델의 기본이었습니다. 그러나 변화된 환경에서는 더 이상 효과적이지 않습니다. 가장 큰 변화는 '원격지(재택)와 클라우드' 입니다. 이로 인해 내부와 외부의 구분이 불가능 해 졌습니다. 내부자는 어디에나 있고 서비스와 접근이 필요한 자원(Resource) 역시 안팎에 존재 합니다. 위치에 따른 신뢰는 모델은 무너졌습니다.

이를 해결하기 위해 다양한 네트워크 접근통제 모델이 제시 되고 있습니다. 특히 클라우드 접근통제는 그 특성으로 인해 기존 모델의 적용이 어렵습니다. 5 Tuple (IP 및 Port 정보)은 더 이상 유효하지 않으며 클라우드 모델(IaaS, PaaS & SaaS)에 따라 어플라이언스(H/W), 가상머신(VM), 컨테이너, 애플리케이션 등 통제의 대상(Object) 역시 다양합니다. 아울러 클라우드 사업자(CSP, Cloud Service Provider)의 API(Application Programming Interface) 제공 여부 등에 따라 접근통제의 정도(Granularity) 역시 달라질 수 있습니다.

그럼에도 클라우드 접근통제를 위한 대안은 존재 합니다. 각각의 올바른 이해를 통해 접근통제의 대상 및 정책을 고려한 최적의 방법을 선택할 수 있습니다. 본 백서에서는 SDP, CASB, SWG 그리고 SASE를 소개 합니다.

A. SDP (Software Defined Perimeter, 소프트웨어 정의 경계)

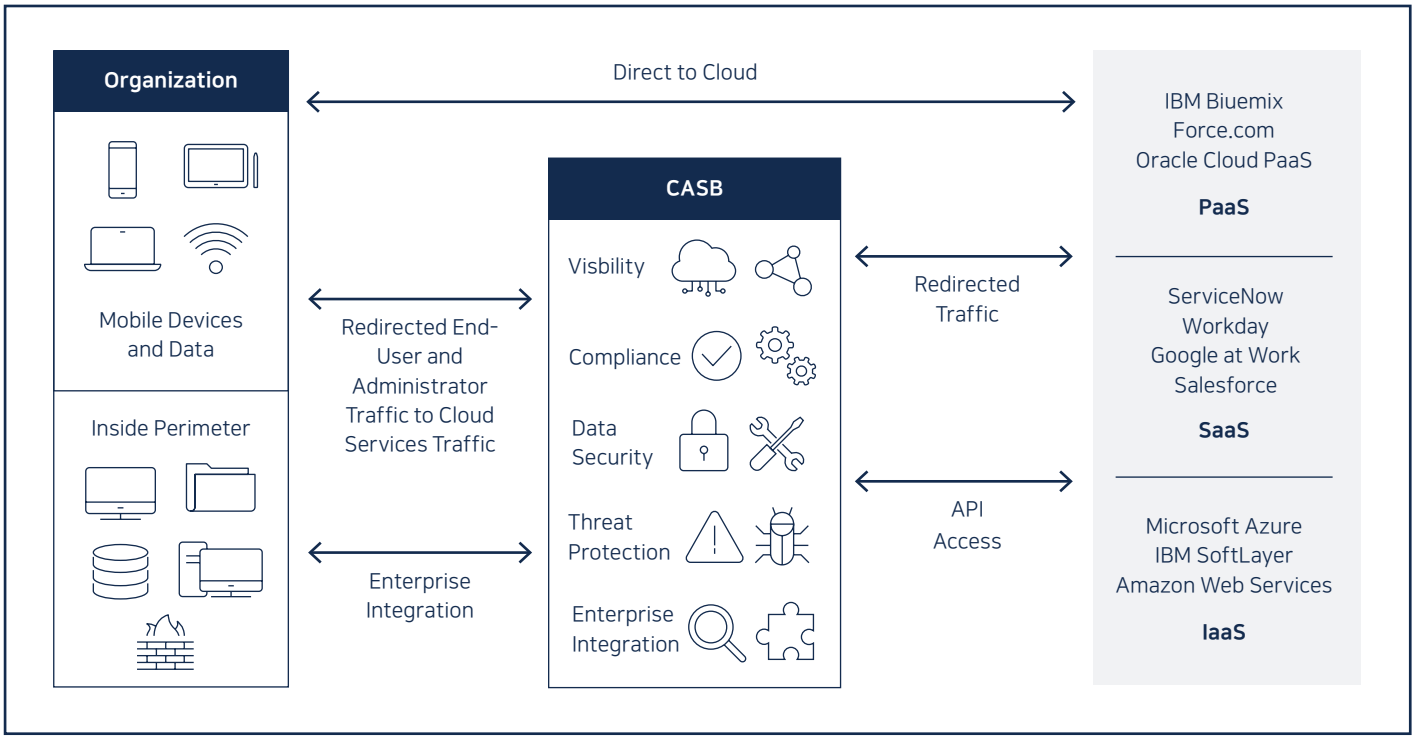
SDP는 CSA(Cloud Security Alliance)가 추진하는 접근통제를 위한 차세대 프레임워크 입니다. SDP는 컨트롤러, 게이트웨이(또는 서버), 클라이언트로 구성되어 모호해진 경계를 명확히 설정할 수 있으며, 이를 기반으로 접근통제를 수행합니다. 기존의 네트워크가 '선 연결, 후 인증' 방식 인 것에 비해 SDP는 '선 인증, 후 연결' 방식으로 동작하여 인증 결과에 따라 연결이 제한됩니다. 이러한 특징으로 권한이 없는 사용자(인증 실패자)는 연결 대상을 확인조차 할 수 없는 상태가 됩니다. 이것이 SDP를 '블랙 클라우드(Black Cloud)' 기술 이라고 부르는 이유이기도 합니다.



[SDP 아키텍쳐, SDP Specification 1.0, CSA]

B. CASB (Cloud Access Security Broker)

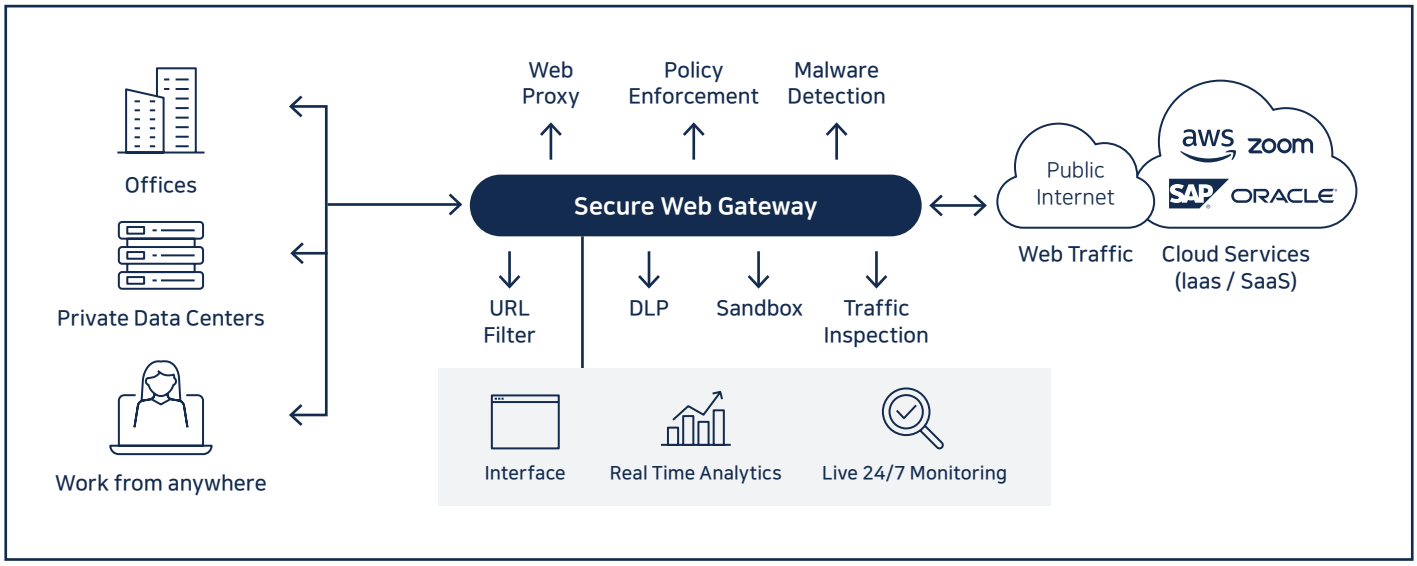
CASB는 이용자와 클라우스 서비스 사이에 위치하여 독립적으로 보안 기능을 수행하는 솔루션 입니다. 에이전트, 어플라이언스(Appliance), API 등 다양한 형태로 제공됩니다. 클라우드 서비스 이용에 대한 가시성, 접근제어, 내부정보 유출방지(DLP), 이상탐지, 로깅(Logging), 감사(Audit) 등의 보안 기능을 수행합니다. 일반적인 CASB는 API를 통해 보안 기능을 제공하며 클라우드 서비스에 특화된 정교한 보안 정책을 제공합니다. 반면 신규 서비스에 대한 지속적인 지원이 필요 합니다.



[CASB – 클라우드 접속 보안 브로커, ITFIND]

C. SWG (Secure Web Gateway)

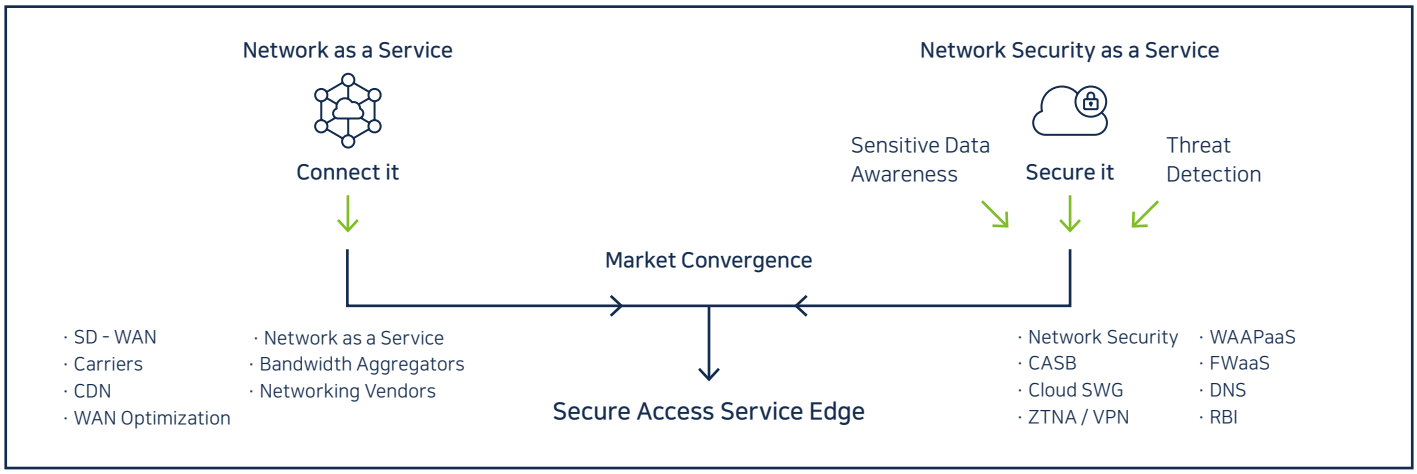
SWG 역시 사용자와 클라우드 사이에 위치 합니다. 다수의 클라우드 서비스는 웹(web) 기반이며 SWG는 웹에 특화된 기능을 제공합니다. 보안 정책에 따라 데이터 유출 방지, 안티바이러스, URL 필터링, HTTPS 검사, 애플리케이션 제어 등의 보안 기능을 제공합니다. SWG는 웹 콘텐츠가 내부에 도달하기 전에 이를 선별하고 필터링 할 수 있습니다. 이것은 매우 큰 장점이지만 모든 트래픽이 SWG를 경유해야 합니다. 따라서 독립적으로 실행되거나 또는 SASE의 일부로 배포되어 사용될 수 있습니다. SWG와 CASB는 제공하는 보안 기능의 수준(Granular) 과 범위(Coverage) 차이가 있습니다. 그러나 아래 SASE 또는 SSE(Secure Service Edge) 등의 모델에서는 통합된 형태로 제공될 수 있습니다.



[How Secure Web Gateway Works, Toolbox]

D. SASE (Secure Access & Service Edge, 새시)

SASE는 2019년 가트너(Gartner)가 제시한 새로운 개념으로 네트워크와 보안이 통합이 핵심입니다. SASE는 WAN(Wide Area Network)과 CASB, FWaaS(Firewall as a Service), SDP, SWG 등의 보안서비스를 단일 클라우드 또는 플랫폼으로 통합하여 제공합니다. 가트너는 이를 통해 다양한 네트워크 환경 및 보안 서비스 구축에 대한 유연성을 확보하면서 비용과 복잡성을 감소시킬 수 있다고 예상합니다. 또한 모든 연결과 컨텐츠를 SASE에서 검사하는 것으로 가시성과 보안성을 동시에 확보할 수 있다고 기대하고 있습니다.



[SASE Convergence – The Future of Network is in the Cloud, Gartner]

3 . 제로트러스트(Zero Trust)

가장 큰 환경의 변화는 '사무실(HQ)과 원격지(Home & Branch) 그리고 클라우드(IaaS & SaaS)' 라고 할 수 있습니다. 이렇게 복잡하고 분산된 환경에서 어떻게 균일하고 높은 보안수준을 유지할 수 있을까요? 이것이 제로트러스트 보안 모델이 주목 받는 이유입니다.

제로트러스트는 이미 침해가 발생했다(Compromised)는 가정하에 불확실성을 제거하고 피해를 최소화 하기 위한 보안모델(컨셉) 입니다. **제로트러스트의 핵심은 '데이터(Data) 중심 아키텍처' 라는 점** 입니다. 따라서 기존 경계선(Perimeter)과 신뢰(Trust/Untrust)기반의 보안 모델로 해결이 어려운 지금의 상황을 효과적으로 해결할 수 있습니다. 제로트러스트는 지금의 (모든)보안 솔루션 또는 서비스가 수용해야 하는 철학 또는 원칙(Tenet)이 라고 할 수 있습니다.

이미 시장에는 제로트러스트와 관련된 다양한 정의와 용어가 사용되고 있습니다.
관련 내용(https://genians.co.kr/genians-nac/zt/)을 참고하십시오.

A. 제로트러스트 원칙 (Tenets of Zero Trust)

미국국립표준기술연구소(NIST)는 제로트러스트의 이해 및 적용을 위한 다양한 가이드라인을 제시하고 있습니다. 이 중 'Zero Trust Architecture(NIST Special Publication 800-207)'에서는 제로트러스트의 개념과 함께 기본 원칙을 제시하고 있습니다. 아래의 내용은 신뢰성이 보장되지 않은 네트워크 환경을 가정하여 최소한의 권한(엑세스 최소화)과 세밀한 통제(지속적 인증/인가)를 수행하기 위한 일곱 가지 원칙과 세부 내용을 언급하고 있습니다.

① 모든 데이터 소스와 컴퓨팅 서비스는 리소스로 간주
네트워크는 스토리지, SaaS, 개인 소유 단말기 등 여러 종류의 디바이스로 구성될 수 있으며 이는 모두 리소스로 간주함

② 네트워크 위치에 관계 없이 모든 통신 보호
단말이 기업 내부 네트워크에 있다고 해서 신뢰를 보장하지 않으며, 모든 통신의 기밀성과 무결성을 보호해야 함

③ 기업 리소스에 대한 엑세스를 세션 단위로 승인
작업을 완료하는데 필요한 최소한의 접근으로 엑세스를 허가하며, 각 세션에 따라 달리 검토하여 승인해야 함

④ 동적 정책으로 리소스에 대한 접근 결정
동적 정책에는 클라이언트 아이덴티티(Identity), 어플리케이션, 요청을 보낸 자산상태, 행동 및 환경 속성 등이 포함되며, 동적으로 리소스의 접근 결정 필요

⑤ 모든 자산의 무결성 및 보안 상태 감시 조치
기본적으로 자산을 신뢰하지 않으며, 리소스에 대한 접근요청을 판단할 때 자산 상태 감시, 필요에 따라 패치 등 보완조치 및 모니터링

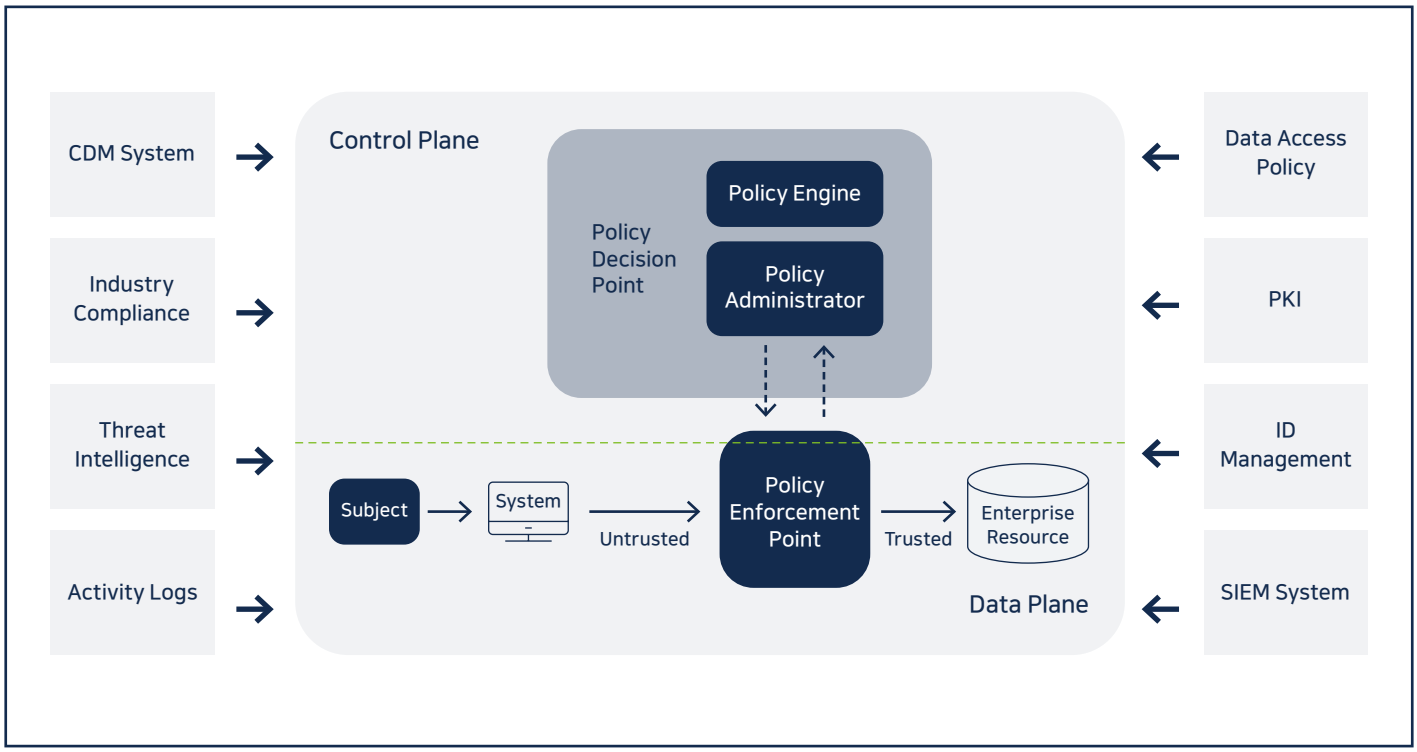
⑥ 모든 리소스의 인증/인가를 강력하게 점검 후 허용
모든 리소스에 대해 '접근-위협평가-조정-(지속적)재평가' 라는 일정한 주기로 ICAM(Identity, Credential, and Access Management), 자산관리 시스템 및 다중 인증(MFA) 사용을 권장함

⑦ 자산, 네트워크, 인프라 등 현 상태에 대한 정보 수집
자산의 보안상태, 네트워크 트래픽, 엑세스 요청과 관련된 데이터를 수집하고 처리하여 획득한 지식을 보안 정책을 개선하기 위해 사용해야 함

[Tenets of Zero Trust, Zero Trust Architecture, NIST]

B. 제로트러스트 아키텍쳐 (Zero Trust Architecture)

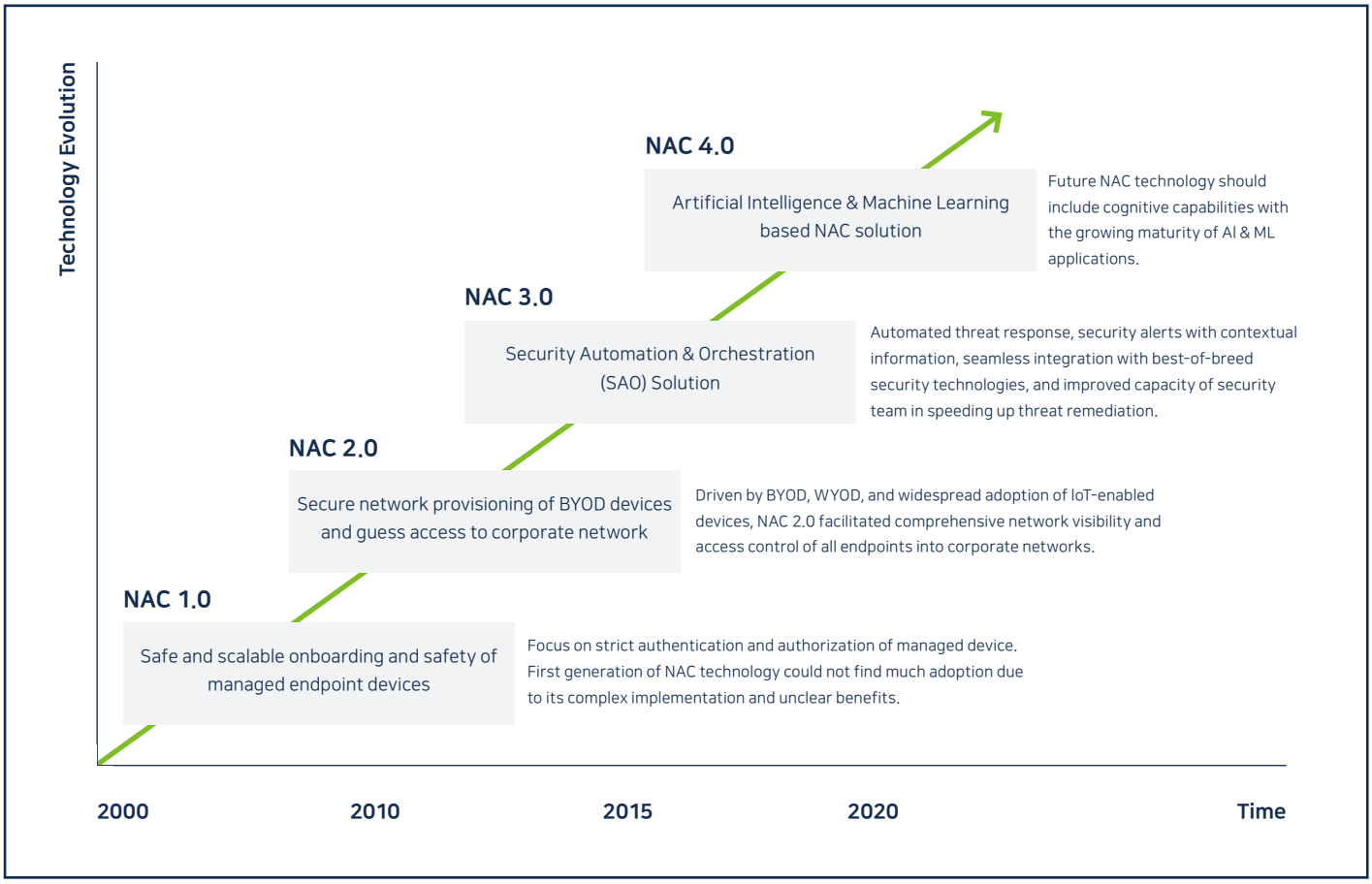
보안모델을 이해하는 것과 실제 적용하는 것은 다른 문제 입니다. 제로트러스트의 적용을 위해 제로트러스트 아키텍처를 참고할 수 있습니다. 앞에서 제로트러스트를 위한 원칙을 언급하였습니다. 내용에 따르면 '제로트러스트 아키텍처는 (기업 내) 존재하는 구성요소(component)의 관계, 워크플로우, 접근정책 등에 제로트러스트(컨셉)를 적용하기 위한 사이버보안 계획' 이라고 이해할 수 있습니다. 그럼 누구를 대상으로 어떻게 관계나 워크플로우를 이해하고 정보를 확인하여 최소한의 권한을 부여하고 세밀한 통제를 해야 할까요? 결국 제로트러스트 아키텍처(ZTA)의 시작은 **'누구(Components)' 를 어떻게 누락 없이 탐지하고 식별할 수 있는지의 가시성(Visibility)의 확보'** 라고 할 수 있습니다. 즉 여기서의 누구는 조직활동에 참여하는 모든 자산(Asset)이라고 할 수 있으며 구성원(사람)을 포함하여 서버, 네트워크 장비, 어플리케이션뿐만 아니라 정책, 워크플로우, 네트워크 연결 등 모든 것이 포함된다고 할 수 있습니다.



[Core Zero Trust Logical Components, Zero Trust Architecture, NIST]

4. 제로트러스트와 NAC(Network Access Control)

NAC는 오랜 기간 내부 보안을 위한 플랫폼으로 확고히 자리매김 하였습니다. 보안정책에 따라 사용자 및 단말에 대한 접근통제뿐 아니라 통합인증(IAM), IP관리(IPM), 자산관리(DMS), 패치관리(PMS) 등의 부가기능을 제공하였습니다. 현재의 NAC는 5G, IoT 등 단말의 증가와 보안환경의 복잡성을 해소하기 위해 보안자동화(Security Automation) 및 오케스트레이션(Orchestration)을 지원하고 인공지능이나 머신러닝(Machine Learning) 기술이 적용되고 있습니다.



[NAC의 발전, Market Outlook: Network Access Control, 2018 – 2023, Quadrant]

그러나 이제 신뢰를 기반으로 하는 경계선 보안이 무너지는 환경이 도래하면서 NAC는 새로운 도전에 직면하고 있습니다. 불행히도 NAC는 변화된 환경과 제로트러스트를 지원하기에 충분하지 않습니다. 지니언스㈜는 1등 NAC 개발사로 NAC의 한계를 명확하게 인지하고 있습니다.

A. NAC의 한계

① CLOUD 확장의 한계

내부통제를 목적으로 구축한 NAC는 클라우드를 지원할 수 없습니다. 여기에는 내부 자산의 이동(IaaS, PaaS) 뿐 아니라 애플리케이션(SaaS)의 통제 역시 포함됩니다.

② VLAN 구성에 의존

다수의 NAC 솔루션에서 통제를 위해 VLAN 구성이 요구됩니다. VLAN을 구성하는 것은 어렵지 않습니다. 그러나 VLAN의 확장에는 물리적 한계가 존재하며 항상 최신의 상태로 유지되는 것은 또 다른 문제 입니다.

③ 트래픽 암호화

이미 많은 네트워크와 어플리케이션이 암호화(encryption)를 지원합니다. HTTPS, TLS 등을 이용한 통신은 별도의 방법을 이용하지 않는 경우 그 내용을 확인하기 쉽지 않으며 이를 통해 보안정책의 우회가 발생할 수 있습니다.

④ 접근통제 누수

NAC의 접근통제 정책은 존재하거나 접근이 가능한 네트워크 및 네트워크 장비를 대상으로 합니다. 만약 IP를 보유하고 있지 않거나 IP가 수시로 변하는 대상이 있다면 이것에 대한 접근제어 정책을 수립 운용하기는 쉽지 않습니다.

⑤ 원격지 사용자(Remote User)

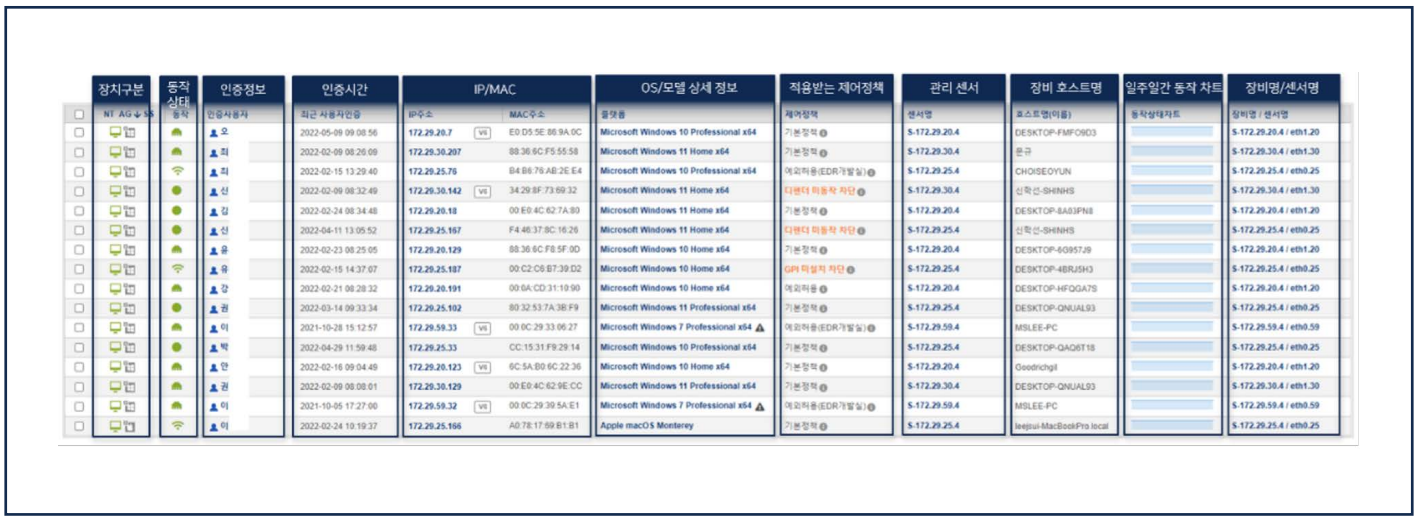
원격지 사용자가 내부 접근을 시도하거나 원격지 간의 접근을 시도하는 행위에 대하여 NAC는 효과적인 대응방법을 제공하지 못 합니다. 별도의 클라이언트 에이전트 또는 사용자 인증 등이 필요할 수 있습니다. 복잡한 보안정책의 운용이 필요할 수 있습니다.

⑥ 동적(Dynamic) 업무환경

5 tuple(IP, Port, Protocol 등)기반의 전통적인 NAC 보안정책은 동적 업무환경을 지원하기에 충분하지 않습니다. WFA(Work From Anywhere)를 위해 IP를 기반으로 누수 없는 접근제어 정책을 수립하는 것은 용이하지 않습니다.

B. NAC의 가능성

그럼에도 우리는 NAC의 가능성을 확인할 수 있습니다. 앞서 설명한 제로트러스트원칙(Tenets of Zero Trust)에 해답이 있습니다. 위의 원칙을 간단히 정리하자면 모든 **'자산(Asset)에 대하여 지속적인 보안성(무결성 등)을 검증하여 최소한의 (접근)권을 부여할 것'** 이라고 할 수 있습니다. NAC는 제로트러스트가 주목을 받기 이전부터 이미 이러한 원칙을 준수하고 있었습니다. NAC는 사용자(인증) 및 내부 자산에 대한 가장 많은 정보를 보유하고 있으며 이를 통한 가시성(Visibility)의 확보와 다양한 정보의 조합을 통한 보안정책의 운용이 가능합니다. 또한 단말과 네트워크에서 다양한 통제를 수행할 수 있습니다.



[Genian NAC 가 제공하는 사용자 및 단말 가시성, 지니언스]

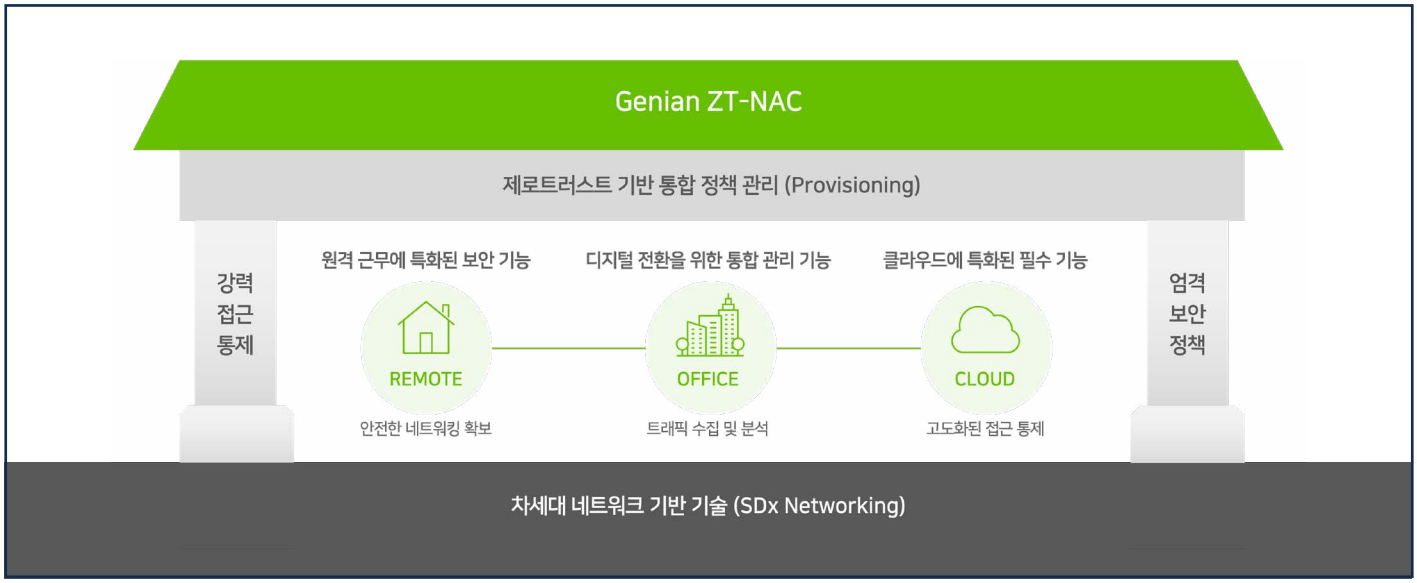
가트너(Gartner)는 '2021 Market Guide for Network Access Control' 보고서를 통해 '다수의 기업이 NAC가 제공하는 포괄적인 가시성과 인증을 기반으로 제로트러스트 전략을 통해 사용자 및 단말의 보안을 강화하는 것에 관심이 많다' 라고 첫 번째로 언급하면서 제로트러스트와 NAC의 가능성을 언급하고 있습니다. 이제 필요한 것은 NAC의 역할범위를 원격지와 클라우드로 확대함과 동시에 통제의 수준을 어플리케이션과 컨택스트(Context) 수준까지 정교화 하는 일 입니다.

5. 제로트러스트 보안의 모든 것, Genian ZTNA(Zero Trust Network Access)

Genian ZTNA는 제로트러스트 보안을 위한 이상적인 솔루션 입니다. 우리는 누구보다 NAC를 잘 이해하고 있습니다. 우리의 전문성은 기술에 국한되지 않습니다. NAC를 도입하고 관리해야 하는 운영자 그리고 NAC의 (영향을 받는)사용자에 대해서도 잘 알고 있습니다. 사내에서 운영되던 보안 정책은 사용자와 자산(Asset)의 이동에 맞추어 원격지와 클라우드에도 동일하게 적용되어야 합니다. 새로운 서비스(SaaS)는 사용자의 역할과 위치, 권한, 목적 등에 따라 적절히 통제 되어야 합니다. 이를 위한 보안 정책은 중앙에서 통합관리되어야 하며 원격지와 클라우드에 균일하게 적용되어야 합니다.
새로운 업무 환경에 맞는 Genian NAC의 확장, 이것이 Genian ZTNA의 핵심 입니다.

A. Genian ZTNA 아키텍쳐

지난해 발간된 '(백서) 재택근무자 보안, VPN 과 VDI 만으로 충분한가요?' 에는 Genian NAC의 발전 방향에 대한 고민이 보입니다. 여기에서 원격지를 포함한 WFA(Work From Anywhere) 보안을 위한 궁극의 대안으로 제로트러스트를 언급하고 있습니다. WFA는 광범위한 엑세스 환경의 일부이며 클라우드도 포함됩니다. Genian ZTNA는 이러한 고민에 대한 해답 입니다. 우리는 원격지와 클라우드를 포함하는 아키텍처를 설계하였으며 핵심적인 보안 기능을 정의 하였습니다.

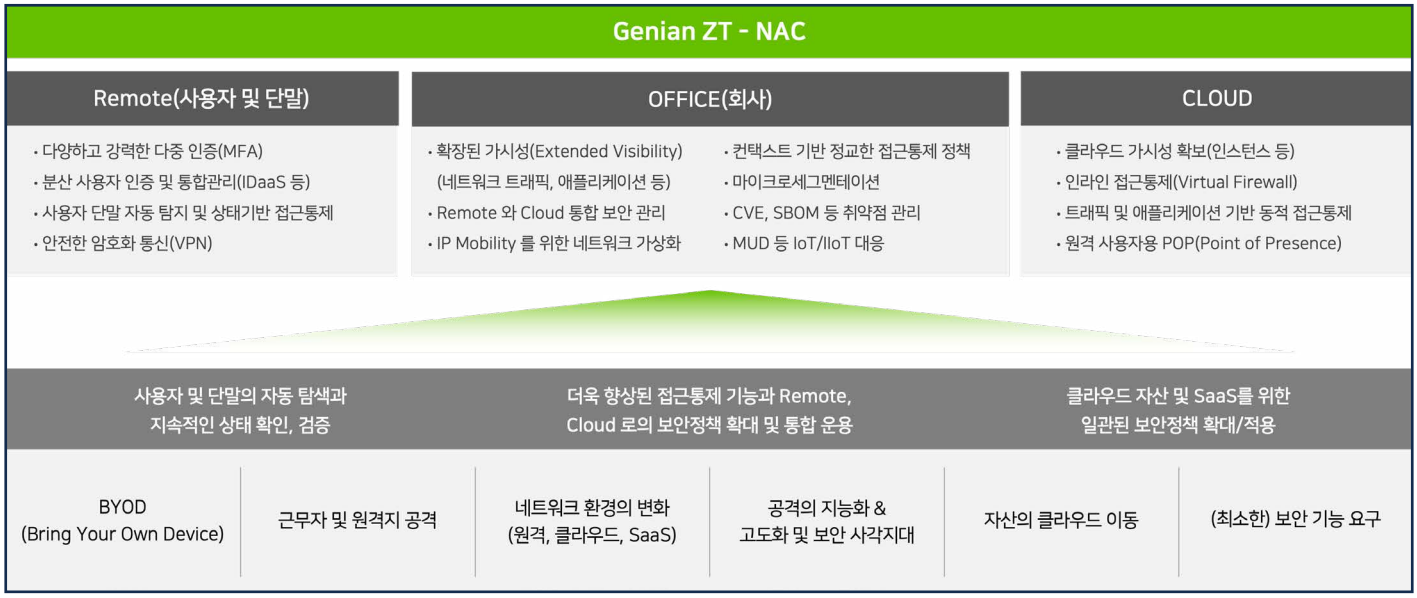


[Genian ZTNA 아키텍처, 지니언스]

Genian ZTNA 아키텍처의 핵심은 분명 합니다. 그것은 '정보수집 – 정책수립 – 접근통제' 라는 NAC의 핵심 기능의 원격지(Remote)과 클라우드(Cloud)로의 확대 입니다. 그러나 그것은 간단하지 않습니다. 클라우드 자산의 정보수집은 사무실(Office)의 방법과 다릅니다. 원격 사용자는 사무실을 거치지 않고 클라우드로 통신할 수 있습니다. 출발지 기준 외에 목적지 기준의 접근통제도 필요 합니다. 출발지와

목적지가 수시로 변하는 환경도 존재 합니다. 이러한 모든 환경에서도 보안정책은 수립되어야 하며 올바르게 동작해야 합니다.

우리는 이러한 문제를 해결하기 위해 제로트러스트를 기반으로 원격지와 클라우드 사무실에 맞는 기능을 선별하였고 핵심 보안스택(Security Stack)을 완성할 수 있었습니다.



[Genian ZTNA 핵심 기능, 지니언스]

B. Genian ZTNA 특장점

Genian ZTNA는 원격지와 클라우드를 위한 특화된 보안기능을 제공합니다.
이를 위해 ZTNA 에이전트와 게이트웨이가 새롭게 개발되었습니다.

① 원격근무를 위한 Always On ZTNA

Genian ZTNA를 통해 기존의 VPN(Virtual Private Network)과 동일한 업무 환경을 구축할 수 있습니다. 뿐만 아니라 게이트웨이를 클라우드에 설치하는 경우 원격 사용자의 모든 트래픽을 클라우드로 통합하고 보안스택을 적용할 수 있습니다. 이것은 SASE (Secure Access, Service Edge)의 개념과 유사합니다. 기업은 이러한 환경을 자체적(Private)으로 운영하거나 서비스 형태(MSSP)로 제공받을 수 있습니다. 사용자와 단말은 강력한 인증을 통해 검증되고 적절한 권한이 부여됩니다. 그리고 권한의 적합성은 업무가 종료될 때까지 반복적으로 검증됩니다. 만약 상태가 변경되거나 정책을 위반하는 경우 그 즉시 다양한 조치가 진행됩니다.

② 클라우드 접근통제 (Cloud Gateway)

클라우드 접근통제의 핵심은 가시성(Visibility)의 확보 입니다. 이것은 클라우드 자산(IaaS, PaaS)으로의 접근과 클라우드 서비스(SaaS)의 이용 모두에 해당합니다. Genian ZTNA는 이를 위해 별도의 보안 게이트웨이가 제공됩니다. 게이트웨이는 클라우드 내부의 자산정보(VM, Instance 등)를 자동으로 수집하며 이를 통해 보안정책을 수립할 수 있습니다. 이를 위해 Security Group 이라는 개념이 도입되었습니다. 클라우드에 존재하는 자산은 개별적인 네트워크 보안정책을 가질 수 있으며 Security Group을 통해 In/Outbound 정책을 수립할 수 있습니다. 또한 게이트웨이를 통과하는 모든 트래픽을

조사하여 애플리케이션 수준의 접근통제를 지원합니다. 게이트웨이는 VPN 종단장치의 역할을 겸하며 어플라이언스(H/W), 가상머신(VM), 컨테이너(Docker) 등의 형태로 설치 운영될 수 있습니다.

③ 더욱 세분화된 정책(Micro Segmentation)

달라진 업무환경에 따라 더욱 세밀한 보안정책이 필요합니다. 수립된 보안 정책은 근무자의 이동 등 네트워크 환경이 변해도 유지되어야 합니다. Genian ZTNA는 애플리케이션 기반의 접근통제를 지원하며 사용자(인증) 역할과 결합하여 마이크로세그멘테이션을 구현할 수 있습니다. 또한 동적(Dynamic) 목적지 제어를 통해 SaaS 애플리케이션의 대응도 가능합니다. 사용자와 단말의 다양한 보안 상태에 따라 필요한 시점(Just In Time)에 필요한 권한(Just Enough Access) 만이 부여 됩니다.

④ FIDO(Fast Identity Online) 지원으로 더욱 강력해진 인증

Genian ZTNA는 FIDO2 인증 표준을 지원합니다. 이를 통해 지문 등 생체인증 기능을 통해 보다 강력한 다중인증체계(MFA) 운영이 가능합니다. FIDO2는 웹 서비스 환경에서도 생체인증이 가능하며 UAF(패스워드 없이 사용) 및 U2F(패스워드와 함께 사용) 방식이 결합된 이상적인 인증방식으로 평가 받고 있습니다. 이제 사용자는 에이전트 인증창에서 FIDO 기반 간편로그인을 통해 Always On ZTNA 정책을 적용 받게 됩니다.

C. 제로트러스트 보안의 완성, Genian ZTNA

앞서 제로트러스트의 7가지 원칙에 대해 언급하였습니다. 그리고 제로트러스트를 위한 NAC의 가능성을 언급하였습니다. Genian ZTNA는 이러한 원칙을 충실히 이행하기 위해 노력하고 있습니다. 기존 NAC의 기본기능 외에 ZTNA에 새롭게 추가된 게이트웨이 및 에이전트 그리고 애플리케이션을 포함한 컨텍스트 기반의 접근통제를 활용하면 보다 빠르게 제로트러스트 보안 정책을 적용할 수 있습니다.

제로트러스트를 위한 7가지 원칙(NIST)	Genian ZT-NAC 대응
1. 모든 데이터 및 컴퓨팅 서비스는 리소스로 간주	1-1. 연결된 모든 객체(사용자, 단말, 트래픽, 애플리케이션 등)는 자동으로 탐지 1-2. 탐지된 모든 정보는 보안정책으로 수립되어 접근통제 등에 활용 1-3. 탐지 및 정보 수집 위한 DPI(Device Platform Intelligence) 등 요소기술 고도화
2. 모든 통신은 위치에 관계없이 보호	2-1. ZTNA Agent 와 Gateway 를 통한 양종단간 통신 암호화 지원 2-2. POP 를 통한 네트워크 트래픽 통합 및 보안기능 제공 (SASE)
3. 리소스에 대한 접근은 세션별로 부여	3-1. 네트워크 트래픽, 애플리케이션 및 동적 접근제어 지원 3-2. 최소 정보 기반 최소 접근권한 제공 (Least Privilege)
4. 리소스에 대한 접근은 다양한 상태에 따라 통제	4-1. 사용자 인증, 위치, 단말 보안 등 약 600가지 이상의 상태 조합을 통한 접근통제
5. 모든 자산에 대한 무결성 및 보안상태에 대한 측정	5-1. 연결된 모든 객체의 자동 탐지 및 탐지 후 상태정보의 실시간 감시/추적 5-2. 상태 정보 변경 시 그에 따른 다양한 제어 정책 적용 (차단, 재 인증, 교정 등)
6. 인증과 권한은 접근 이전에 동적이고 엄격하게 수행	6-1. 사용자 및 단말 인증에 따른 리소스 사용(접근) 권한 결정 6-2. 선 인증, 후 연결(SDP) 지원 및 연결 이후라도 상태 변경 시 즉시 대응
7. 가능한 많은 정보를 수집하고 보안 개선을 위해 활용	7-1. 기존 객체 탐지 외 SBOM, MUD 등 추가정보 제공 및 정책 적용 7-2. 취약점(CVE) 외 컨텍스트 기반 접근통제 구현

[제로트러스트 원칙과 Genian ZTNA 대응, 지니언스]

6. Conclusion

코로나는 IT 환경에 거대하고 빠른 변화를 가져왔습니다. 사티아 나텔라 마이크로소프트(MS) 최고 경영자는 과거 연례 개발자 컨퍼런스에서 "2년이 걸릴 디지털 트랜스포메이션(전환)이 2개월 만에 이뤄졌다" 라고 언급했습니다. 가장 대표적인 디지털 전환은 클라우드의 확대와 재택/원격의 병행을 통한 하이브리드 업무 환경의 정착입니다.

이제 정보보안 분야는 디지털 전환의 지원을 넘어 유지하기 위한 발전이 진행 중 입니다. 많은 전문가들은 현재의 디지털 전환을 가장 잘 보호/유지해 줄 수 있는 대안으로 '제로트러스트(ZT) 보안 모델'을 언급합니다. 지난 해 미국은 '사이버안보 행정명령(EO 14028)'을 통해 제로트러스트를 포함하는 사이버안보 강화 전략을 시행한 바 있습니다. 이미 제로트러스트는 가장 많은 주목을 받고 있으며 이를 지원하거나 목표로 하는 다양한 솔루션 및 서비스가 시장에 등장하고 있습니다.

누구에게나 변화는 두렵습니다. 도입과 전환에 따른 부담을 예상하기 어렵습니다. 그렇지만 변화를 멈출 수는 없습니다. 너무 늦은 변화의 수용은 오히려 더 큰 부담을 감당해야 하는 부메랑으로 우리에게 돌아올 수 있습니다. 지금은 변화를 검토해야 할 때 입니다.

지니언스(주)
14058 경기도 안양시 동안구 벌말로66 하이필드 지식산업센터 A동 12층
본 자료 및 내용문의 : mkt@genians.com
대표번호 : 031-8084-9770
기술지원 : 1600-9750
FAX : 070-4332-1683
홈페이지 : www.genians.co.kr

2005년 설립된 지니언스㈜는 국내 NAC(Network Access Control) 시장을 선도하며 글로벌 비즈니스 확장을 통해 보안 소프트웨어 전문기업으로 성장하고 있습니다. 네트워크 보안 및 단말 분석 분야 특화기술을 기반으로 내부 보안에 특화된 제품 라인업을 보유 중입니다. 네트워크에 접속하는 단말의 가시성을 확보하여 제어하는 네트워크 접근 제어 솔루션 '지니안 NAC(Genian NAC)'를 통해 국내 시장을 선도하고 있습니다. 2017년 단말 기반 지능형 위협 탐지 및 대응 솔루션 '지니안 EDR(Genian EDR)'를 출시하며 EDR(Endpoint Detection & Response) 시장에 진출했습니다. 2016년 1월 해외사업 시작과 함께 미국 보스턴에 현지법인을 설립한 바 있으며 2017년 8월 코스닥에 상장했습니다.