이동성 관리 - 기업의 안전한 무선 네트워크 제어

이 홍 인

Red-M Communications, Inc.

Managing Mobility - Enterprise Secure Wireless Control

Daniel H. Lee

Red-M Communications, Inc.

Abstract

80년대 초반에 등장한 퍼스널 컴퓨터에서부터 90년대에 급격히 확산된 클라이언트/서버 환경에 이르기까지 분산 컴퓨팅은 관리가 어렵다고 증명되었다. IBM의 Tivoli나 HP의 OpenView 등을 포함한 거대한 엔터프라이즈 관리 시스템 산업이 이러한 표면상의 극복하기 힘든 법칙처럼 여겨지는 것이 그 증거라고 하겠다.

이 후 무선의 개념이 등장했다. NOP World Technology가 Cisco사를 위해 2001년에 시행한 조사에 의하면 최종 사용자는 무선랜을 사용함으로써 생산성이 최고 22% 향상되었고 조사 대상의 63%가 일상적인 직무에서 정확도가 향상되었다. 이 모든 것은 투자대비수익(ROI) 계산상 사용자 당 $550 해당한다. 현재 이동성과 IT 관리 기능의 딜레마를 동시에 고려하며 저렴한 몇몇 솔루션들이 소개되고 있다. 본 논문에서는 분산 컴퓨팅의 다음 진화 단계인 무선 네트워킹과 관련된 문제를 해결할 수 있는 혁신적이고 전체적인 접근법을 소개한다.

본 논문에서는 무선 컴퓨팅과 보안의 본질 및 무선랜이라는 새로운 컴퓨팅 패러다임으로 인하여 파생되는 운영과 관리의 어려움을 소개한다. 이러한 환경이 정의되면 본 논문은 이해하기 쉬운 5x5 레이어 매트릭스를 바탕으로 각 레이어의 독특한 본질을 고려한 혁신적인 무선랜 관리 방법에 대해 설명한다. 마지막으로 무선 네트워킹, 컨버전스, 궁극적으로 분산 컴퓨팅만이 가지는 문제점을 해결할 수 있는 Red-M의 백 오피스 애플리케이션에 기반한 솔루션을 소개한다.

본 논문의 목표는 Red-M의 성공에 관한 두 가지 중요한 관점을 설명하고자 함이다. 이는 안전한 무선 네트워크 제어에서 비롯되는 무선 환경이 약속하는 장점들을 고루 제공하는 것과 나쁜 의도의 사용자를 차단할 뿐 아니라 올바른 사용자와 또한 나머지 일반 사용자를 총체적으로 관리할 수 있는, 안정적이고 확장 가능하며 직관적인 시스템을 제공하는 것이다.

1. 서 론

요즘 누구의 말을 듣던지 주요 기술 애널리스트는 무선 네크워크 시대가 열렸다는 사실에 동의한다.

IDC가 무선랜 관리 분야가 미국에서 2억달러 시장이라고 하거나 Jupiter Research가 미국의 무선랜 장비 시장이 8억8천만 달러라고 하는 것을 믿는지는 중요하지 않다. 또한 Infonetics Research가 2002년 북미 무선랜 하드웨어 매출액이 16억8천만 달러라고 하는 것을 받아들이는지도 중요하지 않다.

이는 결국 모두가 같은 말을 하고 있기 때문이다. 시장은 거대하며 빠르게 성장하고 있다는 것이다. Jupiter는 무선 장비 시장이 매년 2배 이상으로 증가하여 2006년에는 23억 달러에 이를 것이라고 과감히 예측하고 있다.

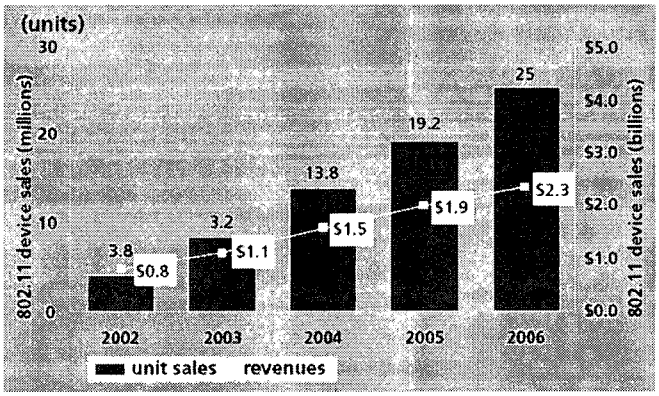


그림 1. 기업용 Wi-Fi 장치 매출액 (미국)

(출처: Jupiter Research Wi-Fi Model, 2003년 3월)

이렇게 폭발적인 무선 장비 시장의 성장 보고서들은 서로 다른 이종의 기술 환경을 관리하는데 따르는 어려움을 쉽게 인식하게 만든다. 여기에 IT 자산에 이동성이 부여되어 돌아다니게 되고 분주한 공항처럼 새로운 노드가 수시로 생성되고 소멸되는 모바일차원을 결부시켜 생각한다면 결국 이런 모든 유동적인 환경은 IT 관리를 거의 불가능한 것처럼 보이게 만들 것이다.

이동성을 고려하여 설계된 장치는 수시로 네트워크

간 또는 서브넷 간을 자유롭게 로밍하기 때문에 우리에게 이미 익숙한 분산 컴퓨팅 관리의 어려움은 더더욱 증폭되는 것이다. 이러한 대개의 IT 자산들은 자유로운 이동성이 부가되었을 뿐 아니라 더 이상 컴퓨터처럼 생기지도 않았다. 무선의 팽창으로 촉발된 통신 산업과 컴퓨팅의 융합을 의미하는 컨버전스는 공상과학 소설에서 나온 것 같은 완전히 새로운 장르의 장치를 만들어냈다.

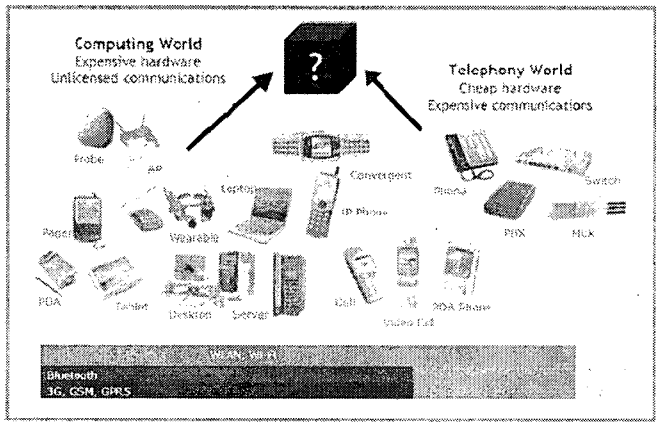


그림 2. 컨버전스 - 통신과 컴퓨팅의 융합

2. 본 론

2.1 새로운 위협

무선의 등장과 팽창, 분산 컴퓨팅 관리의 어려움과 컨버전스 현상은 새로운 종류의 위협을 초래한다. 새로운 위협은 명백한 것부터 잘 알 수 없는 것까지 다양하고 치명적일 수 있다. 인가되지 않은 사용자가 네트워크 대역폭을 점유하거나 데이터를 기록할 수도 있고, Rogue AP로 불리는 인가되지 않은 AP 장치를 통하여 아이디나 암호 같은 로그인 정보를 획득하고 전자우편을 해독하거나 통신을 불통시켜 업무를 마비시키는 서비스 거부 공격(DoS)을 감행할 수도 있다.

이러한 새로운 위협은 네트워크 사용자가 자신의 환경을 조금 개선하기 위해 취하는 무해한 행동에 의해 아주 흔히 발생한다.

윈도우 기반의 노트북끼리 ad-hoc 방식의 간단한 peer-to-peer 네트워크를 구성하거나, PDA로 파일 전송, 전자우편 동기화 등을 위하여 블루투스 또는 무선랜을 사용하는 등의 안전하지 않은 네트워크 연결을 시도하는 경우는 아주 흔하다. 그러나 결국 이런 무해하고 눈에 보이지 않는 연결들이 사용 네트워크를 새로운 형태의 업무마비 위협에 손쉽게 노출시키는 것이다.

무선 칩셋과 무선 기능이 탑재된 운영체제는 일반 사용자가 상당한 비용을 들여 구축한 방화벽 속에서도 빠르고 쉽게 결함을 만들 수 있기 때문에 악의적인 해커가 쉽게 활동하거나 서비스 중단을 초래할 수 있는 환경을 제공하게 된다.

실제로 도심지를 전형적으로 조사하면 사용 중인 모든 무선랜 장치의 70% 이상이 아무런 보안 수단이 없이 사용되고 있다. 이런 높은 수치는 대부분의 무선랜 하드웨어에 포함된 기본 보안 설정은 노트북과 50달러 정도의 추가 하드웨어, 인터넷에서 다운 받을 수 있는 프리웨어 유틸리티 프로그램만 있으면 약 20분 이내에 해킹이 가능하므로 놀라운 일도 아니다.

초보 해커라도 그 정도만 있으면 Wired Equivalent Privacy (WEP) 암호화 방식을 해킹할 수 있다. WEP은 대부분의 경우 비활성화 상태로 출고 되고 WEP을 적용한 간단한 무선 네트워크를 구성하려면 조금의 노력이 더 필요하므로 무선 장치의 3분의 2가 아무런 보안도 사용하지 않는 것은 당연한 결과이다. 상기 조사에서 대부분의 무선 AP가 출고 시 설정을 그대로 사용하 고 있어서 ID 정보를 송출하고 있음을 알 수 있다. 이는 해커들이 더욱 손쉽게 AP를 발견하고 해킹을 시도 할 수 있음을 의미한다.

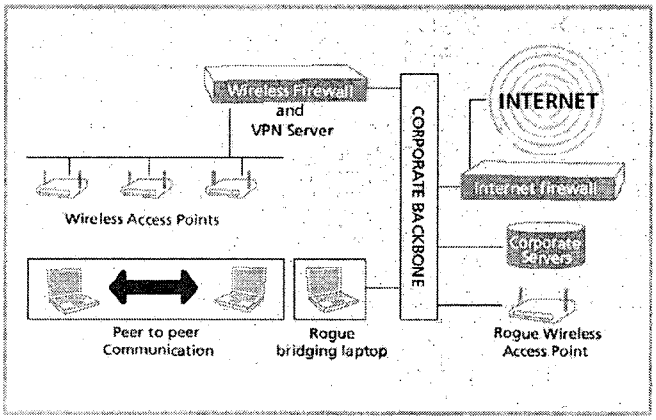


그림 3. 네트워크 내 무선 보안의 위협

2.2 다양한 솔루션

새로운 장치와 기존의 문제점, 그리고 눈에 보이지 않는 위협들은 급기야 다양한 솔루션과 솔루션 제공자를 탄생시켰다. 하지만 이러한 소프트웨어, 하드웨어, 전문가 서비스를 통한 문제 해결책은 표준화 기구가 확대되는 이동성 요구를 수용하기에는 역부족일 만큼 많이 쏟아져 나온 것이 현실이다. 현재 1세대 보안 형태 (예: 802.1x, WPA 등)의 문제점을 보완하기 위해 다수의 새로운 표준화 작업이 진행 중이지만 새로운 표준이 확정되더라도 항상 새로운 소프트웨어, 하드웨어 및 실제 네트워크 구축에 적용에는 긴 시간이 더 필요하다는 것은

자명한 일이라 하겠다.

물론 현재에도 IT 관리자는 더욱 강력한 암호화 기술과 확고한 인증 방식을 채택한 솔루션을 이용하여 안정적이고 생산적인 무선 네트워크 환경을 구축할 수 있다. 하지만 제조사들이 경쟁적으로 주의를 끌려고 하거나 간혹 두려움, 불확실성 또는 의구심을 가지게 하는 상황에서 네트워크를 어떻게 구성하는 것이 최상의 방안이라 할 수 있는가?

무선 영역에서의 보안성 확보를 위해 가장 많이 사용하고 있는 방법은 안정성이 입증된 가상 사설망 (VPN)을 이용하는 것이다. 이 방법은 보안을 요하는 컴퓨터를 기업 중심에 위치시키며 무선 영역을 접근할 때에는 보안 수준이 매우 높은 방법으로 사용자를 인증한다. 그러나 이러한 방법은 태생적으로 보안의 결점을 지닌 무선 네트워크에 보안 개념을 도입하기 위한 첫 단계에 지나지 않으며 궁극적인 무선 보안 수단이 될 수는 없다. VPN은 보안성이 아주 높지만 본질적으로 병목이 되며 자연스럽게 확장이 가능하지 않다.

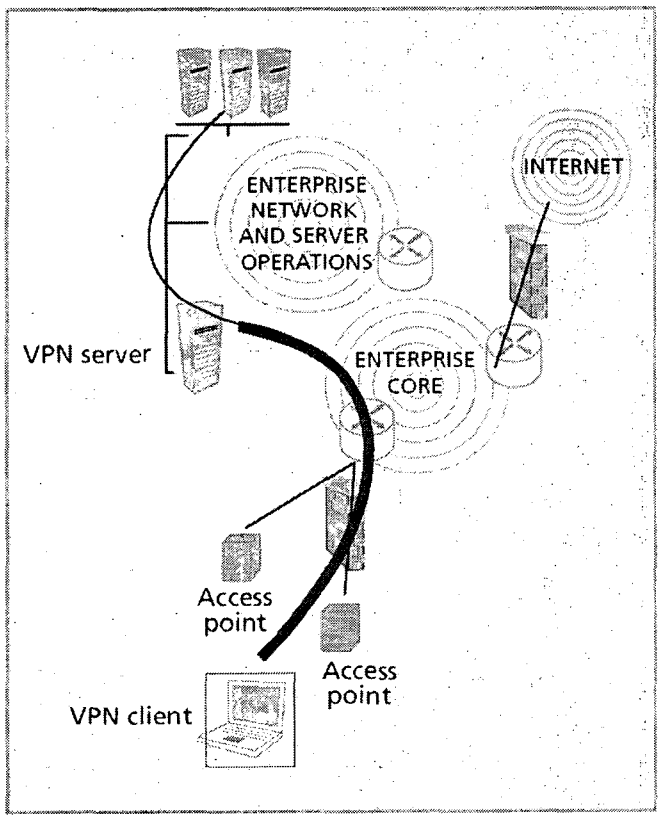


그림 4. 무선 VPN 구현 모델

Accenture는 자사의 "Wireless LAN: Friend or Foe" 라는 기술백서에서 무선랜의 문제가 제어가 불가능한 상태로 발전하기 전에 무선 네트워크를 이해하는 방법에 대하여 지속적인 위험요소 평가, 보호 전략, 지속적인 관리 등의 3단계로 표현했다. 또한 이 3단계 절차를 적절한 도구와 업계의 최상의 운영방안을 토대로 통합했을 때야만 비로서 무선 네트워킹이 제공하는 투자대비수익(ROI)을 실현할 수 있다고 지적했다.

그러나 무선 영역은 진공상태에 존재하지 않는다. 크고 작은 조직이 고정된 네트워크에서 이동 환경으로 변화하면서 무선 네트워크는 예상대로 기존 유선 네트워크에 연결된다. 진정으로 전체적인 솔루션을 추구한다면 기존의 유선 네트워크의 많은 부분이 무선 영역과 연동되므로 기존 유선 네트워크도 함께 고려되어야만 한다.

실제로 이미 전통적인 네트워크와 무선 움직임의 경계선이 되돌릴 수 없을 만큼 불분명해졌으며 만일 이 중 어느 하나만 관리하려고 한다거나 두 가지 환경을 모두 고려하지 않은 솔루션을 사용하고자 한다면 시작부터 결국 실패하고 말 것이다. 여기에 반드시 고려되어야 하는 독특하고 도전할만한 분산 컴퓨팅의 특성도 여전히 존재하고 있다. 사용자들은 더미 터미널에서 데스크탑 컴퓨터로 기술의 흐름 전환이 이루어지는 가운데 오늘날에는 거의 없어진 메인 프레임의 가장 성공적인 면, 즉 중앙 집중 제어라는 컨셉트를 포기했다.

컴퓨터가 개인용으로 전환되면서 제어에 관한 문제는 비공식적이지만 각각의 개인 사용자에게 맡겨진 것이다. 권한의 분배를 수반해야 했을 책임의 분배는 결코 실현되지 않았고 이미 상황은 걷잡을 수 없어진 것이다. 무어의 법칙이 실제 재현되는 상황 속에서 심각한 제어 능력의 부재, 이것이 오늘날 우리가 처한 현실이라 하겠다.

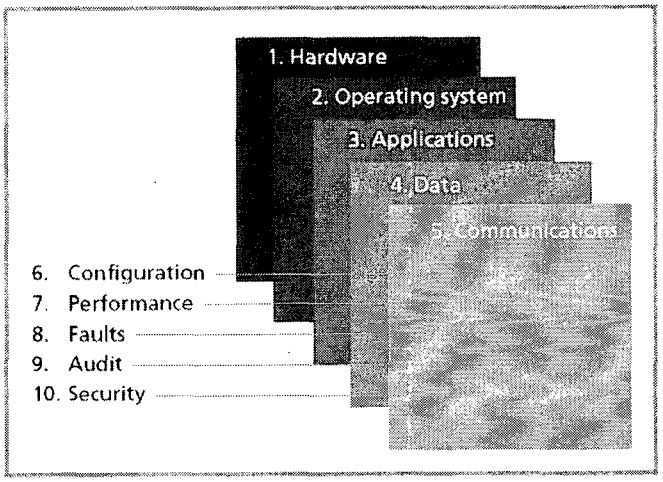


그림 5. 5x5 레이어 모델 - 네트워크 장치 x 관리

최종 사용자 단말장치 수준에서 발생하는 문제는 각각의 사안별로 대처할 수 있게 세분화 되었을 때에만 완벽하게 관리할 수 있다.

레이어는 하드웨 어, 운영체제, 응용프로그램, 데이터 통신의 5가지 논리적 장치 레이어를 한 축으로 하고

설정, 성능, 오류, 오디트, 보안의 5가지 논리적 관리 레이어를 다른 축으로 하는 매트릭스로 세분화 할 수 있다.

Red-M의 솔루션은 이러한 중요한 목표를 달성하도록 고려하여 설계되었다. 이러한 주요 관점들과 기업 네트워크 관리의 문제점에 대한 Red-M의 장기적인 지식이 접목되어 독특하고 혁신적인 Red-M 솔루션을 탄생시킨 것이다.

2.3 고정 무선 감시

무선 영역의 관리와 안전한 무선 제어의 제공은 컴퓨팅 환경의 최종 단에서 시작해야 한다. 바로 이 최종 단에서 중요한 실시간 데이터를 수집해야 하며 그것을 토대로 새로운 환경을 분석하기 시작해야 한다. 지능형 프로브를 고정된 메쉬 망 형태로 배치하고 상시(24x7) 정보를 획득한다는 착상은 새롭거나 Red-M만의 생각은 아니지만 이를 구현한 방법이나 플랫폼은 절대 쉬운 일이 아니며 현재 Red-M 만이 가지고 있는 독창적인 부분이라 하겠다.

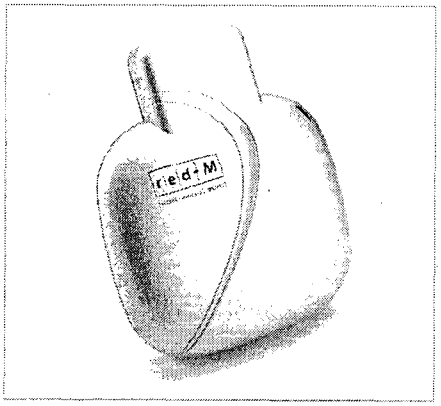


그림 6. Red-M사의 Red-Alert PRO 프로브

Red-M의 Red-Alert PRO 무선 감시용 프로브는 현재 가장 많이 사용중인 2.40 ~ 2.48GHz 대역의 802.11b나 g의 신호를 탐지할 뿐만 아니라 Red-M의 특허 기술을 적용하여 다른 대역의 무선 네트워크 주파수까지도 탐지할 수 있다. 북미에서 제조한 탐지 장비는 채널 1에서 12까지 사용하지만 Red-M의 지능형 프로브는 아시아에서 제조된 칩을 사용하여 추가적으로 채널 13과 14도 역시 검색하고 탐지할 수 있다. 다른 시스템에서는 채널 13과 14를 이용하면 보안에 구멍이 뚫린다. 따라서 Red-Alert PRO는 무선 침입탐지시스템(IDS)를 구축하는데 최고로 튼튼한 기초가 된다 하겠다. Red-Alert PRO 프로브는 가장 작은 외형으로 여러 대가 함께 배치될 수 있으며 추가 안테나를 사용하면 사용 빈도가 적은 주파수까지 탐지 할 수 있다. 5.72 ~ 5.85GHz 대역의 802.11a 무선랜이나 블루투스가 여기에 해당된다. 100미터 범위를 갖는 블루투스 탐지 기능을 포함 함으로써 Red-Alert PRO는 컨버전스의 공백을 메울 수 있는 유일한 독립형 무선 침입 탐지 솔루션으로 인정된다. Red-Alert PRO 프로브는 802.11a/b/g 또는 블루투스를 장착한 노트북 등의 존재를 포착할 뿐만 아니라 대중적인 소 출력 네크워크 용 무선 주파수(RF)에 기반한 최신의 타블렛 PC, 휴대전화기, PDA, 기타 소형 휴대 데이터 장치의 존재마저도 손쉽게 포착할 수 있다.

Red-Alert PRO는 작은 외형, 기능 및 가격의 조합으로 인한 성공이라 할 수 있다. 이 놀라운 장치는 60MHz의 강력한 ARM 940T 프로세서, 32MB 램, 2MB의 읽기 전용 플래시메모리를 내장하고 있어 한번에 1000개 정도의 무선 이벤트를 저장할 수 있다. Red-Alert PRO는 실행속도, 보안 및 코드 사이즈를 고려하여 eCOS라 불리는 아주 가볍고 독립화된 버전의 레드햇 리눅스를 운영체제로 사용하고 있다.

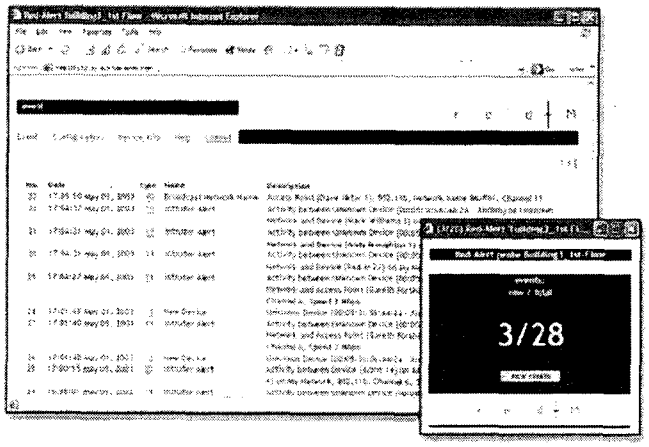


그림 7. Red-M Red-Alert PRO 이벤트 화면

Red-Alert PRO는 표준 규격의 RJ-45 LAN 커넥터를 사용하며 원격 업그레이드를 지원하고 IEEE 802.3af PoE (Power over Ethernet) 표준을 준수하여 손쉬운 배치와 사용, 그리고 관리가 가능하다.

2.3 완벽한 공중 영역의 관리

무선 도메인에 대한 위협은 다양한 형태와 크기로 나타나며 기술과 해킹의 지속적인 발전으로 두드러진다. 일반적으로 해킹이나 공격의 범위는 간단하고 보편적인 형태에서부터 심각한 피해를 줄 수 있는 것까지 다양하다. 예를 들자면 넷스텀블러 프로브와 같은 도구를 사용하여 단순히 무료 접속을 시도하는 워 드라이버 (war driver)같이 표면적으로는 악의가 없는 유형에서 간단한 위협이 발생할 수도

있지만, 또 한편 이러한 프로브 장치가 고의적인 해커에 의하여 악의적인 목적으로 주요 사용자 네트워크 인프라 정보를 수집하거나 취약점을 알아내는 도구로 사용되기도 한다.

더 심각한 위협들은 이보다 훨씬 더 고약하고 큰 피해를 입힐 수 있는 것이 많은데 그 중에**"Man-in-the-middle"**이라 불리우는 공격의 경우는 대상 클라이언트로 하여금 원하는 대상 접속 포인트로 믿도록 네트워크가 제공하는 최적의 암호화 및 인증 메커니즘까지 투명 전달하는 기능의 인가되지 않은 엑세스 포인트를 통하여 기업의 기밀정보에 접근할 수 있는 사용자 권한을 가로채기도 한다.

무선 침입 탐지(IDS) 및 공중 영역 관리 (airspace management)는 무선통신 활동의 시작이 되는 구간인 무선 주파수 감시에 그 기초를 두게 된다. 즉, 일반적인 무선 인프라 운용과 더불어 무선 구간에 고정 메쉬 형태의 탐지 프로브들을 추가 설치함으로써 사용자는 자신이 사업을 영위하는 주요한 공중 영역에 대하여 확고한 제어와 소유권을 확보하게 되는 것이다. 이러한 메쉬 형태의 **24x7** 감시 프로브들은 기업으로 하여금 눈에 보이지 않는 공중 영역의 통신 상태와 **Rogue AP,** 인가되지 않은 네트워크의 설치 또는 통신, 그리고 **Peer-to-peer** 형태의 무선통신 활동 모두에 대하여 직접적이며 실시간으로 검색 및 탐지가 가능하게 해준다.

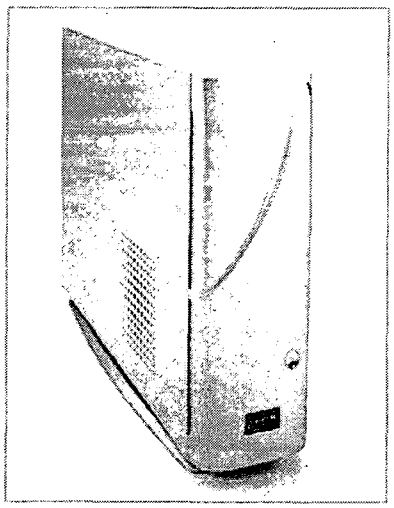


그림 **8. Red-M**사의 **Red-Detect** 서버

또한 이 무선 모니터링 기술은 모든 무선 활동 및 무선 설비에 대한 정보를 취합하거나 오디트 **(audit)** 기록을 저장할 수 있도록 하며, 기본적인 용량과 성능에 대한 계획을 수립할 수 있도록 하여준다. 이러한 일련의 요소들은 급격하게 발전하는 기업 설비에 의해 정의되는 엄격한 성능 수준을 만족시킬 수 있게 한다고 하겠다.

Red-M의 무선 침입 탐지 시스템은 특허 출원된 프로빙 기술과 서버 기반 기술인 장치의 분산 메쉬 형태의 네트워크를 활용한다. 프로브는 모든 눈에 보이지 않는 무선 통신 이벤트에 대하여 **24x7** 기반으로 탐지하고 기록하며 그들의 로컬 이벤트 데이터베이스를 **Red-Detect** 서버 장치로 실시간 전달한다. 여기서 **Red-Detect** 서버는 공격 유형과 높은 위험성의 접속 형태에 대한 상호 관계를 분석하기 위하여 취합 전달된 다수의 무선 활동 정보를 서버 내부의 지식베이스와 비교하게 된다.

Red-Detect 서버는 **Rogue AP** 및 디바이스에 대한 실시간 탐지, 불안정한 통신 상태 또는 **ad-hoc** 커뮤니케이션 등의 통신 상태 검색, 기업의 무선랜 정책 구현, 즉각적인 침입차단 및 전체 무선 도메인 구간의 운영 상태를 포괄적으로 감시하는 기능을 갖추고 확장성과 유연성을 동시에 보유한 중앙 집중 형태의 강력한 관리 시스템을 제공하게 된다.

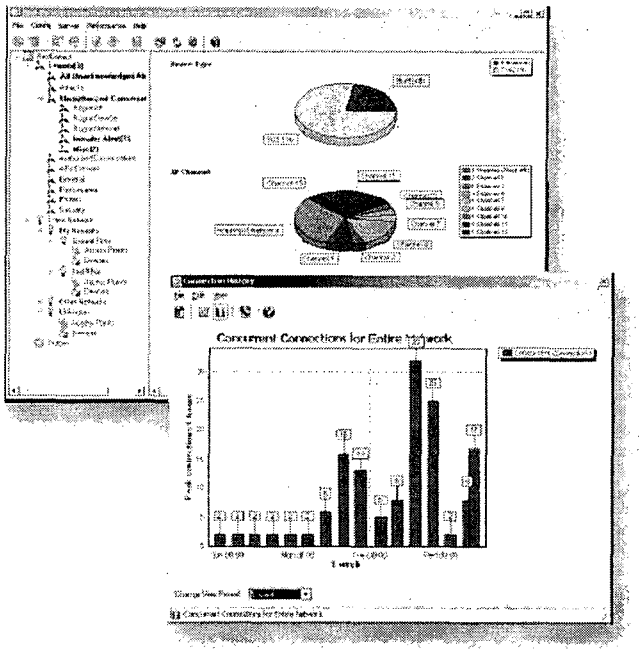


그림 **9. Red-Detect** 윈도우콘솔 화면

사용자 주변의 공중 영역과 관련된 정보의 지속적인 실시간 전달은 이벤트 정보를 취합하기 위한 중앙저장소, 실시간 정보연계, 그리고 미리 정해진 포맷과 **ad-hoc**과 같은 보고서를 필요로 한다. 무선 환경의 구성 요소들은 지속적으로 변화(모바일 디바이스들은 대부분 애초에 디자인되는 시점부터 짧은 라이프사이클을 지닌다.)하며 네트워크에 대한 때때로의 감시나 고정된 시점의 스냅샷 정도로는 오늘날의 보안 위협 또는 취약점의 범람 속에서 충분하지 않다고 하겠다.

그러므로 무선 **IDS**의 목적은 주변의 공중 영역상의 보안을 확고히 다지고 전체 무선환경에 대한 제어 권한을 소유하는데 있다고 할 수 있다. 이러한

이유에서 **Red-M**은 **Red-Alert PRO** 프로브에 기반하는 엔터프라이즈 급의 **IDS** 시스템인 **Red-Detect**를 제공한다. **Red-Detect** 중앙 서버에 의하여 연결된 모든 프로브에 대하여 분석이 이루어지고 그 결과는 무선 활동에 대한 포괄적이고 직관적인 화면과 관리보고서를 위한 유형별 그래프를 생성한다. 이러한 광범위한 무선 정보들은 의미 있는 오디트 트레일 **(audit trail)**, 미리 정해진 포맷이나 **ad-hoc** 보고 기능, 능동적인 경보 및 용량 관리 등을 제공하기 위하여 데이터베이스에 저장된다. **Red-Detect**는 수천 개의 프로브를 지원할 수 있도록 확장성을 지니며, 확장 필터들을 사용하여 사용자 정의 이벤트나 주요 관심 항목들만 나타낼 수 있도록 지능적인 형태로 커스터마이징이 가능하다.

Red-Detect는 앞서 설명한 업계 최고 기능의 프로브, 강력한 중앙 서버, 그리고 윈도우 관리 콘솔의 3가지 요소로 구성된다. 서버는 **2U** 랙 마운트 형의 서버 플랫폼 또는 소형 데스크탑 유니트로 구성할 수 있는데 공히 **2.6GHz** 펜티엄 **4** 프로세서, **533Mhz** 프론트사이드버스 **(FSB)** 구조, **40GB 7200RPM** 디스크 서브시스템, **512MB** 시스템 램 등의 사양을 지니며, **RedHat Linux 7.3, Red-Detect** 서버 소프트웨어, **DHCP,** 그리고 **PostgreSQL** 관계형 데이터베이스 서비스로 운영된다.

Red-Detect의 진 면목은 윈도우 **2000** 시스템 또는 윈도우 **XP**의 **Win32** 애플리케이션인 관리 콘솔에서 찾아볼 수 있다. 이 같이 잘 다듬어지고 안정화된 네이티브 윈도우 애플리케이션은 일반적인 **JAVA** 기반 또는 **HTML** 인터페이스 기반의 네트워크 관리 분야가 제공할 수 있는 것보다 훨씬 더 향상된 응답성과 확장성을 지닌 인터페이스를 제공한다. 콘솔은 사용자의 무선 도메인에 대하여 효율적이고 직관적인 단일, 가상, 계층적인 구조 보기 기능을 각각 제공하며, 사용자의 공중 영역에 대하여 모든 무선 트래픽 상황을 관리할 수 있는 인터페이스를 제공한다.

2.4 최상의 방어

최상의 방어가 때때로 좋은 공격이 된다는 말이야말로 기업의 무선랜 환경의 보호에 관한 적절한 표현이라고 생각된다. 사용자의 무선 도메인에 대한 위협은 순간순간 수시로 찾아오고 사라지며, 어떠한 사전 경고도 없이 사용자의 접속, 일상적인 네트워크 운용, 주요 데이터에 대하여 위험을 초래한다. 간단한 워 드라이버에서부터 고의적이고 악의적인 **"Mand-in-the-middle"**와 같은 위협들이 사용자의 무선네트워크에 적극적인 위협을 가하기 시작한다면 침입자를 탐지하기 위한 실시간 침입 감지 시스템이 필수적으로 요구되는 것뿐만이 아니라 이들 침입자를 차단하기 위한 응답시스템 역시 필수적이라 하겠다.

이러한 필요에 의해서 **Red-Detect**는 기업의 네트워크에 위협을 가하는 **Rogue** 디바이스들을 검색하고 그 기능을 방해하기 위한 방법으로 지능형 모니터링 센서들의 메쉬 망 활용을 극대화한다. **Red-Detect**는 잠재적 적의를 지닌 **Rogue** 디바이스가 사용자의 무선 네트워크에 있는 디바이스들에 타당하지 않은 연결을 시도하게 되면 이를 자동으로 찾아낸다.

이 시점에서 **Red-Detect**의 **CounterMeasures** 기능이 네크워크 운영자의 그래픽 사용자 인터페이스에 의하여 실행되며 **Rogue** 디바이스의 특정 연결 시도를 위한 기능을 차단하게 된다. 이 **Rogue** 디바이스는 **Red-Detect**와 인접한 프로브에 의하여 격리 감시되며 **Red-M**의 독자적인 기술 방식으로 위협 요소를 무력화시키게 된다. 이 후 격리된 위협의 요소들은 해당 네트워크 운영자 또는 보안관련 담당자가 적절한 보안정책을 적용하여 문제점을 해결할 수 있도록 정해놓은 시간 동안 지속적인 격리 감시를 받게 된다.

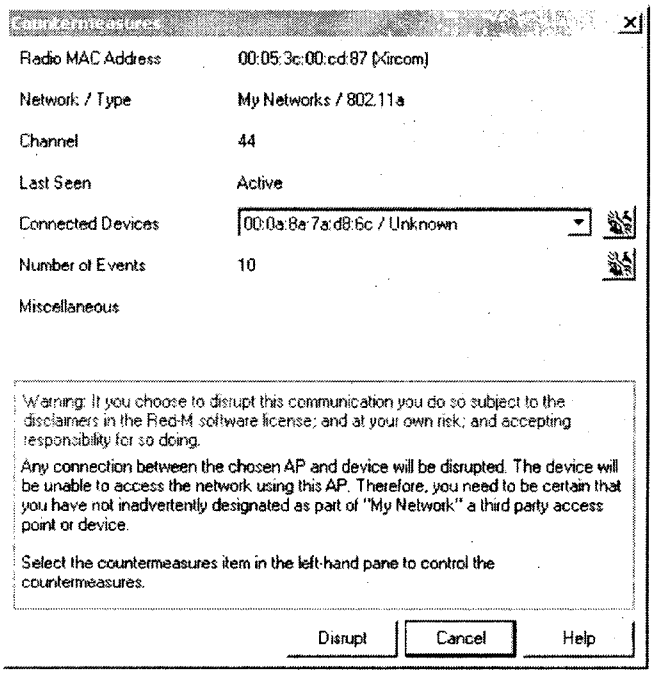


그림 **10. Red-Detect CounterMeasure** 화면

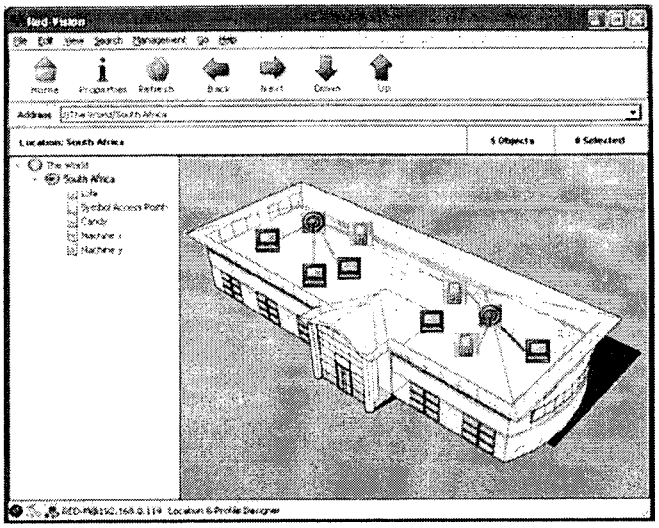
공중 영역에 설치된 고정 센서들의 지능형 메쉬 망과 중앙의 공격 프로파일에 대한 지식베이스의 조합을 통하여 **Red-Detect**는 무선 이벤트들의 상관관계를 분석하고 사용자에게 실시간으로 위협에 대한 경보를 전달하게 된다. 기업의 무선 네트워크를 포괄적으로 관리하기 위한 직관적이고 편리한 그래픽 사용자 인터페이스와, 잠재적인 위협 요소를 탐지하고 무력화 시키기 위한 능동적 **CounterMeasures**에 의하여 **Red-Detect**는 기업으로

하여금 무선 네트워킹의 다음 단계로 나아갈 수 있는 환경을 제공하고 이동성이 가져다 주는 이득과 장점을 완벽하게 인식하고 누릴 수 있도록 한다.

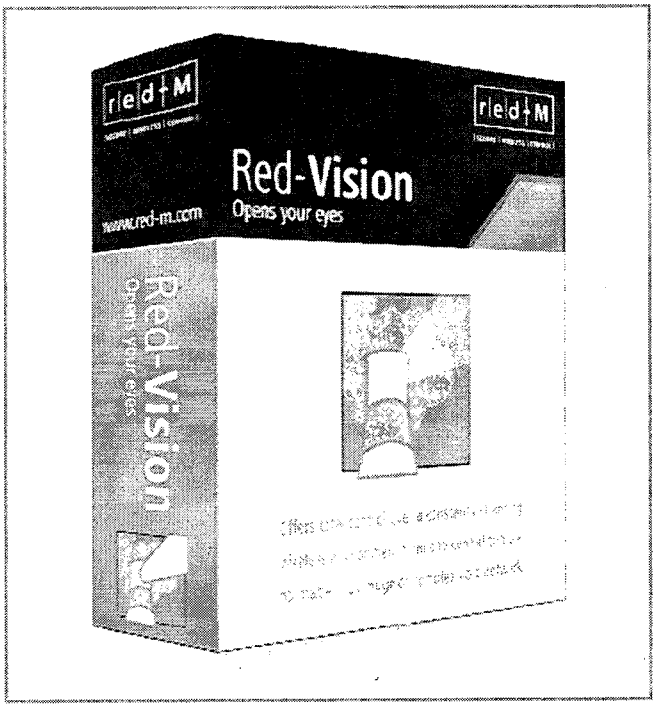
2.5 직관적인 중앙 관리 시스템

일단 적절한 IDS가 도입되고 나면 또 다른 보안 메커니즘과의 조합 유무와 상관없이 기업은 대부분 무선 기술의 활용을 확대하기 시작한다. 이러한 확장은 마침내 생산성 향성, 업무의 정확도 향상 및 총 설비비용과 지원비용을 감소시키는 등 약속된 투자대비 수익의 극대화 효과를 가져오게 된다.

그러나 이러한 이득이 있는 반면, 추가적인 무선의 의존도는 새로운 위험 요소들과 정보의 노출 등과 관련하여 전체 인프라 제어 레벨을 상승시켜야만 하는 결과를 가져오게 된다. 무선 기술은 전체 네트워크 환경을 2차원에서 3차원 공간으로 확장시키는 결과를 가져온다. 이러한 기하급수적인 복잡성의 수위 상승은 Red-M의 기업용 관리 프레임워크인 Red-Vision에 의하여 혁신적인 관리가 가능하며 Red-Vision은 네트워크 관리자로 하여금 기업 무선 네트워크의 총체적 제어를 효과적으로 지속할 수 있도록 한다. 이는 Red-Vision이 내부에 탑재된 보안 모듈과 일반 AP군 수용 관리 모듈을 통하여 제어 및 보안 관련 작업을 자동화하기에 기업은 실질적인 생산성 향상 및 업무효율 증대와, 안정되고 확장성을 지닌 무선 관리 프레임워크를 소유하게 된다. Red-Vision은 클라이언트 관리와 AP 관리, 무선 보안 관리 및 침입 탐지 기능들을 손쉽게 사용할 수 있는 단일 콘솔을 제공하는 통합 관리 플랫폼이라 하겠다. Red-Vision의 룰 기반 예외 관리 프로세스는 네트워크 운영자로 하여금 원하는 정책을 자유롭게 설정할 수 있게 하며 임계치를 벗어난 결정적인 이벤트에 대하여만 특히 집약된 주의를 기울일 수 있도록 하여 준다. 이러한 정보들은 네트워크가 구현된 사이트의 지도정보 인터페이스에 나타나게 되며, 이는 기업 내 문제의 요인 및 소재를 정확하고 쉽게 접근할 수 있는 장점이 있다 하겠다.



시스템의 주된 모듈은 윈도우 XP Professional 플랫폼 기반의 Red-Vision 서버와 뷰어, 그리고 윈도우 XP Professional 또는 Home 기반의 Red-Vision Labtop 클라이언트로 구성된다. Red-Vision 클라이언트는 상기에서 미리 언급한 5x5 레이어 모델의 첫 5개 레이어를 식별하고 예외에 대한 보고를 하게 된다. Red-Vision은 클라이언트에서의 무선 커뮤니케이션 auditing기능을 위한 모듈화 프레임워크로 이루어져 있으며, 이는 업체별로 고유한 보안 설정, 윈도우 98과 Pocket Window와 같은 추가적인 운영체제, 또는 PDA나 다른 컨버전스 디바이스를 지원하는 디바이스 플랫폼 등과 연계된다.



2.6 End-To-End 통합 솔루션

Red-M은 일반적인 틈새 솔루션이 아니라 새로운 무선 기술을 도입하고, 보다 적극적으로 활용하고자 하는 기업들에게 논리적인 네트워크의 성장 방향을 제시하는 솔루션이라 하겠다. 무선랜을 도입하기를 원하거나 무선랜 사용 불가를 못박는 기업 양쪽 모두에게 무선랜을 안전하게 시작할 수 있도록 하는 도구와 무선랜이 기업 통신의 주된 통신 수단이 될 가까운 미래에 꼭 필요한 시스템을 제공한다. 여기에서 키 포인트는 오픈 아키텍처의 적용이며 이는 Red-M 제품군 사이에서 데이터를 송수신할 때 사용하는 SNMP로부터 시작된다. SNMP는 Red-M 제품이 다른 계층의 네트워크 관리 시스템과 통합할 때 사용되는 수단이다. Red-M 제품군은 현재 데이터 교환에서 가장 널리 사용되고 있는 XML을 채택하여 snap-in 모듈 형태로 수용하도록 설계되어 있다.

Red-Detect와 Red-Vision은 모듈화된 아키텍처를 기반으로 유연하고 확장 가능하며 미래의 기술도 수용할 수 있게 설계되어 있다. 또한 장치의 인증 및 인가 등 접근제어를 위한 802.1x 표준이나 Wi-Fi Alliance의 Wi-Fi Protected Access (WPA) 암호화 방법 등 최근에 생겨난 보안과 무선 표준도 지속적으로 지원한다. Red-M 제품군은 이와 같은 표준을 엄격하게 지원하여 미래 기술에 대처하고 네트워크 상의 위험 요소들을 최소화 한다.

Red-Vision은 공중영역 관리 데이터를 그래픽 사용자 인터페이스로 불러올 수 있게 하는 Red-Detect 연결 모듈을 옵션으로 제공한다. 이 결합은 프로브와 협동하여 무선영역 내에 모든 장치를 감시할 수 있다.

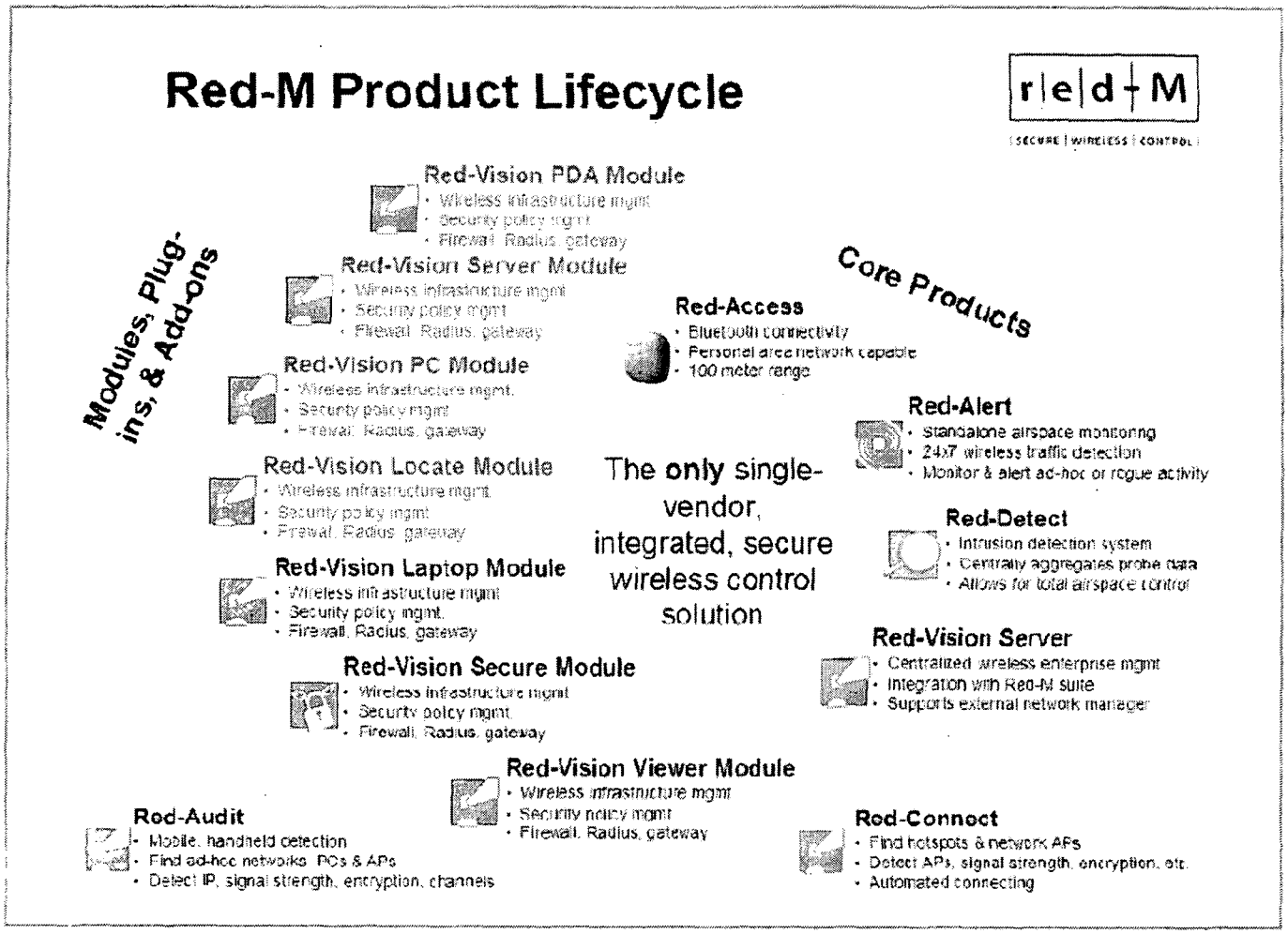
Red-Vision은 기본적인 시스템 요구사항이 있는 순수한 소프트웨어이다. Red-Vision 서버는 SNMP 서비스를 가동 중인 윈도우즈 서버가 필요하며 운영을 위해서는 최소한 2GHz 프로세서와 512MB 램, 1GB 하드디스크 용량을 필요로 한다. 또한 표준 HTML 인터페이스를 통해 현존하는 모든 기업형 AP를 지원하는 것도 커다란 특장점이라 할 수 있겠다.

3. 결 론

무선 기술은 오늘날의 IT 환경 속에 서는 휴대폰이나 PDA처럼 피하기 어려운 상황이 되었다. 이제 과연 무선 기술에 대해서 어떻게 할 것인가를 스스로에게 물어볼 시점이다. VPN만이 대답은 아니다. 무선 구간의 통신 활동을 무시한 유선 구간의 보안화 만이 대답이 아닌 것은 더욱 명백하다.

완전한 솔루션은 좋은 보안 수단과 안전한 보안 정책을 바탕으로, 무선구간인 공중영역의 완벽한 제어 및 감시를 위한 침입 탐지 프로브의 능동적인 메쉬 배치, 이벤트와 위협을 관리할 수 있는 중앙집중 시스템, 기업 네트워크에 접속하는 모든 인프라를 효율적으로 관리할 수 있는 직관적인 그래픽 사용 환경 등을 추가한 end-to-end 솔루션이어야 한다.

이러한 초기 단계들은 안전한 무선 제어의 바탕이 되며 Red-M은 필요하다면 오늘이라도 안전한 무선 제어를 제공할 수 있다. Red-M은 나쁜 의도의 사용자를 막을 뿐 아니라 올바른 사용자와 또한 나머지 일반 사용자를 아울러 관리할 수 있는 능력을 제공한다.


Red-M Product Lifecycle
r|e|d+M
SECURE | WIRELESS | CONTROL
Modules, Plug-ins, & Add-ons
Red-Vision PDA Module
• Wireless infrastructure mgmt
• Security policy mgmt
• Firewall, Radius, gateway
Red-Vision Server Module
• Wireless infrastructure mgmt
• Security policy mgmt
• Firewall, Radius, gateway
Red-Vision PC Module
• Wireless infrastructure mgmt
• Security policy mgmt
• Firewall, Radius, gateway
Red-Vision Locate Module
• Wireless infrastructure mgmt
• Security policy mgmt
• Firewall, Radius, gateway
Red-Vision Laptop Module
• Wireless infrastructure mgmt
• Security policy mgmt
• Firewall, Radius, gateway
Red-Vision Secure Module
• Wireless infrastructure mgmt
• Security policy mgmt
• Firewall, Radius, gateway
Red-Vision Viewer Module
• Wireless infrastructure mgmt
• Security policy mgmt
• Firewall, Radius, gateway
Red-Audit
• Mobile, handheld detection
• Find ad-hoc networks, PCs & APs
• Detect IP, signal strength, encryption, channels
Core Products
Red-Access
• Bluetooth connectivity
• Personal area network capable
• 100 meter range
Red-Alert
• Standalone airspace monitoring
• 24x7 wireless traffic detection
• Monitor & alert ad-hoc or rogue activity
Red-Detect
• Intrusion detection system
• Centrally aggregates probe data
• Allows for total airspace control
Red-Vision Server
• Centralized wireless enterprise mgmt
• Integration with Red-M suite
• Supports external network manager
Red-Connect
• Find hotspots & network APs
• Detect APs, signal strength, encryption, etc.
• Automated connecting
The only single-vendor, integrated, secure wireless control solution