GENIANS WHITEPAPER

What's Best for Remote Workers: VPN? VDI?

재택근무자 보안, VPN과 VDI만으로 충분한가요?

Genians | FORTINET

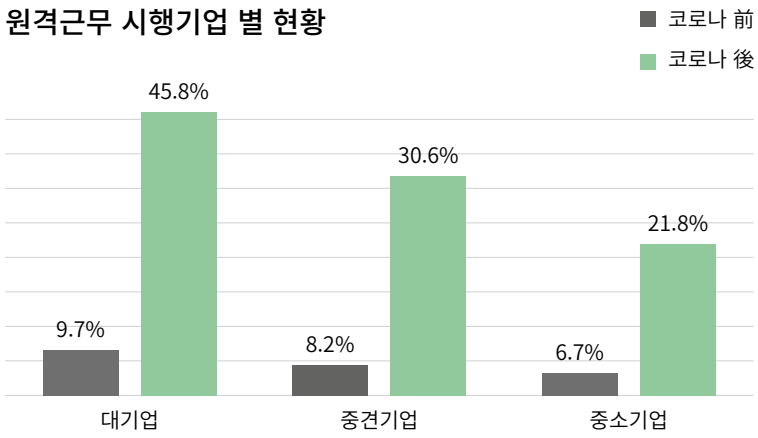
GENIANS, INC.
Next-Gen Network Access Control for the IoT era
mkt@genians.com

Introduction

뉴노멀(New Normal) - 재택근무, 새로운 업무의 표준

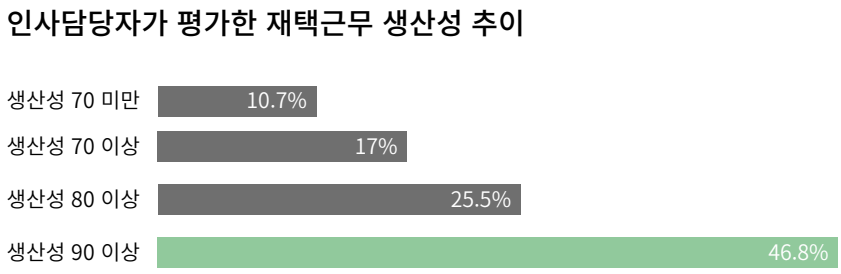
코로나(Covid-19)로 우리의 삶은 달라졌습니다. 거리 두기는 오프라인 모임 문화를 바꾸었고 모든 것이 온라인으로 바뀌었습니다. 많은 부분이 비대면(언택트)으로 바뀌면서 업무환경도 바뀌고 새로운 가치가 창출되고 있습니다. 전문가들은 코로나가 종식되더라도 완전히 이전의 상황으로 복귀하기는 어렵다고 전망하고 있습니다. 업무환경 역시 빠르게 바뀌고 있습니다. 재택 / 원격근무는 이제 새로운 표준(뉴노멀)이 되었습니다.

직원들의 안전을 이유로 재택근무를 시행하는 기업이 코로나 이전 8.3%에서 34.3%로 4배 이상 증가했습니다.제조, 유통, 통신, ICT 등 많은 분야의 기업들이 재택근무 시행에 동참하고 있습니다. 관련 기관(고용노동부 등)에서는 '재택근무 가이드라인'을 발표하는 등 변화수용에 노력하고 있습니다. 일이 있는 곳으로 이동하는 것이 아니라 내가 있는 곳으로 일이 오는 문화로 점차 바뀌어 가고 있습니다.



[코로나19 이후 업무방식 변화 실태조사, 대한상공회의소]

실제로 재택근무에 대한 평가는 나쁘지 않은 것으로 확인되고 조사에 따르면 업무 효율성에서 비슷하거나 좋다는 의견이 84%, 직원 만족도 역시 83%로 높게 나타났습니다. 재택근무로 인한 업무 효율성 저하 문제는 걱정한 것보다 매우 긍정적으로 평가되었습니다. 한국경영자총협회의의 조사에 따르면 정상 출근시 생산성을 100%으로 봤을 때, 응답자 절반 이상이 80% 이상의 업무 생산성을 나타낸다고 답했습니다.



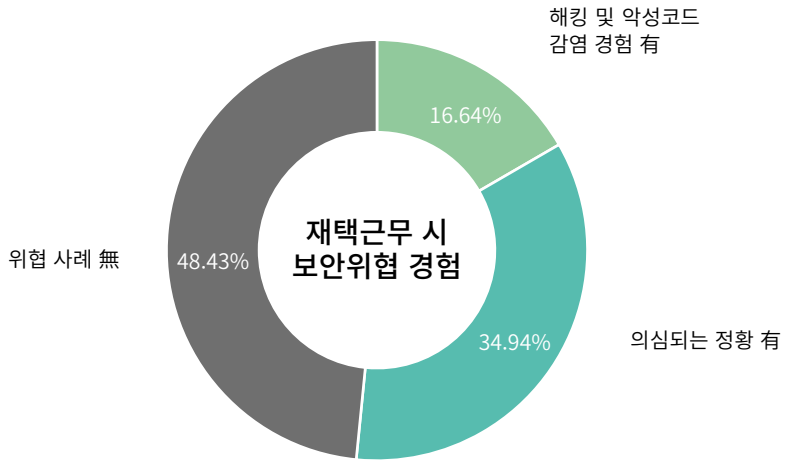
[사회적 거리 두기에 따른 매출 100대 기업 재택근무 현황조사, 한국경영자총협회]

기업들도 재택근무에 대한 긍정적인 인식을 갖고 있으며, 변화의 가운데서 좀 더 효율적이고 생산성을 높일 수 있는 방법들을 고민하고 있습니다. 협업 툴, 업무 메신저, 화상회의 시스템 등 비대면 업무를 위한 인프라의 도입이 빠르게 증가하고 있으며 원격 접근, 노트북 반출 / 입 등 기존 업무와의 연속성을 위한 프로세스 개선 등도 확대되고 있습니다.

원격 및 재택근무 보안위협

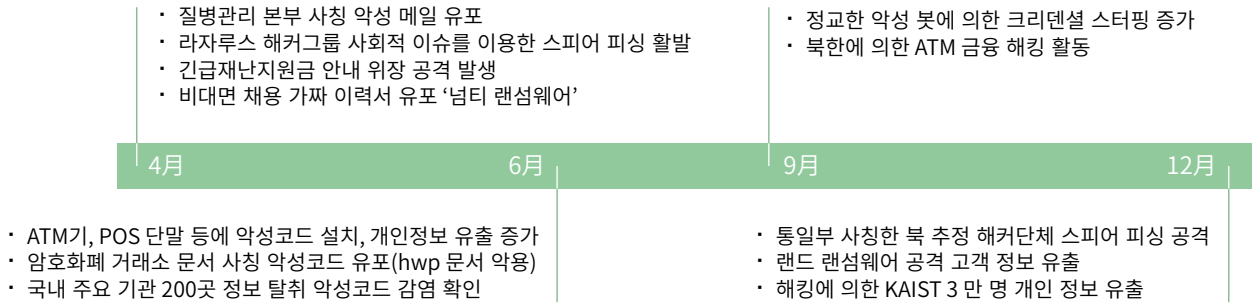
원격 및 재택근무에 따른 위협의 증가

변화된 업무환경을 위하여 기업들은 새로운 보안정책(Security Policy)을 수립하고 있습니다. 이전에는 많은 신경을 쓰지 않았던 부분들이었고, 특정 부분들에 고려되었습니다. 기존에 설계된 다수의 보안정책은 물리적인 내/외부의 구분 및 신뢰(Trust)/비신뢰(Untrust)의 명확한 기준을 통해 수립되었습니다. 그러나 이러한 보안 정책은 더 이상 효과적이지 않습니다. 클라우드와 재택근무로 물리적인 내/외부의 구분이 불가능 해졌으며 신뢰와 비신뢰의 판단은 수시로 바뀌고 있습니다.



[사이버 위협 동향 보고서, KISA(한국인터넷진흥원)]

여전히 기업 외부에는 악의적인 해커 또는 악성코드 등의 많은 위협들이 도사리고 있습니다. KISA(한국인터넷진흥원)의 조사 결과에 따르면 재택근무자 중 50% 이상이 위협이나 의심의 행동을 경험했다고 합니다. 이러한 현상은 전 세계적으로 유사하게 발생하고 있습니다. 사회적 이슈 및 금전 취득 등을 목적으로 하는 전통적인 공격뿐만 아니라 코로나 이슈를 이용한 새로운 공격들 역시 크게 증가하고 있습니다.



[2020년 사이버 공격 및 코로나 관련 해킹 사례, 자체조사]

이제 공격자들은 공격의 대상을 기업에서 집(재택근무자)으로 이동하고 있으며 이를 이용하여 중요 데이터를 탈취하거나 기업 내부로 접근하기 위한 창구로 이용하려는(island hoping) 공격이 증가하고 있습니다. [1]이러한 변화 속에서 보안 관리자는 어느 부분에 집중해야 할까요? 무엇을 기준으로 보안정책을 수립하고 관련 솔루션을 도입하는 것이 효과적일까요? 지니언스는 '공격 지점의 축소' 와 '가시성의 확대'의 두 기준이 가장 중요하다고 생각합니다.

공격 지점(Attack Surface)의 축소 필요

기업은 변화된 업무 형태를 수용하면서 새로운 보안 위협으로부터 보호받아야 합니다.
그러나 현재의 재택근무 환경은 아래와 같은 잠재적인 위협을 포함하고 있습니다.

첫째, 새로운 네트워크에 의한 위협입니다.
재택/원격 근무 시 커피숍이나, 보안이 적용되지 않은 공용 또는 개방된 Wi-Fi를 사용하는 경우가 있습니다. 상대적으로 관리가 허술한 네트워크는 보안에 취약할 수밖에 없습니다. 이렇게 보안이 적용되지 않은, 또는 공용 패스워드의 사용은 불특정 다수와 네트워크를 공유하게 되며 암호화되지 않은 통신은 중요정보의 유출 등으로 이어질 수 있습니다.

둘째, 새로운 단말에 의한 위협입니다.
재택근무자 다수는 본인이 희망하는 기기로 업무를 수행합니다. 여기에는 게임용PC, 스마트패드, 구형 노트북 등 다양한 기기가 포함될 수 있습니다. 이러한 다양성은 기업의 보안정책을 우회할 수 있는 통로로 사용될 수 있습니다.

마지막으로 사용자에 의한 위험입니다.
많은 기업이 원격 업무를 위하여 VPN(가상사설망)서비스를 제공하고 있습니다. ID/PW로 인증이 완료되면 제한 없이 내부에 바로 연결됩니다. 누군가가 습득한 ID/PW로 연결을 시도하는 경우라면 어떨까요? 실제로 최근 [2]다크웹(DarkWeb)을 통해 대기업 VPN 접속 계정이 거래되는 등 주의가 필요 합니다.

가시성(Visibility)의 확대 필요

클라우드 사용 확대와 재택근무로 보안의 경계가 점점 희미해지고 있습니다. 내부(Trust) / 외부(Untrusted)의 명확한 구분은 어려워지고 IP 기반의 보안정책 등은 더 이상 효과적이지 않습니다. 새로운 환경에서는 보다 높은 가시성이 요구됩니다. '누가(Who) / 무엇(What)' 이 네트워크에 존재하고 접속을 시도하는지를 알 수 있어야 합니다. 접속 이후에도 '어떠한(How)' 업무 및 행위를 수행하는지를 지속적으로 관찰해야 합니다.

기타 다른 문제점

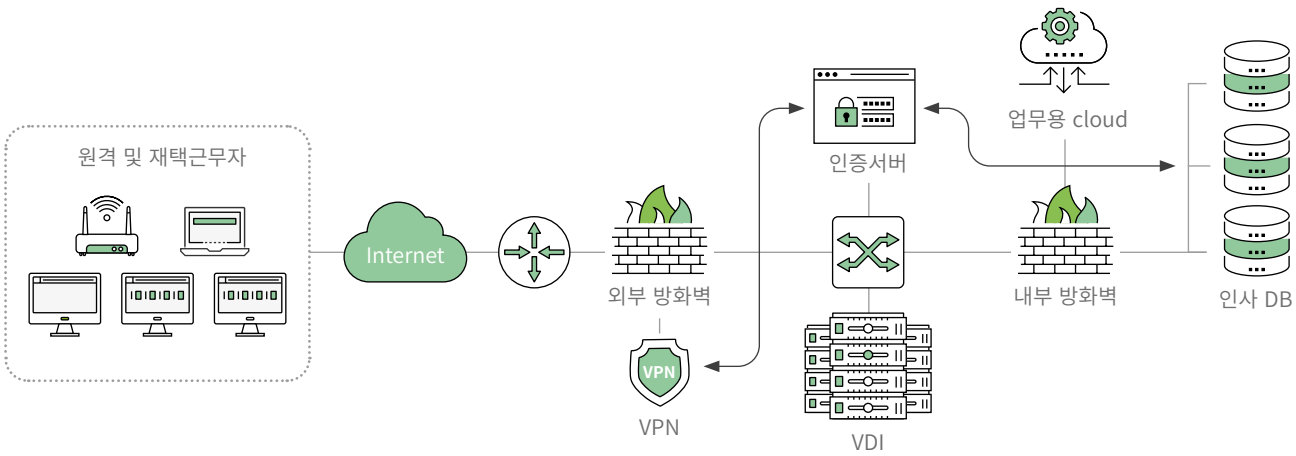
재택근무로 인해 업무용 중요데이터의 사용범위가 확대되고 있으며 이로 인한 정보유출 역시 증가할 것으로 전망하고 있습니다. 공격자는 취약점을 이용하여 악성코드를 설치하거나 사회공학적 방법으로 데이터 유출을 시도할 수 있습니다. 또한 개인 계정관리에도 철저한 주의가 필요합니다. 유출된 계정 정보를 업무시스템에 활용하는 크리덴셜스터핑(Credential Stuffing) 공격이 빠르게 증가하고 있습니다.

이러한 위협에 대응하기 위하여 기업과 보안관리자는 많은 준비를 하고 있습니다. 그에 못지않게 재택근무자의 노력도 중요합니다. 재택근무자는 항상 최신의 업데이트 상태를 유지해야 하며 DLP, 백신 등 권고하는 보안 소프트웨어를 반드시 설치 / 사용해야 합니다. 가능하다면 별도의 업무용 PC를 마련하시는 것이 좋습니다. 만약 이것이 어렵다면 계정 정보라도 분리해서 사용하십시오. 슈팅게임과 VPN 접속에 같은 계정을 사용한다면 우리 조직의 보안은 내PC에서부터 무너져 내릴지도 모릅니다.

고객의 현황과 요구사항

재택근무를 위한 표준 네트워크

현재 가장 일반적인 형태의 재택근무 환경은 VPN(Virtual Private Network)과 VDI(Virtual Desktop Infrastructure)의 도입 및 운용이라고 할 수 있습니다. VPN을 통하여 재택근무자와 회사내부를 연결하는 가상의 네트워크를 만들 수 있습니다. VDI는 VPN 연결 후 재택근무자에게 적합한 업무 환경을 제공하거나 중요 데이터 또는 시스템에 접속하기 위한 경로를 제공해 줍니다. 이러한 구성에서 VDI는 VPN의 한계를 보완해 주는 역할을 할 수 있습니다. VDI를 이용하면 사내 환경을 크게 변경하지 않고도 IP 기반의 접근통제 등 기존 보안 정책을 재사용 할 수 있으며 중요 시스템에 접근하는 단말에 요구되는 보안수준을 강제화 하고 데이터 유출을 방지하는 등의 부가적인 효과를 기대할 수 있습니다.



[재택근무 환경을 위한 표준 네트워크, 지니언스]

결과적으로 위와 같은 구성은 재택근무 환경을 지원하고 내부의 자산을 보호하기 위한 효과적인 방법임에는 분명합니다. 그러나 우리는 다수의 고객으로부터 VPN 과 VDI 환경에서도 추가적인 보안조치가 필요하다는 것을 확인할 수 있었습니다. 대표적인 사항은 아래와 같습니다.

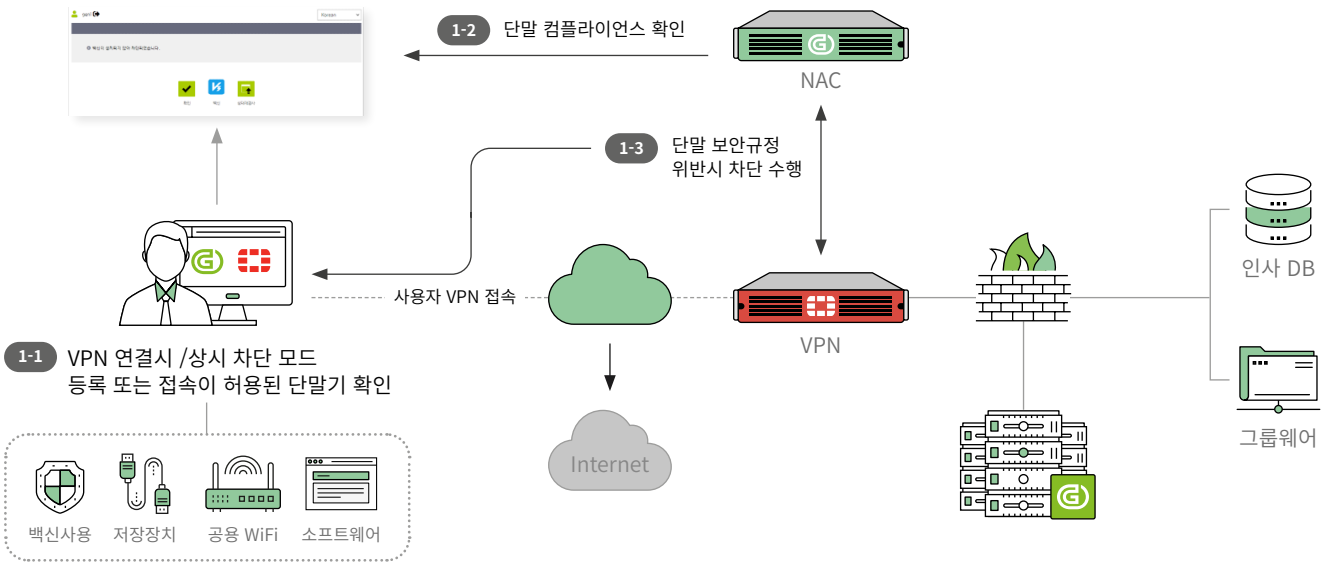
- 단말의 보안 상태를 점검하고 VPN 연결을 할 수는 없을까?
- 등록 또는 접속이 허용된 단말기만 VPN접속을 하게 할 수 없을까?
- VPN 연결 시 일반 인터넷을 차단할 수는 없을까?
- VPN 이 제공하는 인증 이외에 더 강력하고 편리한 인증 방법은 없을까?
- VPN 연결 후 VDI(Virtual Desktop Infra) 사용현황을 모니터링 할 수는 없을까?
- VPN 연결 후 보안정책을 위반하면 VPN 연결을 강제로 종료시킬 수는 없을까?

이러한 고객의 요구사항을 해결할 수 있는 방법은 없을까요? 이것이 NAC 와 VPN 의 긴밀한 협업이 필요한 이유 입니다.

재택근무 Our Approach

NAC를 이용하면 앞에서 언급한 추가적인 보안조치가 가능하므로 보다 안전한 VPN 및 VDI 환경을 운영할 수 있습니다. 대표적인 요구사항에 대하여 어떻게 대응이 가능한지 확인해 보겠습니다.

단말의 보안 상태를 점검 후 VPN 연결을 할 수는 없을까?
등록 또는 접속이 허용된 단말기만 VPN접속을 하게 할 수 없을까?
그리고 VPN 연결 후 보안정책을 위반하면 VPN 연결을 강제로 종료시킬 수는 없을까?



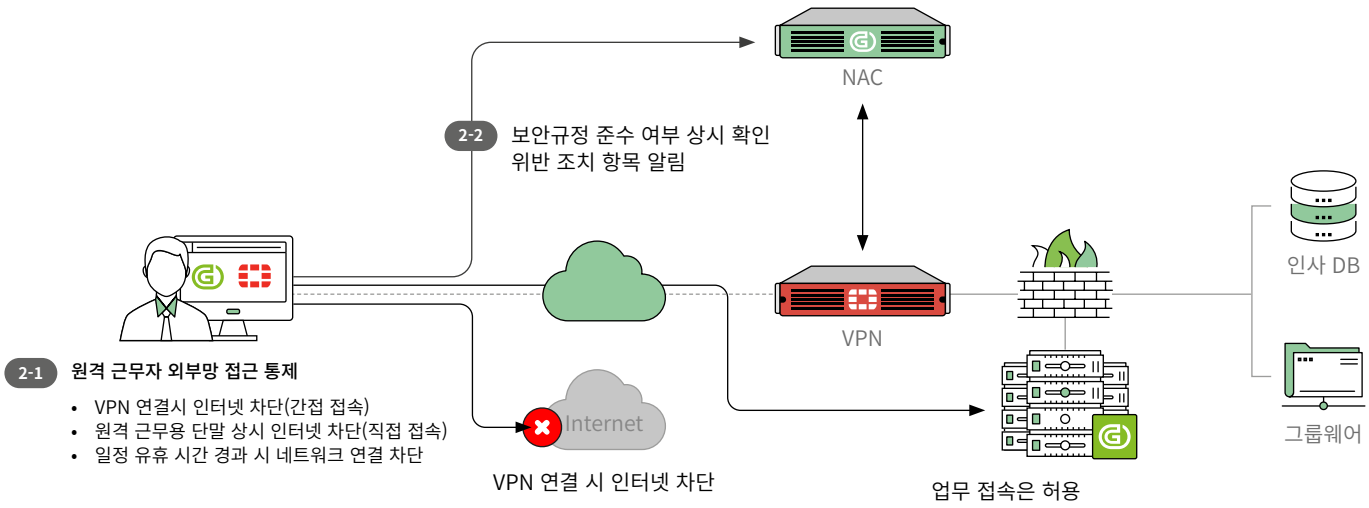
[내부 접속 전 단말의 보안상태 점검]

보안 관리자들은 재택근무자가 안전한 PC를 업무에 사용하기를 희망합니다. 그러나 원격지의 안전을 확인하고 강제화하는 것은 매우 어렵습니다. VPN 특성상 인증 이후에는 모든 접속이 허용되며 전송 구간에서 위협을 탐지하는 것도 거의 불가능합니다. 따라서 접속 전에 PC의 보안상태를 확인하여 안전이 확인된 경우에만 접속을 허용하거나 VPN 접속이 허용된 등록된 단말기를 사용하거나 VPN 종단 지점에서 단말의 상태를 즉시 확인, 조치할 수 있는 방법이 필요합니다. 또한 VPN 연결 후 PC의 보안상태가 변경된다면 그에 따른 적절한 조치가 필요합니다.

NAC는 VPN 솔루션과의 연동을 통해 VPN 연결 전 단말의 상태를 점검하고 그 결과에 따라서 VPN 연결을 제어할 수 있습니다. 또는 우선 VPN 연결 후 CWP(Captive Web Portal)을 통하여 단말의 상태를 검사하거나 패치 업데이트 및 필수 소프트웨어(AV 등)를 설치하는 것도 가능합니다. 작업 중 PC가 악성코드에 감염되는 등 보안상태가 변경되는 경우 즉시 VPN으로 위반 단말에 대한 차단 명령을 전송합니다. 이러한 일련의 행위들은 NAC의 정책 서버와 VPN 게이트웨이가 서로 연동하여 구현되는 방식입니다.

VPN 연결 시 일반 인터넷을 차단할 수는 없을까?

우선, 이 부분에서는 원격근무자의 PC가 사내에서 지급된 경우, 사내 접속을 제외한 어떠한 통신이라도 차단되어야 합니다. 즉 업무 용도로만 사용되어지도록 해야 합니다. 하지만, 만약 사내 지급이 아닌 원격근무자의 개인 PC일 경우, 원격근무자의 PC에서 'DB 마이그레이션'과 '슈팅게임' 이 동시에 수행되기를 바라는 보안관리자는 없을 것입니다. VPN 연결은 업무 수행을 의미하며 이 때 VPN을 제외한 인터넷 연결은 통제되어야 합니다. 이러한 조치는 악성코드의 사내 확산을 방지하고 VPN을 이용하여 사내로 접근하려는 시도 등을 차단할 수 있는 효과적인 방법입니다.

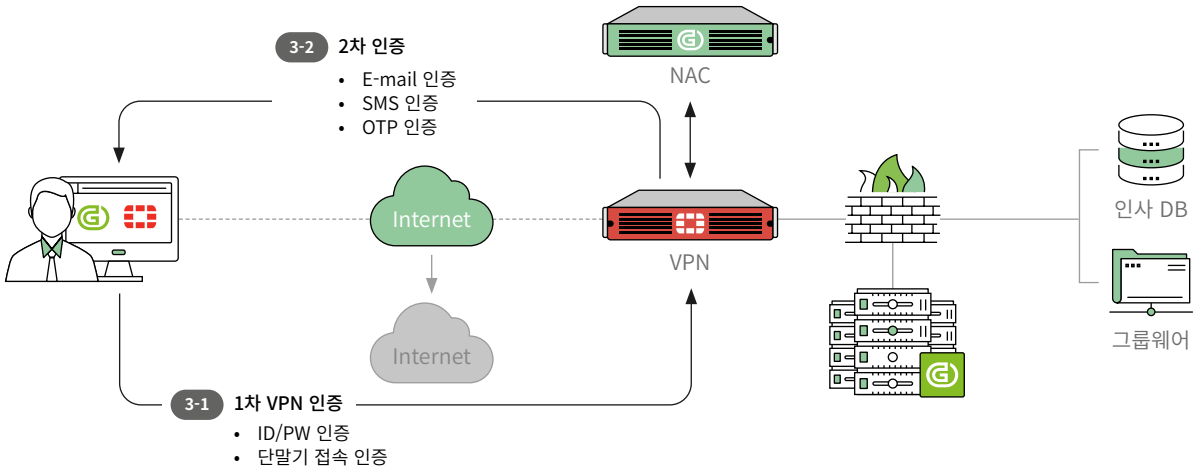


[차단 정책을 이용한 VPN 연결 시 단말 인터넷 차단]

먼저 VPN 게이트웨이를 통해 외부 네트워크 접근 제어를 할 수 있습니다. 원격 근무자가 내부망으로 직접 접속하는 경우 상시 인터넷을 차단하고, VDI와 같은 간접 접속을 하는 사용자는 VPN 연결 시에 인터넷을 제어할 수 있습니다. 또한 NAC의 에이전트(Agent) 정책을 이용하거나 'VPN Kill Switch' 기능을 이용하여 재택근무자의 VPN 연결이 완료되는 경우 VPN을 제외한 인터넷 통신을 자체적으로 차단할 수 있습니다. 이후 사용자의 VPN 연결이 해제되면 이전 상태로 복구됩니다.

VPN이 제공하는 인증 이외에 더 강력하고 편리한 인증 방법은 없을까?

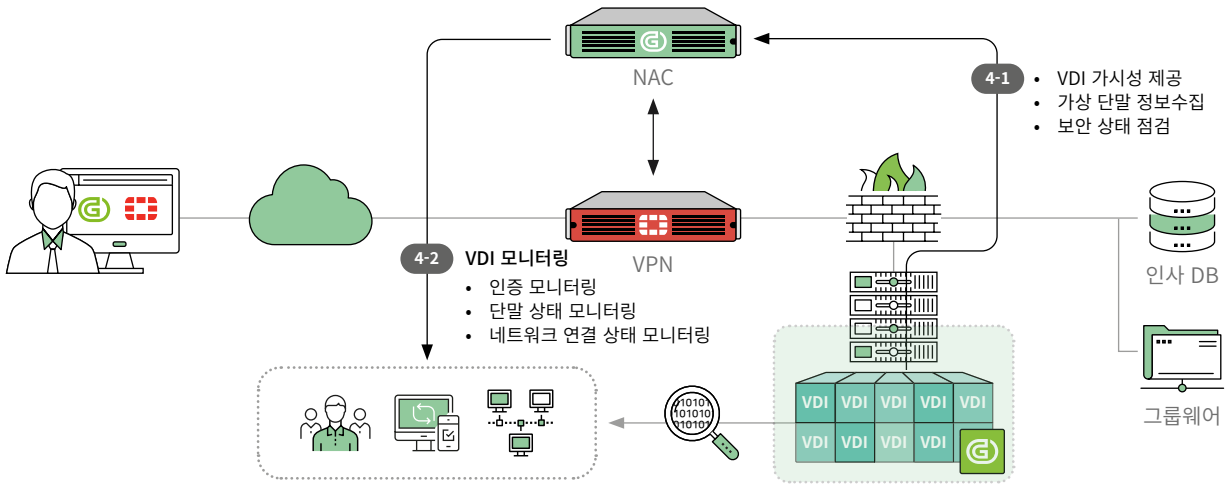
VPN 솔루션은 다양한 인증 기능을 지원합니다. ID / PW 는 기본이고 단말의 MAC, 인증서뿐 아니라 앱(App), OTP 등을 통한 다중인증(MFA: Multi Factor Authentication) 기능도 제공합니다. 그러나 다양한 인증방법의 제공보다 더 중요한 것은 계정의 통합관리와 사용자의 편의성입니다. 솔루션 별로 서로 다른 계정을 사용하는 것이 원칙이나 동일한 패스워드를 사용하는 등 허술한 관리는 계정유출과 불법접근 등의 사고로 이어질 수 있습니다. 강력한 인증기능의 제공과 더불어 SSO(Single Signe On) 등의 편의성 지원이 필수적입니다.



[Genian NAC를 이용한 다중인증]

NAC 역시 자체적인 인증기능을 제공하며 생체인증을 포함한 다양한 다중인증(MFA)을 제공합니다. 또한 [3]RADIUS를 내장하고 있어 NAC를 유 / 무선 통합 인증서버로 사용할 수 있습니다. 그 어떤 솔루션보다 다양한 인사DB와 연동이 가능하며 향상된 SSO 지원을 위한 SAML(Security Assertion Markup Language) 표준을 통해 IDaaS 등의 서비스를 이용하는 것도 가능합니다. 보안관리자는 NAC를 활용하여 사용자와 단말에 대한 관리 및 계정관리 업무까지도 통합관리 할 수 있습니다.

VPN 연결 후 VDI(Virtual Desktop Infra) 사용 현황을 모니터링할 수는 없을까?



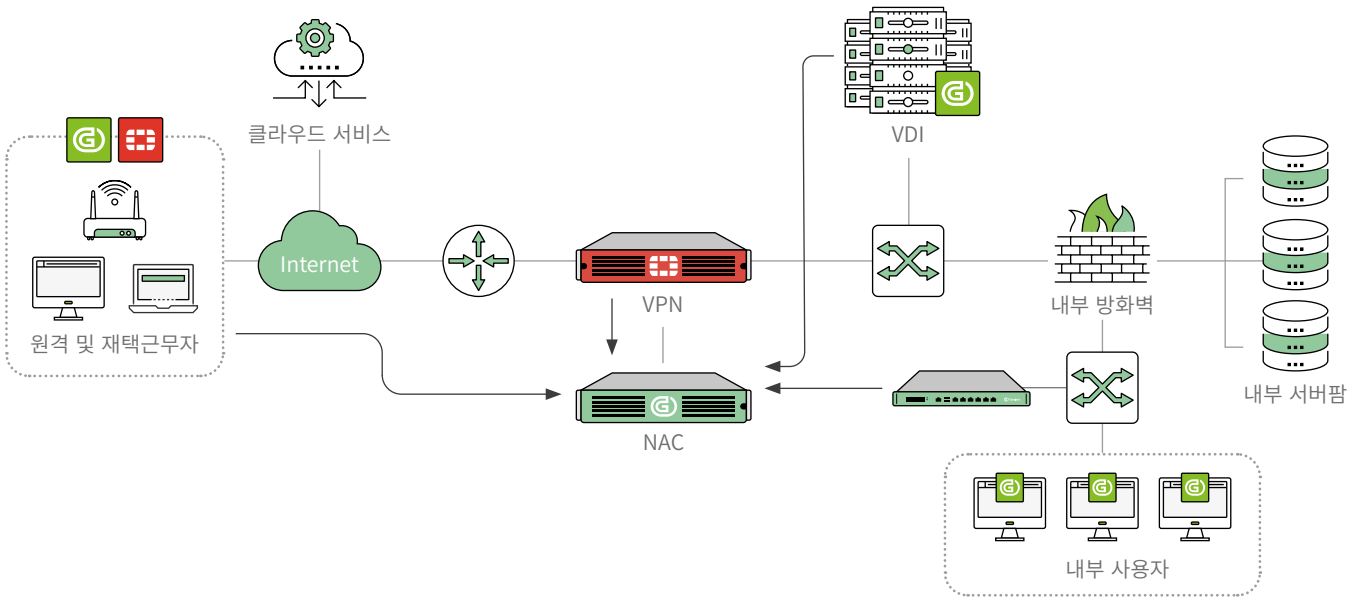
[Genian NAC를 이용한 VDI 가시성 확보]

VDI는 가상의 업무환경을 제공하지만 운영체제와 어플리케이션이 동작한다는 관점에서는 내부 업무용 단말과 동일한 보안수준을 유지 / 강제화 할 필요가 있습니다. 불법 소프트웨어 설치, 네트워크 접속, 백신(AV) 설치 여부 등 내부 단말과 같은 보안수준을 유지하는 것이 안전 합니다.

NAC는 다양한 VDI 환경을 지원합니다. 에이전트를 VDI에 설치하는 경우 가상데스크톱 역시 기타의 단말(노드)과 동일하게 관리할 수 있습니다. 단말의 상세한 정보를 확인할 수 있으며 보안정책을 적용하고 통제할 수 있습니다. 네트워크 수준의 통제를 위하여 VDI 환경에 NAC 차단 센서를 설치하여 운영하는 것도 가능 합니다. 이 경우 VDI 간의 통신(East – West) 뿐 아니라 VDI 와 다른 네트워크와의 통신(North – South) 까지도 모니터링하고 제어할 수 있게 됩니다.

Genian NAC를 이용한 개선된 재택근무 네트워크 제안

NAC를 이용하면 VPN과 VDI환경을 보완하여 보다 안전한 재택근무 환경을 완성할 수 있습니다. NAC는 Windows, Mac, Linux 등 다양한 운영체제를 지원하며, 통합된 유 / 무선 인증서버의 기능을 제공합니다. VPN과 연계를 통해 외부로부터 접속하는 사용자를 식별 / 인증하고 단말의 보안 수준을 강제화 할 수 있습니다. 사내에 연결된 이후에도 가상의 VDI 환경에서 실제 단말과 동일한 단말의 가시성을 확보할 수 있습니다. 만약 사용자와 단말이 보안정책을 위반하는 경우 그 내용은 탐지되고 단말과 네트워크 그리고 경계선에서 즉시 통제될 수 있습니다. 이 모든 내용은 실시간으로 동작하며 정책에 따라서 자동으로 이루어 집니다.

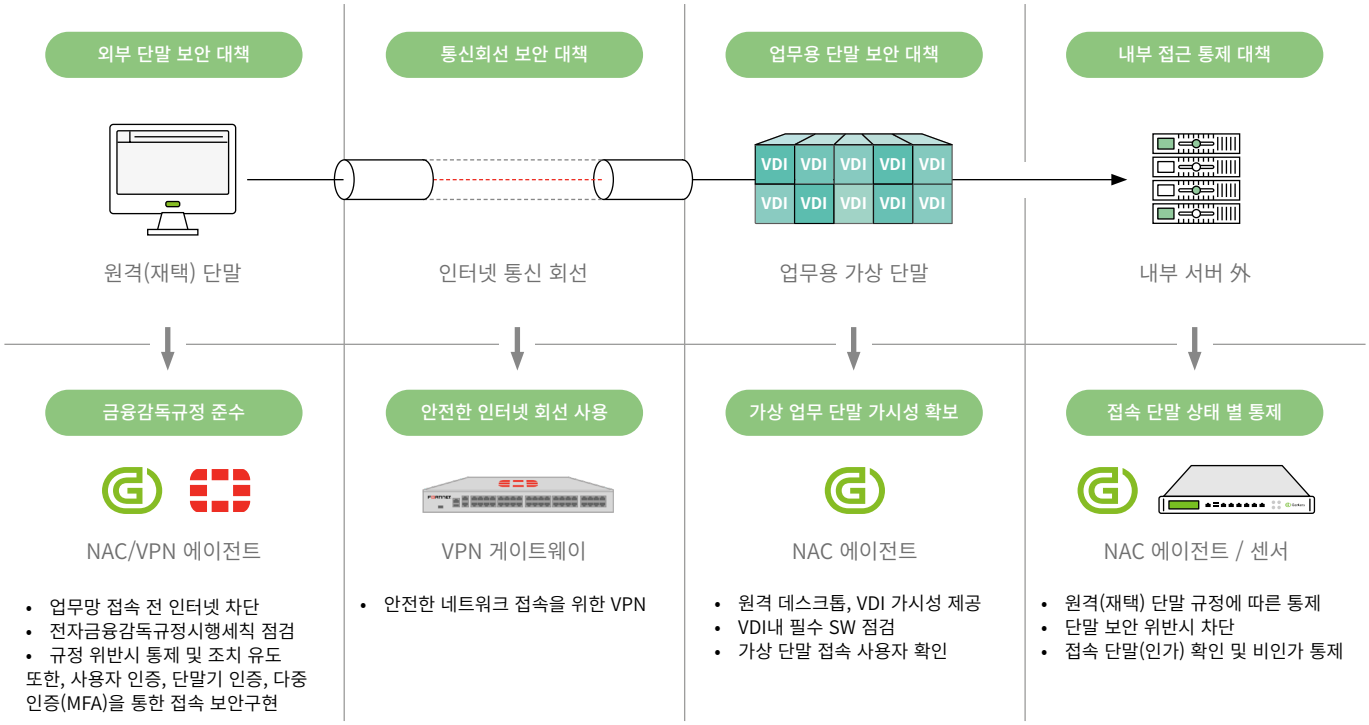


[재택근무 환경을 위한 개선된 네트워크 제안, 지니언스]

Genian NAC와 Forti-VPN의 협업으로 만드는 안전한 재택 근무

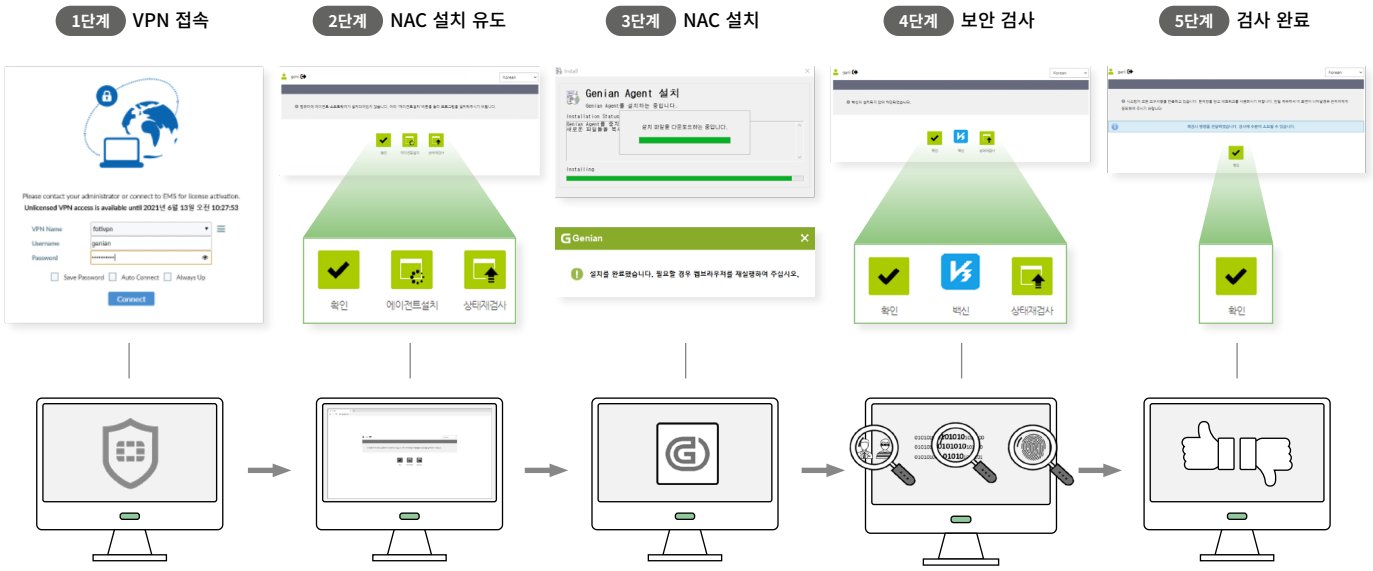
지금까지 보다 안전한 재택근무 환경을 위한 몇 가지 시나리오를 살펴보았습니다. 그러나 이것은 단순한 시나리오에 그치는 것은 아닙니다. 이를 실현해 시나리오를 가능케 하는 다양한 방법이 있으며 대표적인 사례가 NAC 와 VPN의 연동입니다. 그러나 긴밀한 연동은 쉽게 이루어 지지 않습니다. 설계부터 타 보안 솔루션과의 연동을 고려한 다양한 인터페이스가 필요합니다. 대표적으로 RESTful API(Application Programming Interface), Syslog, Webhook, SNMP 등의 방법이 사용될 수 있습니다. 이러한 방법을 통해 보다 많은 보안 솔루션과의 연동이 가능하며 보안 시너지를 높일 수 있습니다. NAC의 경우 이미 방화벽, VPN 등의 레거시 솔루션은 물론 EDR, SOAR, IDaaS(ID as a Service) 등 다양한 솔루션과의 연동을 통해 보안 시너지를 창출하고 있습니다. 이것이 이번에 Genian NAC 와 Forti-VPN 이 긴밀한 연동을 추진하게 된 배경 입니다.

양사의 제품은 이미 해당 영역을 대표하는 솔루션으로 자리매김 하였으며 다양한 사업적 경험과 글로벌 표준을 포함하는 연동을 위한 다양한 방법을 제공하고 있습니다. 양사 제품의 연동을 통해 창출되는 보안 시너지 효과는 앞에서 언급한 시나리오를 현실화 하는데 부족함이 없다고 생각합니다. 이제 우리는 보다 안전한 재택근무 환경을 구축 및 운영할 수 있게 되었습니다.



[NAC와 VPN 연동을 통한 안전한 재택근무 제공]

뿐만 아니라 이러한 연동의 결과로 다양한 규제에 대비하는 것이 가능합니다. 공공기관 및 금융기관 등 에서는 안전한 재택근무 환경의 구축 및 운영을 위한 다양한 가이드라인을 제공하고 있습니다. 가이드라인은 단말보안 점검, 안전한 연결, 사용자 및 단말의 인증 등 중요한 사항에 대한 점검 및 조치에 관한 내용을 포함하고 있습니다. NAC 와 VPN 의 대표기능을 활용하여 이러한 내용을 사전에 점검하는 것은 물론 조치까지도 자동으로 수행할 수 있어 누수 없는 보안 관리가 가능합니다.



[NAC-VPN 연동을 통한 단말 검사 및 조치 자동화]

Conclusion

코로나-19 팬데믹(Pandemic)으로 우리의 업무환경은 크게 바뀌었고 변화는 지금도 계속되고 있습니다. 기업은 격리와 재택의 제한된 상황에서도 업무 생산성을 유지하기 위하여 시스템을 새로 구축하거나 기존 보안정책을 완전히 새롭게 설계하는 등 그들 만의 방식으로 생존을 유지하기 위해 힘쓰고 있습니다. 그러나 많은 전문가 들은 코로나가 종식된다 하여도 새로운 업무 방식이 완전히 예전으로 돌아가지는 않을 것이라 전망하고 있습니다. 페이스북 최고경영자는 “향후 10년에 걸쳐 재택근무를 중심으로 회사의 운영 방식을 영구적으로 조정하겠다”는 공약을 내세웠으며 캐나다 소재 전자상거래 업체인 소피파이(Shopify) CEO 역시 “사무실 중심의 시대는 끝났다며, 2021년까지 사무실을 폐쇄하기로 결정했습니다.” 라고 발표하는 등 기업들 역시 변화를 적극적으로 수용하고 있습니다.

변화의 가운데에 디지털 전환(DX)이 있습니다. 더 많은 업무가 IT에 의존하고 있으며 이러한 현상은 가속화될 것입니다. 미처 대비하지 못한 변화는 틈새를 만들고 틈새는 위협으로 이어질 수 있습니다. 누군가는 이러한 틈새에 집중합니다. 그리고 틈새를 새로운 기회로 만들고자 노력할 것입니다. 지금 기업은 변화에 대처하면서 틈새 역시 메워야 하는 긴박한 상황이 이어지고 있습니다.

언젠가 코로나는 종식되겠지만 재택근무는 종식이라는 의미가 없습니다. 언제 다시 새로운 바이러스가 우리의 생활을 멈추게 할지 모릅니다. 재택근무는 새로운 근무 형태로 자리잡아가고 있습니다. 변화를 거부할 수 없다면 안전하게 수용할 수 있는 방법에 대한 고민과 노력이 무엇보다 필요한 때입니다.

참조 URL

[1]50% of cyber-attacks now use island hopping
https://ims.geninetworks.com/jira/browse/AP-5163

[2]다크웹에 VPN 계정 정보 수천 건 유출……한국 기업도 포함
http://www.inews24.com/view/1288495

[3]Genian NAC RADIUS 소개
https://genians.co.kr/genians-nac/wah_radiun/
https://docs.genians.com/release/ko/authentication/enabling-authentication/8021x.html

CONTACT US
본 자료 및 내용문의 : mkt@genians.com

Genians

Next-Gen Network Access Control for the IoT era

2005년 설립된 지니언스㈜는 국내 NAC(Network Access Control) 시장을 선도하며 글로벌 비즈니스 확장을 통해 보안 소프트웨어 전문 기업으로 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 인사이츠 E (Genian Insights E)'를 출시하며 EDR (Endpoint Detection & Response) 시장에 진출했습니다. 2016년 1월 해외사업 시작과 함께 미국 보스턴에 현지법인을 설립한 바 있으며 2017년 8월 코스닥에 상장했습니다.

Doc. v 1.0-KO