White Paper

From Remote Access to Secure Mobility: Enabling Next Generation Workforce Productivity (원격 액세스부터 시큐어 모빌리티까지: 차세대 인재 기반의 생산성 향상)

모빌리티가 중요한 이유

기술은 생산성을 증진할 수 있는 새로운 기회를 항상 만들어냈습니다. 기술 혁신, 특히 그 대대적 변화를 수용하고 적극 활용하는 기업은 시장을 제패하거나 그렇게 하지 못한 경쟁사를 누르고 시장 점유율을 확보합니다. 현재 새로운 기술의 대변혁이 시작되고 있습니다. 전사적 모빌리티가 대규모로 확장되면서 직원들은 언제 어디서나 일할 수 있게 되었습니다.

전사적 모빌리티가 기업에 새로운 개념은 아닙니다. 사실 원격 액세스와 재택근무 솔루션은 오래전부터 있었습니다. 그러나 새로운 것은 전사적 모빌리티 플랫폼에서 일어나는 놀랄 만한 속도의 변화 그리고 이를 뒷받침하는 기업의 능력이며, 또한 이러한 변화가 기존의 IT 조직이 아닌 직원들에 의해 시작되었다는 사실입니다.

각 기업에서 경쟁력을 유지하고 새로운 효율적 워크로드 모델로 발전하기 위해서는 모빌리티를 받아들여야 합니다. 오늘날 경기 침체로 인해 다운사이징과 글로벌 아웃소싱이 일반화되고 있습니다. 기업들은 더 적은 자원으로 더 많은 일을 해내야 합니다. 모빌리티의 수용은 인터넷으로 가능했던 것보다 훨씬 높은 수준의 생산성 증진이 가능하기 때문에 기업에 이득이 될 것입니다.

이는 경쟁력 측면에서 필연적 과제일 뿐 아니라 오늘날 노동 인구의 통계적 변화 또한 모빌리티를 요구하고 있습니다. 국제 사회에서 앞으로 20년 동안 베이비붐 세대가 은퇴하고 노동 인구의 비중이 줄어들게 되면서, Y 세대와 밀레니엄 세대가 빠른 속도로 늘어나 X 세대의 일부 노동력과 같거나 그보다 더 많아질 것입니다. 이 세대들은 소셜 웹, 인터넷 커뮤니티, 지속적인 커뮤니케이션, 정보 교환을 신봉합니다. 오늘날 젊은 직원 중 상당수는 퍼베이시브 인터넷 환경에서 성장한 만큼 "24시간 온라인" 생활을 하는 능력을 기업적 목적을 위해 사용한다면 생산성 향상에 매우 유용하게 사용될 것입니다.

모빌리티 도입의 과제

기업들은 네트워크 및 보안 인프라를 구축하고 경계 영역에 정교한 연결 지점을 마련하면서 원격 연결을 지원하는 데 많은 비용을 투자했습니다. 실제로 VPN은 노트북 컴퓨터가 대표적인 모빌리티 디바이스로 자리 잡는 데 큰 역할을 했습니다. 그러나 상황은 빠르게 바뀌고 있습니다. 스마트폰과 태블릿이 불과 몇 년 전에 PC 기반 디바이스에서 제공하던 수준을 뛰어넘는 컴퓨팅 성능을 갖추고 더 내실 있고 뛰어난 디자인의 사용자 인터페이스, 스마트폰의 경우 음성 통신 디바이스로서의 위상, 기본적으로 지원되는 퍼베이시브 무선 연결 기능을 내세우면서 직원들이 선호하는 디바이스로 급부상했습니다.

아마 기업의 최대 당면 과제는 통제를 상실한 것일 것입니다. 이 새로운 시대에는 기업의 직원이기도 한 소비자가 흐름을 주도하고 있습니다. 이들은 더 세련된 인터페이스, 우수한 사용자 환경, 뛰어난 편의성을 지닌 디바이스에 기꺼이 투자합니다. 직원들은 회사 네트워크에서 (허가를 받거나 받지 않은 채로) 이러한 디바이스를 활용할 방법을 모색하며, 이를 저지하는 회사의 기준은 빠른 속도로 도외시되고 있습니다.

변화의 속도 역시 기업에 만만치 않은 과제입니다. 기업의 IT 팀은 더욱 늘어나는 새로운 모바일 플랫폼에 신속하게 적응하면서 새로운 디바이스의 관점에서 보안 실태와 프레임워크를 재평가해야 합니다. 소비자는 표준이 제정되는 속도보다 빠르게 새로운 기술을 받아들이고 있습니다. 그리고 이 새로운 모바일 폼 팩터에 대한 지원 요청이 쇄도하면서 이를 관리하는 툴이 감당할 수 없는 상황입니다.

아마도 가장 근본적인 과제는 새로운 액세스 모드를 보호하는 것입니다. 사실상 "외강내유"의 기존 보안 패러다임은 현재의 모빌리티 환경에서 더 이상 유효하지 않습니다. 경계 영역은 이미 사라졌으며 네트워크 에지는 모바일 직원의 손바닥을 비롯하여 어디에나 있습니다. 이러한 모바일 디바이스를 분실할 경우 기업은 어떤 책임을 지게 될까요? 기존의 보안 위협이 네트워크에 유입되는 데 모바일 디바이스는 어떤 역할을 할까요? 기업은 PC와 같은 폼 팩터에 대해서는 이러한 문제를 해결할 인프라를 갖추고 있을 것입니다. 하지만 새로운 폼 팩터의 경우 기업 데이터를 지키고 네트워크를 보호하고 애플리케이션 액세스를 위해 적합한 서비스 레벨을 제공하지 못하고 있습니다.

해결책: Secure Mobility

기업과 그 IT 팀은 안전하게 모빌리티를 활성화할 프레임워크와 솔루션이 필요합니다. Cisco는 액세스, 보안, 선택을 지원하는 시큐어 모빌리티(Secure Mobility)가 해결책이라고 확신합니다.

- 사용자가 업무 수행에 필요한 애플리케이션 및 정보에 손쉽게 **액세스**
- 위협으로부터 엔드포인트를 보호하고 디바이스에 전사적 정책을 적용하는 정확한 **보안**
- 사용자가 어떤 툴을 사용할지 **선택할 수 있게** 다양한 디바이스를 지원

이러한 근본적인 요소가 기업에서 모빌리티를 수용하기 위해 갖춰야 할 토대가 됩니다.

Cisco의 가치 제안

Cisco는 시큐어 모빌리티를 선보이면서 기업의 활동과 관련된 모든 사람에게 "언제 어디서나" 최적화된 연결을 제공하는 네트워크 보안 상태를 제시합니다. 효과적으로 안전하게 모바일 인력을 지원하는 각종 솔루션으로 구성된 Cisco® AnyConnect Secure Mobility 솔루션이 이 프레임워크에 해당됩니다. AnyConnect 솔루션은 Cisco ASA Series 어플라이언스, Cisco AnyConnect Secure Mobility 클라이언트 그리고 웹 보안을 위한 Cisco IronPort Web Security Appliance 또는 Cisco ScanSafe로 구성됩니다.

AnyConnect Secure Mobility Solution

Cisco AnyConnect 클라이언트는 통합 엔드포인트 소프트웨어 클라이언트로서 현재 판매되는 모든 주요 엔터프라이즈 모빌리티 플랫폼(PC와 소형 폼 팩터)과의 호환성을 제공합니다. 기본 VPN 기술을 토대로 한 AnyConnect Secure Mobility 솔루션은 가치 제안의 범위를 원격 액세스에 한정하지 않고 새로운 차원의 사용자 편의성 및 첨단 네트워크 기반 보안으로 확장합니다. 엔드포인트 컴퓨터 디바이스에서 실행되는 AnyConnect Secure Mobility는 방화벽의 뒤에서 네트워크 패브릭의 보안을 지원하고, 회사 방화벽의 바깥에서 액세스하는 모바일 사용자에게 전례 없는 수준의 보안 및 기업 정책을 적용합니다.

이제 모빌리티 지원에 나선 기업들이 해결해야 할 보안 과제를 자세히 조명하고, AnyConnect Secure Mobility 솔루션으로 현재의 실태와 시큐어 모빌리티가 약속하는 미래의 격차를 해소할 방법을 알아보겠습니다.

엔터프라이즈 모빌리티 지원에서 겪게 될 문제

VPN의 구멍—VPN은 모바일 직원에게 유연성이라는 장점을 제공하지만 현재 엔터프라이즈 환경에서 가장 큰 보안 허점 중 하나로 지목됩니다. 기업들은 인터넷 에지 경계를 강화하는 데 엄청난 비용을 투자하고 있으나, 노트북 컴퓨터가 그 에지의 일부라는 사실을 깨닫지 못하고 있습니다. 인터넷 활동이 기업 네트워크를 통해 유입될 때 추가적인 웹 프록시 기술로 유해한 사이트를 차단할 수 있습니다. 현재 시판 중인 대부분의 VPN 클라이언트는 종종 세션 시작을 반복해야 하므로 엔드 유저에게 큰 불편을 줄 수 있습니다. 이러한 제약 및 대역폭과 관련된 문제가 맞물리면서 엔드 유저는 VPN을 시작하지 않고 자유자재로 인터넷을 돌아다닐 수 있게 되었습니다. 보호되지 않는 인터넷 서핑으로 인해 사실상 스플릿 터널이 생겨나면서 악성코드가 엔드포인트를 감염시키고 더 나아가 그 디바이스가 연결되면 회사 네트워크에 확산될 위험이 있습니다.

Cisco AnyConnect Secure Mobility Solution은 기존 VPN의 허점을 해결할 수 있도록 지원합니다. 2010년에 Cisco는 구성 가능한 지속적인 VPN과 통합형 웹 보안을 갖춘 PC용 크로스 플랫폼(Windows, Mac, Linux) 솔루션을 내놓은 최초의 벤더가 되었습니다. "항상 연결" 모드에서 실행되는 이 AnyConnect 솔루션은 Cisco IronPort® Web Security Appliance를 통해 일관성 있는 사용 및 보안 정책의 적용을 지원합니다. Cisco AnyConnect 클라이언트의 인증서는 사용자가 연결된 위치(물리적 기업 경계의 안쪽 또는 바깥쪽)에 따라 달라질 수 있는 구체적인 웹 사용 정책과 보안을 적용합니다.

"다크 웹(Dark Web)"—웹 도메인이 폭발적으로 늘어나면서 인터넷의 대부분은 미분류 상태입니다. 그리고 현재 PC 엔드포인트 감염 대부분은 악성 웹 사이트를 통해 확산됩니다. 다크 웹을 이루는 IP 주소를 더 정확하게 분류하기 위해서는 상관성 분석과 적극적인 검사가 필요합니다. Cisco는 업계 최고의 웹 평판 필터링 및 동적 실시간 분류 기술을 사용하여 이러한 웹 사이트를 파악합니다. Cisco의 SIO(Security Intelligence Operations) 센터에서는 장기적으로 글로벌 차원에서 Cisco 보안 어플라이언스 및 제품 대부분으로부터 수집한 IP 정보의 상관성을 분석합니다.

포트 80 포털(Port 80 Portal)—인스턴트 메시징과 같은 TCP 기반 애플리케이션이 엔드포인트 보안 감염의 주요 경로라는 사실이 오래전에 밝혀졌지만 상황은 더욱 나빠졌습니다. 오늘날 Web 2.0 애플리케이션을 통해 새로운 차원의 고속 커뮤니케이션과 소셜 인터랙션이 활성화되면서 악성 링크와 보안 위협은 과거 어느 때보다도 심각한 위험이 되었습니다.

AnyConnect Secure Mobility 솔루션은 포트 80을 지나는 모든 엔드포인트 트래픽을 대상으로 정밀한 악성 콘텐츠 검사를 실시합니다. 또한 사용자 또는 그룹 ID에 따른 일관성 있는 보안 정책을 적용하여 특정 웹 애플리케이션에 대한 액세스를 허용하거나 거부할 수 있습니다.

SaaS 누설—모빌리티의 가속화에 기여한 또 다른 부차적 트렌드는 기업의 애플리케이션이 사내 데이터 센터의 바깥으로 이동한 것입니다. 웹 기반 애플리케이션은 인터넷 연결을 지원하고 브라우저 액세스를 제공하는 어떤 디바이스에서도 액세스할 수 있습니다. 이러한 흐름에 힘입어 기업 데이터가 SaaS(software-as-a-service) 비즈니스 애플리케이션을 호스팅하는 공용 인터넷 사이트에 저장되는 경우가 늘고 있습니다. IT 팀은 사내에서 얼마나 광범위하게 SaaS 애플리케이션이 사용되는지조차 모를 수도 있습니다. 허가받고 지원되는 SaaS 애플리케이션에서도 이 분산된 애플리케이션에 대한 액세스를 모니터링하고 관리하는 것은 만만치 않은 일일 것입니다. AnyConnect Secure Mobility 솔루션은 SAML(Security Assertion Markup Language)을 사용하여 한군데서 SaaS 애플리케이션을 관리하고 인증을 취소할 수 있도록 지원합니다. 사용자는 지원되는 애플리케이션에서 또 다른 비밀번호를 기억할 필요가 없습니다. IT 팀에서 그 사용자의 액세스를 차단하지 않았다면 주요 SaaS 애플리케이션에 편리하게 액세스할 수 있습니다.

디바이스 분실—스마트폰이나 태블릿을 분실하거나 도난당하면 금전적 손해, 개인 정보와 업무 정보 상실, 생산성 저하 등 그 소유자에게 큰 타격이 될 수 있습니다. 하지만 회사가 운영 및 법적 차원에서 입을 수 있는 피해는 그보다 훨씬 심각합니다. 그 디바이스에 저장되었던 중요 정보의 유출 및 남용 가능성과 디바이스가 주요 비즈니스 시스템에 접근하는 데 사용될 가능성 때문에 기업은 사고 대응, 정보 및 시스템 복구, 정보 공개로 인한 의무 비용으로 수백만 달러는 아니더라도 수천 달러를 지출해야 합니다.

모바일 디바이스 분실에 대비한 일차적인 보호 수단으로, 기업 정보에 액세스할 수 있는 모든 모바일 사용자에 대해 종합적인 디바이스 보안을 적용해야 합니다. Cisco AnyConnect Secure Mobility 솔루션은 디지털 인증서의 사용을 지원합니다. 디바이스가 분실될 경우 즉시 인증서를 취소하여 네트워크에 대한 액세스를 차단할 수 있습니다. PIN 잠금, 디바이스 암호화, 전화기 "탈옥" 금지와 같은 정책을 시행하면 디바이스가 분실되더라도 보호하고 모바일 OS 플랫폼의 개방으로 유입되는 위협을 줄일 수 있습니다. 모든 기업은 어떤 스마트폰 및 태블릿 정책이 필요한지 판단하고 각 플랫폼의 기능과 연계하면서 그러한 수준의 보안을 적용해야 합니다. Exchange ActiveSync 정도면 충분한 곳도 있고, AnyConnect의 기본 디바이스 보안 기능을 보완하고 확장할 모바일 디바이스 관리 솔루션의 고급 기능이 필요한 곳도 있을 것입니다.

IT의 소비자화 —옛날에는 직원이 사용할 IT 장비의 유형을 회사에서 지정 했습니다. IT 팀은 이러한 조치를 통해 디바이스 및 엔드포인트를 지속적으로 제어하면서 일관성 있는 보안을 적용할 수 있었습니다. 이제 IT 환경은 직원이 각자의 모바일 디바이스를 구매하거나 IT 팀에서 디바이스 구매 비용을 보조하는 모델로 바뀌고 있습니다. 어느 쪽이든 직원이 기업 네트워크에서 사용할 디바이스를 직접 선택합니다. 이와 같이 직원이 유연성과 선택의 혜택을 누리게 됨에 따라 IT 팀은 더 이상 각 디바이스에서 어떤 이미지를 사용할지 지정할 수 없게 되었습니다. 각 디바이스가 개인 소유이기 때문입니다.

AnyConnect Secure Mobility는 각 엔드포인트에서 AnyConnect 클라이언트를 실행하면서 이러한 문제를 해결합니다. 노트북 컴퓨터, 스마트폰, 태블릿의 다양한 디바이스를 지원하므로 기본적인 보안 연결 기능을 수월하게 적용하고 항상 실행할 수 있습니다. 뿐만 아니라 Cisco Web Security Appliance 또는 ScanSafe의 기본적인 웹 보안 기능이 사용자가 사무실에서 또는 원격으로 정보에 액세스하는 어떤 경우에도 일관성 있는 정책의 적용을 보장합니다.

결론

기업은 IT 소비자화와 그에 따른 새로운 모바일 디바이스, 연결, 애플리케이션의 유입에 맞서기보다는 직원과 파트너의 생산성과 창의력을 강화할 수 있는 모델로서 모바일 환경을 받아들여야 합니다. 모빌리티는 대세로 자리 잡았습니다. 이제 IT 팀은 이 모바일 디바이스에서 일관성 있게 보안을 적용할 방법을 찾아야 합니다.

Cisco AnyConnect Secure Mobility를 선택한 기업은 모빌리티를 받아들이고 기존 인프라와 프로세스를 십분 활용하면서 언제 어디서든 어떤 디바이스의 누구에게나 보안 액세스를 제공할 수 있습니다.

Cisco AnyConnect Secure Mobility Client에 대한 자세한 내용은 다음 사이트에서 확인하십시오.
http://www.cisco.com/en/US/netsol/ns1049/index.html

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C11-641140-01 04/11