

요약 보고서: 보안 모바일 액세스가 전략적 비즈니스 요건인 이유

모바일 액세스는 혼란스럽고 역동적인 환경에서 생산성을 유지할 수 있도록 해줍니다.

개요

전 세계적으로 모바일 근무의 중요성이 대두되고 비중이 증가하고 있습니다. 민첩성, 지속성, 생산성과 관련한 이점으로 보안 모바일 액세스는 오늘날의 비즈니스에서 전략적 필수 사항이 되고 있습니다. 그러나 이러한 모바일 근무를 효과적으로 지원하기 위해 IT 팀은 여러 난제와 싸우고 있습니다. 엔드포인트 수의 큰 증가, 보다 교묘해진 위협, 내부 리소스 액세스와 SaaS 리소스 액세스의 필요성, 예산 내 운영 요건 등이 그러한 난제의 예라 할 수 있습니다.

서론

매일 일어나는 뉴스로 역동적 기술 솔루션이 필요한 어려운 상황이 야기되고 있습니다. 공중보건 비상사태, 지진, 쓰나미, 허리케인, 눈보라 등의 자연재해, 정치적 위기는 중요 직원이 출장을 가거나 물리적 장소에 있는 리소스를 접근하는 일을 막을 수 있습니다. 수익의 연속성을 보장하기 위해 기업들은 언제 어디서나 업무를 수행할 수 있는 민첩성을 지니고 있어야 합니다.

또한 많은 기업들이 직원들의 생산성 증가와 직원 유지를 원하면서도 물리적 사무실 유지에 따른 운영 비용 부담은 줄이고 언제 어디서나 직원들이 일할 수 있도록 환경을 조성하기를 원합니다.

80개 국가의 여러 산업 분야에서 15,000명의 전문가들이 참여한 글로벌 [2019 IWG](#) 설문조사에 따르면:

- 85%가 증대된 유연성으로 생산성이 확대되었다고 하였습니다.
- 65%가 유연 근무제가 자본 지출과 운영 지출을 줄이고 위험요소를 줄이는 데 도움이 되었다고 하였습니다.
- 75%가 유연 근무제가 표준 방식이라고 생각하였습니다.
- 전 세계 62% 기업들이 현재 유연 근무제 정책을 가지고 있습니다.
- 전 세계 직원들의 절반 이상이 주 중 2.5일을 넘게 원격으로 근무를 하고 있습니다.

- 80% 이상의 직원들이 비유연근무 직장 대신 유연근무 직장을 선택할 것이라고 하였습니다.
- 미국 경제 단독으로만 유연근무를 통해 4.5조 달러의 상승 효과를 내는 것으로 보았습니다.

결과적으로 기업들은 전통적인 네트워크 경계 밖에서 회사의 지금 기기와 개인 기기 모두를 통해 모바일로 리소스를 이용하는 경우가 증가하였습니다.

효과적인 사이버 보안은 안전한 모바일 액세스가 수반되어야 합니다

오늘날 언제 어디서나 모바일 액세스를 자유롭게 제공하는 환경에서는 잠재적으로 보안이 되지 않는 수많은 모바일 사용자 장치들을 통해 여러 보안 취약점을 노출시킬 수 있습니다.

사용자의 부주의와 위험스런 온라인 행태로 인해 각 모바일 기기의 보안을 단순히 직원 개인에게만 맡길 수는 없게 되었습니다.

더욱이, 위협 유형들은 다양해지고 심화되고 있으며 더욱 교묘해지고 있습니다. 표적화된 랜섬웨어, 완전히 새로운 형태의 위협, 메모리 기반 맬웨어, 사이드 채널 공격, 암호화된 위협 등이 그러한 예입니다.

궁극적으로, 모바일 네트워크의 보안은 유선 네트워크의 보안과 같은 수준으로 유지되어야 합니다. 이렇게 하려면 사내에 있거나 클라우드에 있는 기업 리소스와 연결을 시도하는 모든 모바일 장치를 신뢰할 수 없다는 가정에서 출발해야 합니다. 보안 모바일 액세스에서 시간과 장소에 구애받지 않는 액세스를 가능하게 하려면 신뢰성에 의구심을 갖는 접근 방식이 핵심 요소입니다.

IT 팀은 또한 한정된 예산과 숙련된 직원을 운용하면서도 이러한 모바일 엔드포인트로부터의 액세스를 안전하게 관리해야 합니다. 이것은 구축의 간소화, 가용성 확보 및 지원을 통해 총 소유 비용을 절감시켜야 함을 의미합니다. 사이버 보안을 효율적이게 하려면 모바일 환경에서 일하는

직원들에게 민첩하고 사용이 쉬우며 비용 효율적이고 확장 가능한 방식으로 주요 비즈니스 리소스에 대한 액세스를 안전하고 쉽게 연중 내내 그리고 하루 24시간 가능하게 해야 합니다.

결론

사업 지속성 보장이든 직원 유지와 생산성 보장을 위해서든 보안 모바일 액세스는 전략적 비즈니스 요건이 되었습니다. SonicWall Secure Mobile Access(SMA) 솔루션을 통해 고도로 분산된 기업 전반에서 언제 어디서나 액세스가 가능해집니다. 이러한 솔루션으로 고객의 사업체는 향후의 불확실성을 극복하고 현재의 운영을 유지할 수 있는 기민성을 가질 수 있습니다.

자세한 사항을 www.sonicwall.com/products/remote-access 에서 확인해 주십시오.

© 2020 SonicWall Inc. 모든 권한 보유.

SonicWall은 미국 및/또는 기타 국가에서 SonicWall Inc. 및/또는 그 계열사의 상표 또는 등록상표입니다. 그 밖의 모든 상표와 등록상표는 각 소유권자의 재산입니다.

본 문서의 정보는 SonicWall Inc. 및/또는 그 계열사의 제품과 관련된 정보입니다. 본 문서에 의해서 또는 SonicWall 제품 판매와 연계하여 금반언의 원칙 또는 기타의 방법으로 명시적으로든 암묵적으로든 일체의 지적재산권에 대해 어떠한 라이선스도 부여되지 않습니다. 본 제품의 라이선스 계약에 명시된 바와 같이 계약 조건에 명시된 바를 제외하고, SONICWALL 및/또는 그 계열사는 상품성, 특정 목적에 대한 적합성 또는 비침해에 대한 암묵적 보증(이에만 국한되지 않음)

등을 포함하여 제품과 관련된 명시적, 암묵적 또는 법적 보증을 부인합니다. SONICWALL 및/또는 그 계열사는 어떤 경우에도 본 문서의 이용 또는 이용하지 못함으로 인해 생겨나는 직접적, 간접적, 결과적, 징벌적, 특별 손해 또는 부수적 손해(이익 손실, 사업 중단 또는 정보 손실로 인한 피해를 포함하되 이에만 국한되지 않음)에 대해, 비록 그 피해의 가능성을 숙지하고 있었다 하더라도 법적 책임을 지지 않습니다. SonicWall 및/또는 그 계열사는 본 문서의 내용에 대해 정확성이나 완전성에 관하여 어떤 진술이나 보증도 하지 않으며, 통지 없이 언제든지 명세서와 제품 설명을 변경할 권리가 있습니다. SonicWall 및/또는 그 계열사는 본 문서에 포함된 정보를 업데이트함을 약속하지 않습니다.

SonicWall 소개

SonicWall은 전 세계 중소기업, 대기업, 정부 기관을 보호하기 위해 27여 년을 사이버 범죄에 맞서 싸워왔습니다. 수상 경력에 빛나는 실시간 침입 탐지, 방지 솔루션은 SonicWall Capture Labs 연구의 지원을 받아 215개 이상의 국가와 지역에서 100만 개 이상의 네트워크와 이메일, 애플리케이션 및 데이터를 보호합니다. 당사의 솔루션을 채택한 조직들은 보다 효과적으로 운영되고 보안에 대한 두려움이 적습니다. 자세한 정보를 원하시면 www.sonicwall.com을 방문하시거나, [트위터](#), [링크드인](#), [페이스북](#), [인스타그램](#) 등에서 저희 사이트를 팔로우 해주시기 바랍니다.

본 자료 이용과 관련한 문의사항은 다음으로 연락해 주십시오.

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

저희 웹사이트에서 더 많은 정보를 보실 수 있습니다.

www.sonicwall.com