

IDG Deep Dive

# 상존하는 위협, 준비되지 않은 “엔드포인트를 보호하라”

모든 사이버 공격은 최종 사용자들이 자신의 기기에서 악성링크 클릭, 악성코드 다운로드, 감염 파일 클릭, 즉 엔드포인트에서 시작한다. 기업 관리자들은 현재 보안 현실에서 무수히 많은 접점의 엔드포인트에 대한 공격을 100% 막을 수 없다. 문제는 보안 현실뿐만 아니라 의사결정권자에게도 있다. 한 설문조사에 따르면, IT 책임자 중 강력한 엔드포인트 보안을 구축했다는 응답은 32%에 불과했는데, 동시에 가장 취약한 공격 지점으로 엔드포인트를 지정한 비율이 73%였다. 위협은 상존하지만 제대로 대비가 되어있지 않은 것이다. 엔드포인트 보안 시장 및 기술 현황, 그리고 최적의 보안 대책을 알아본다.

## ※ Market Trends

커지는 위협에도 여전히 부족한 엔드포인트 보안  
엔드포인트 보안의 근원적 문제 “사이버 보안 전문가 부족”  
“통합 스위트 요구 증가!” 거대해질 엔드포인트 보안 시장

## ※ Tech Trends

“약이 아니라 독?” 기업 보안에 위협이 되는 안티바이러스 소프트웨어  
“예외없는” 보안 위협... 공격 행동별 비율은?

## ※ Solutions

정보 보안 프레임워크 구축을 위한 베스트 프랙티스  
“보안, 생산성, 비용” 세 마리 토끼를 잡는 Dell Data Protection



무단 전재 재배포 금지

본 PDF 문서는 IDG Korea의 프리미엄 회원에게 제공하는 문서로, 저작권법의 보호를 받습니다.  
IDG Korea의 허락 없이 PDF 문서를 온라인 사이트 등에 무단 게재, 전재하거나 유포할 수 없습니다.

IDG Deep Dive

# 상존하는 위협, 준비되지 않은 “엔드포인트를 보호하라”

모든 사이버 공격은 최종 사용자들이 자신의 기기에서 악성링크 클릭, 악성코드 다운로드, 감염 파일 클릭, 즉 엔드포인트에서 시작한다. 기업 관리자들은 현재 보안 현실에서 무수히 많은 접점의 엔드포인트에 대한 공격을 100% 막을 수 없다. 문제는 보안 현실뿐만 아니라 의사결정권자에게도 있다. 한 설문조사에 따르면, IT 책임자 중 강력한 엔드포인트 보안을 구축했다는 응답은 32%에 불과했는데, 동시에 가장 취약한 공격 지점으로 엔드포인트를 지정한 비율이 73%였다. 위협은 상존하지만 제대로 대비가 되어있지 않은 것이다. 엔드포인트 보안 시장 및 기술 현황, 그리고 최적의 보안 대책을 알아본다.

## ※ Market Trends

커지는 위협에도 여전히 부족한 엔드포인트 보안  
엔드포인트 보안의 근원적 문제 “사이버 보안 전문가 부족”  
“통합 스위트 요구 증가!” 거대해질 엔드포인트 보안 시장

## ※ Tech Trends

“약이 아니라 독?” 기업 보안에 위협이 되는 안티바이러스 소프트웨어  
“예외없는” 보안 위협... 공격 행동별 비율은?

## ※ Solutions

정보 보안 프레임워크 구축을 위한 베스트 프랙티스  
“보안, 생산성, 비용” 세 마리 토끼를 잡는 Dell Data Protection



무단 전재 재배포 금지

본 PDF 문서는 IDG Korea의 프리미엄 회원에게 제공하는 문서로, 저작권법의 보호를 받습니다.  
IDG Korea의 허락 없이 PDF 문서를 온라인 사이트 등에 무단 게재, 전재하거나 유포할 수 없습니다.

# 커지는 위협에도 여전히 부족한 엔드포인트 보안

David Geer | CSO

엔드포인트 보안 및 컴플라이언스 업체인 프로미섹(Promisec)은 현재 심각한 보안 공백과 취약점, 보안 침해에 대한 우려 증가에도 불구하고 엔드포인트 보안 솔루션이 부족한 상황이라고 지적했다.

프로미섹 데이터에 따르면 설문에 응답한 부사장 및 C레벨의 IT 리더 89%는 내년 보안 침해를 크게 우려한다고 답했지만, 강력한 엔드포인트 보안을 구축했다는 응답은 32%에 불과했다.

특히 응답자의 73%가 가장 취약한 공격 지점으로 엔드포인트를 지목했다는 사실은 우려를 더 증폭시킨다. 엔드포인트 보안에 대한 애널리스트의 시장 평가를 보면 이 분야에 대한 수요는 분명하다.

최근 마켓앤마켓(MarketsandMarkets) 보고서에 따르면 이 시장 가치는 올해 116억 2,000만 달러에서 2020년까지 173억 8,000만 달러 규모로 성장할 전망이다. 애널리스트 그룹 테크나비오(TechNavio)도 2014~2019년 사이 연평균성장률(CAGR)을 10.4%로 예상한다.

이런 수치에서 드러난 바와 같이 기업에는 엔드포인트를 보호하고 우려를 완화하기 위해 CSO가 따라야 할 가이드가 필요하다.

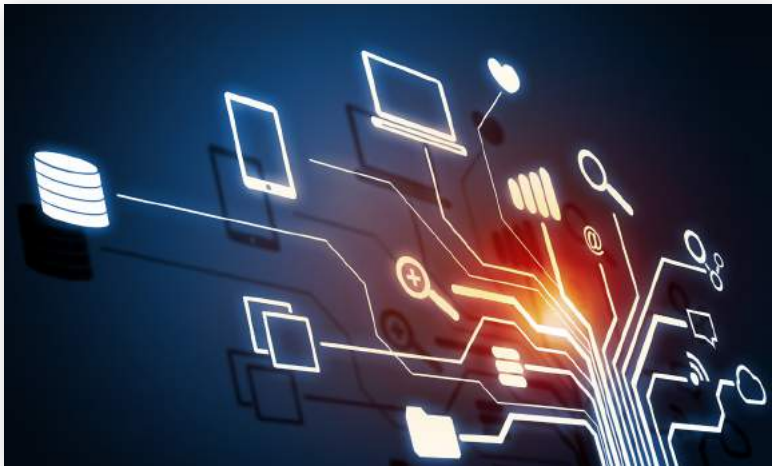
## 취약점의 근원

프로미섹 제품 관리 책임자인 스티브 로윅은 엔드포인트 보안 공백과 취약점의 원인으로 완전하고 정기적인 소프트웨어 패치의 부재, 애플리케이션 차단에서의 공백, 그리고 쉐도우 IT(shadow IT)의 지속적인 발생을 지적했다.

로윅은 “기업은 엔드포인트 시스템을 포함해 가장 위험성이 높은 시스템을 빈틈없이 패치하지 못하고 있다”고 말했다. 예를 들어 BYOD 환경에서 패치 적용 방법을 명확하게 규정하기는 어렵다. 로윅은 이러한 자산은 기업 네트워크에 머무는 시간이 충분하지 않아, 기업이 보안 수준에 완벽을 기할 수 있는 시간적인 틈을 확보할 수 없다고 설명했다.

이런 시간적인 틈 동안 기업은 NAC와 같은 도구를 사용해 안티바이러스, 안티악성코드와 같은 기기 기반 보안 애플리케이션을 업데이트하고 기기를 철저히 검사해 청소하기 전까지는 엔드포인트가 기업 네트워크에 접근할 수 없도록 차단할 수 있다. 보안 소프트웨어는 필요한 보호 계층 가운데 하나에 불과하다.

로윅은 “안티바이러스 등을 항상 최신 상태로 유지하는 것만으로는 엔드포인트를 적절



한 수준으로 보호할 수 없다”고 말했다.

애플리케이션 차단(Application blocking)의 경우 사용이 확산되고 있지만 이런 솔루션을 구축해도 여전히 공백은 존재한다. 사람들이 회사로 가져오거나 업무용으로 사용하는 인증되지 않은 BYOx(BYOA, BYOC를 포함한 Bring Your Own Everything)가 증가하고 있지만, IT 부서는 이를 지원하지 않거나 심지어 이런 기기의 존재조차 인식하지 못하는 상황이다. 즉, 웨도우 IT의 취약점이 커지고 있다.

엔드포인트 보호의 공백과 취약점은 직원이 사용하는 기기에만 국한된 이야기가 아니다. IoT는 기기의 리소스 측면에서 극히 취약하고 따라서 엔드포인트 보호도 가장 취약하다.

트렌드마이크로 사이버보안 전략 담당 부사장 에드 카브레라는 “IoT 기기는 성능이 낮아 전통적인 엔드포인트 보안 솔루션을 지원할 수 없다. 처리 성능과 스토리지, 메모리가 제한되므로 호스트 기반 침입 탐지와 차단 기능을 구현하기가 어렵다”고 말했다. IoT 기기가 지금과 같은 초소형 프로파일을 유지하는 한 이 부분이 앞으로의 과제가 될 것이다.

### 엔드포인트 보호와 우려 완화

기업은 패치의 베스트 프랙티스를 적용해야 한다. 이를 위해서는 패치 관리에 포함되는 모든 시스템을 위한 테스트 환경이 필요하다. 기업은 테스트를 거친 패치를 기기로 푸시하는 과정을 자동화하는 정책을 사용해야 하는데, 이 푸시는 테스트가 완료된 후 일주일 이내에 이루어져야 한다.

많이 사용되는 브라우저와 애플리케이션, 운영체제를 포함해 최대한 많은 시스템을 대상으로 패치 테스트와 적용을 수행해야 한다. 엔드포인트 패치 관리 솔루션을 제공하는 업체로는 루멘션(Lumension), IBM, 시만텍이 있다.

로윅은 “나이나이트(Ninite)와 같은 간단한 도구는 애플리케이션의 업데이트 필요에 따라 엔드포인트를 업데이트할 수 있게 해준다”고 말했다.

애플리케이션에 대한 통제력도 더 강화해야 한다. 모든 보안 도구가 그렇듯이 애플리케이션 제어 제품이 기본 상태에서 바로 각 기업의 엔드포인트 환경에 잘 맞을 가능성은 별로 없다. 관리자는 각 엔드포인트에 적용하면서 소프트웨어와 설정을 하나하나 살피고 구성해야 한다. 단순히 제품을 구입해서 네트워크에 던져 넣는다고 되는 것이 아니라는 점을 알아야 한다.

애플리케이션 통제를 현재 기기 환경에 맞게 조정하려면 각 엔드포인트의 고유한 요구사항을 처리하고 적절한 수준에서 기본적으로 애플리케이션을 거부하도록 블랙리스트/화이트리스트 도구를 구축해야 한다.

로윅에 따르면 기업은 파일, 레지스트리, 드라이버를 선제적으로 검증해 애플리케이션 통제를 보강해야 하며, 이를 위해 최신 위협 인텔리전스 서비스를 사용해 변화의 유형을

식별해야 한다.

엔드포인트에 필요한 기기 운영체제, 애플리케이션, 기기 정책과 통제를 포함하는 완전 무결한 백업 이미지를 유지하면 변화를 파악하기 위한 참조 지점을 확보할 수 있다.


애플리케이션 통제와 차단은 이 이미지와 라이브 엔드포인트의 콘텐츠를 비교하는 방법으로 모든 무단 변경을 탐지해 기기를 보호할 수 있다.

로잉은 최적의 통제와 공격 표면 감소를 위해서는 새 패치가 나오는 즉시 기업에서 이 기준 이미지를 적극적으로 업데이트해야 한다고 말했다. 애플리케이션 차단은 인증되지 않은 BYOx를 포함한 쉘도우 IT에 대처하는 데 도움이 된다.

IoT 기기가 엔드포인트 보안 기술의 기반 역할을 할 정도의 용량과 기타 리소스를 보유한 경우, 각 기기에 설치할 만한 IDS/IPS를 포함한 솔루션을 찾아야 한다. 네트워크 IDS/IPS와 완성도 높은 위협 인텔리전스 솔루션의 평판 데이터를 결합하면 IoT 기기를 장악하고자 하는 공격에 대처할 수 있다.

카브레라에 따르면, 예를 들어 첨단 위협 인텔리전스(advanced threat intelligence) 솔루션은 샌드박싱과 탐지 엔진을 사용해 네트워크 트래픽에서 바이러스, 악성코드, 명령 및 제어 서버와 전송을 비롯한 모든 위협의 징후를 탐지한다.

### 희망의 확대

사물 인터넷과 모빌리티 때문에 엔드포인트의 공격 표면은 갈수록 증가하고 있지만, 그렇다고 사물 인터넷과 모빌리티가 주는 혜택을 포기할 수는 없다. 기업은 지금 상황에 도움이 되는 기존 보안 수단을 최대한 활용해야 하며, 더욱 진보한 엔드포인트별 보안 솔루션을 생산하도록 업체들에게 요구해야 한다. 

# 엔드포인트 보안의 근원적 문제 “사이버 보안 전문가 부족”

Jon Oltsik | Networkworld

거의 모든 사이버 공격이 비슷한 패턴을 따른다. 최종 사용자가 악성 링크를 클릭하도록 현혹되거나 악성코드를 다운로드 하거나 감염된 파일을 열게 만든다. 이는 유명한 록히드 마틴의 “킬 체인”의 초기 단계 중 하나다.


이런 평범한 악성코드 워크플로우에서 엔드포인트 보안은 절대적인 핵심이다. 몇몇 엔드포인트가 침투 초기에 공격을 잡아내면 데이터 탈취 등 뒤이어 나타나는 최악의 상황을 피할 수 있다.

요즘의 엔드포인트 보안 요건을 충족하기 위해 안티바이러스 소프트웨어를 활용하거나 소프트웨어 취약점 패치를 통해 모든 공격을 차단할 수 있다고 가정하면 안 된다. 그보다는 엔드포인트 공격을 감지하고 대응하는데 능력 있는 현명한 보안 분석가가 필요하다.

안타깝게도 이 부분에서 기업 보안 모델에 문제가 생긴다. 이유는? 다시 말하지만 전 세계적인 사이버보안 전문가 부족 때문이다.

ESG 리서치에 의하면, 정도는 다르지만 기업의 43%가 엔드포인트 기술과 프로세스 지원능력을 갖춘 인재 부족을 겪고 있다. 하지만 엔드포인트 보안 전문가 부족만이 문제는 아니다. 최고 엔드포인트 보안 과제에 대해 물었을 때 기업 보안 담당자들의 38%는 기업의 엔드포인트 보안 담당자가 우선순위가 높은 문제들에 너무 많이 신경을 쓰고, 프로세스 향상과 전략 기획에는 충분히 시간을 쏟지 못한다고 이야기했다. 물론, 우선순위가 높은 문제 중 일부는 사건 감지와 대응과 관련되어 있지만, 보안 인력 전체의 효율성과 효과에 영향을 미치는 지속적인 대비 연습은 우선순위가 높은 일에 해당되지 않는다. 따라서, 엔드포인트 보안에 있어서는 많은 기업이 숙련된 전문가나 인력 부족을 겪고 있다고 볼 수 있다.

CISO가 채용으로 이 문제를 해결하기 힘들다면 다른 어떤 방법이 있을까? 단기 사이버 보안 능력 부족을 겪는 조직은 BT, Dell Secureworks, 유니시스, 버라이즌 같은 서비스 제공자들로부터 전문성과 직원 강화에 도움을 구할 수 있다. 또한 알고리즘과 인텔리전스를 네트워크와 엔드포인트 검색 데이터에 적용해 감지, 문제 파악, 개선 간소화를 가속시켜주는 보안 애널리틱스 도구를 찾아보는 것도 도움이 될 수 있다. 블루 코트, 시스코, 파이어아이, 헥시스, 사이버 솔루션, 팔로알토 네트워크, 레이션 사이버 프로텍츠, RSA 시큐리티 같은 업체들은 이 분야에 솔루션을 공급하고 있다.

CISO들은 사이버보안 전문가 부족의 영향을 그들이 내리는 모든 결정의 일부로 고려해야만 한다. 앞서 언급한 ESG의 연구 결과는 엔드포인트 보안에 있어서 이런 고려가 필요하다는 것을 증명한다. 

# “통합 스위트 요구 증가!”

## 거대해질 엔드포인트 보안 시장

Jon Oltsik | Networkworld

**과**거 대형 조직들은 단일 제품인 백신 소프트웨어에 엔드포인트 보안 예산의 대부분을 지출했다. 이 결정으로 인해 카스퍼스키 램, 맥아피(인텔 시큐리티), 소포스, 시만텍, 트렌드마이크로 등의 5개 업체가 수 십억 달러 규모의 시장을 지배하게 되었다.

2015년 현재까지 상황이 빠르게 변화하고 있다. 표적 공격과 정교한 악성코드로 인해 CISO들은 고급 악성코드 감지/방지, 엔드포인트 포렌식 수집/분석, 데이터 보안 등을 위한 추가적인 보안 도구로 안티바이러스를 보완하고 있다.

그렇다면 이제 엔드포인트 보안을 위해 여러 개의 제품을 사용해야 할까? 그렇다. 보안 전문가들은 그렇게 생각하고 있다. 최근 ESG는 직원 500~999명 사이의 중견 기업과 직원 1,000명 이상의 대기업에서 근무하는 340명의 보안 전문가들을 대상으로 설문조사를 실시하고 그들에게 엔드포인트 보안에 대한 여러 진술을 제시하고 각각에 대한 동의 여부를 질문했다. 결과는 다음과 같다.

- 보안 전문가 중 63%는 다음의 진술에 “매우 동의”하거나 “동의”했다 : 기업의 엔드포인트 보안 요건을 모두 충족시킬 수 있는 제품 스위트를 제공하는 엔드포인트 보안 업체는 존재하지 않는다.
- 보안 전문가 중 41%는 다음의 진술에 “매우 동의”하거나 “동의”했다 : 엔드포인트 보안에 필요한 특화된 제품/에이전트 수가 너무 많기 때문에 우리가 원하더라도 엔드포인트 보안은 불가능하다.



엔드포인트 보안을 위해서 여러 제품이 필요하다는 부분이 문제가 될까? 그렇다. 여러 제품을 사용하면 각 엔드포인트 시스템에 배치하고 유지해야 하는 에이전트 수가 늘어난다는 의미이다. 보안 직원은 각 제품에 대한 교육을 받고 엔드포인트 시스템을 구축하여 정책을 수립하고 엔드포인트 상태를 모니터링하며 문제를 해결해야 한다. 엔드포인트 보안 통제의 혼용으로 인해 사용자 생산성이 저하될 수 있으며, 이것이 정보 보안의 궁극적인 실수이다. 마지막으로 제품이 많아지면 엔드포인트 보안을 위한 솔루션 도입 및 운영 비용이 커진다.


물론, 여러 제품을 통한 엔드포인트 보안 비용 증가와 복잡성에 대한 대안이 있다. 단일 업체의 포괄적인 엔드포인트 보안 스위트를 이용하는 것이다. 대부분의 보안 전문가들은 이런 유형의 통합된 스위트가 현재는 존재하지 않는다고 보고 있지만, 솔루션이 개발되기를 바라고 있으며 그 가치를 명확히 인정하고 있다. 정보보안 전문가 중 58%는 단일 업체의 통합된 제품 스위트로 전략적인 엔드포인트 보안 요건을 해결하고 싶다고 말했다.

어떤 업체가 엔드포인트 보안 요건을 해소하고 이 유리한 시장 기회를 이용해 수익을 창출하는 통합된 엔드포인트 보안 스위트를 제공할 수 있을까? 필자는 다음과 같이 생각한다.

**1. 안티바이러스 전문 업체 :** 카스퍼스키, 맥아피, 소포스, 시만텍, 트렌드 마이크로는 이미 엔드포인트 보안 부문을 보유하고 있으며 추가적인 엔드포인트 보안 기능으로 자사의 안티바이러스 제품을 보완하기 위한 기술도 보유하고 있다. 점유율 싸움에서 이기기 위해 안티바이러스 기업들은 하드코어 보안 전문가들에게 자신들이 서명 기반의 방어책 이상을 제공하고 있음을 납득시켜야 한다. 하지만 “안티바이러스는 죽었다”는 오해가 꽤 널리 퍼져있는 상황에서 쉽지 않은 일이다. AVG, 맬웨어바이츠 (Malwarebytes), 위브루트(Webroot) 등의 새로운 안티바이러스 업체들에게 더욱 쉬울 수 있다.

**2. 신생기업 :** 지난 수년 동안 엔드포인트 보안이 미국 스타트업 시장의 중심이 되었다. 비트 9(Bit 9), 컨퍼(Confer), 크라우드스트라이크(CrowdStrike), 사이랜스(Cylance), 디지털 가디언(Digital Guardian), 태니움(Tanium), 트riumphant(Triumphant) 등의 신규 또는 기존 신생기업들은 완전한 엔드포인트 보안을 제공하려 하고 있다. 신생기업은 다른 위험이 있지만 위협 상황과 사이버 위험 해소에 대한 압박을 고려할 때 CISO들이 좀 더 개방된 마음가짐을 가질 수 있다.

**3. 핵심 기업 :** 많은 업체들이 다른 강력한 보안 솔루션 인지도를 이용해 엔드포인트 보안으로 전환할 수 있다고 믿고 있다. 시스코, 파이어아이, IBM, 팔로 알토는 엔드포인트 및 네트워크 보안을 연계하려 한다. 이는 기업 시장에서 점수를 따고 자사의 엔드포인트 보안을 더욱 광범위한 보안 분석 프로젝트의 일환으로 진행할 수 있는 좋은 생각이다. 이런 업체들은 보안을 이해하지만 성공을 위해 전통적인 조직 및 예산 장벽을 무너뜨려야 할 것이다.

**4. 와일드카드 :** 블루 코트, 체크 포인트, Dell, 포티넷, HP, 마이크로소프트 등의 업체들은 현 시점에서 엔드포인트 보안 스위트 시장에 발을 담고 있다. 이 기업들은 모두 엔드포인트 보안 협력 관계를 체결하거나 스타트업을 인수하여 제품 공백을 메울 수 있다. 



# “약이 아니라 독?” 기업 보안에 위협이 되는 안티바이러스 소프트웨어

Lucian Constantin | IDG News Service

**회**사 IT 부서에서 워크스테이션에 보안 침해사고가 발생, 하고 있는 일을 즉시 중단해야 한다는 전화를 받았다고 상상해보자. 아주 곤혹스러울 것이다. 회사에서 보안 교육을 받았고, 이메일의 악성 첨부 파일을 열어보지 않았고, 악성 링크를 클릭하지 않았다. 또 패치와 소프트웨어 업데이트를 충실하게 지켰다. 또 업무 시간 동안 업무와 상관없는 웹사이트를 방문하지도 않는다. 그런데 왜 이런 일이 일어났을까?

며칠 뒤, 회사가 보안 사고 조사를 의뢰한 보안 회사가 이에 대한 답을 내어놓았다. 그러나 예상하지 못한 답이었다. 해커가 기업을 보안 공격으로부터 보호해야 하는 안티바이러스 프로그램의 취약점을 악용해 침입한 것이다. 이런 공격에 필요한 유일한 도구는 사용자가 열어보지 않은 이메일 메시지 한 통이었다.

믿기지 않을지 모르겠지만, 현실적인 시나리오이다. 과거 안티바이러스 프로그램을 조사한 취약점 전문가들에 따르면, 이런 형태의 공격이 발생할 가능성이 높다. 아니 어찌면 이미 일어나고 있는지 모른다. 일부 전문가들은 몇 년 전부터 안티바이러스 제품의 취약점을 발견해 악용하기 쉽다고 경고해왔다.

전문가들은 6월 이후에도 카스퍼스키 랩, ESET, 어베스트, AVG 테크놀로지스, 맬웨어 바이츠 등 유명 안티바이러스 업체의 제품에서 수십 개의 중대한 취약점을 발견했다. 공격자가 원격으로 컴퓨터에 악성코드를 실행시키고, 안티바이러스 제품의 기능을 오작동시키고, 이를 통해 감염시킨 시스템의 고급 권한을 획득하고, 서드파티 애플리케이션의 취약점 방어 체계를 무력화할 수 있는 취약점들이다.

일부 취약점은 사용자 대화가 없어도 악용을 할 수 있으며, 자가 프로그래밍이 가능한 악성코드 프로그램인 컴퓨터 웜을 만들 수 있다. 많은 경우, 공격자들은 잠재적 피해자가 적법한 웹사이트를 방문했을 때 악성코드를 주입할 수 있게 제작한 이메일 메시지를 발송하거나, 악성 파일이 든 USB 드라이브를 컴퓨터에 연결하면 된다.

## 눈 앞의 안티바이러스 취약점 공격

기업 환경을 중심으로 안티바이러스 제품을 표적으로 삼는 공격이 발생할 것임을 보여주는 증거들이 있다. 일부 전문가들은 이미 이런 공격이 발생했다고 주장한다. 다만 피해자가 많지 않아 안티바이러스 업체들이 이를 인식하지 못하고 있을 뿐이다.

여러 정부의 정보기관들이 꽤 오랜 기간 안티바이러스 취약점에 관심을 기울여왔다. 뉴스 웹사이트인 인터셉트(The Intercept)가 6월 보도한 내용에 따르면, 영국의

GCHQ(Government Communications Headquarters)는 지난 2008년 카스퍼스키 랩의 안티바이러스 제품을 리버스엔지니어링해 취약점을 찾도록 허용하는 영장 갱신을 요청했다. NSA(National Security Agency)의 계약직 직원이었던 에드워드 스노든이 유출한 비밀 정보 파일에 따르면, NSA 또한 안티바이러스 감지를 회피하는 방법을 연구했었다.

특정 국가의 지원을 받는 것으로 의심되는 사이버스파이 집단인 카레토(Careto) 또한 카스퍼스키의 예전 안티바이러스 제품의 감지 능력을 회피할 목적에서 취약점을 조사해 악용한 것으로 알려졌다. 이 집단은 2014년 2월 스파이 활동이 노출되기 전까지 30여 정부의 수백 개 기관과 민간 기업의 컴퓨터를 침해했다.

감지를 피하기 위해 안티바이러스 취약점을 이용한 사례가 많지만, 안티바이러스 제품에 영향을 주는 원격 코드 실행 취약점 공격에 대한 수요도 있다. 규제되지 않는 취약점 공격 시장의 특수한 중개인들이 판매하고 있는 것들이다.

지난해, 이탈리아 감시 회사인 해킹 팀(Hacking Team)에서 유출된 이메일 중에는 벌너빌리티 브로커리지 인터내셔널(Vulnerabilities Brokerage International)이라는 집단이 취약점 공격을 판매했음을 시사하는 자료 하나가 있었다. 이 자료에는 여러 안티바이러스 제품의 다양한 권한상승 익스플로잇, 정보 공개, 감지 회피 익스플로잇에 대한 내용이 있었다. 또 ESET의 노드32 안티바이러스(NOD32 Antivirus)를 대상으로 한 원격 코드 실행 익스플로잇이 ‘판매됨’이라고 표기된 내용도 있었다.

현재 침입 감지 전문 업체 벡트라(Vectra)의 최고 보안 책임자로 일하고 있으며 과거 보안 연구 회사인 IO액티브(IOActive)의 최고 기술 책임자를 지낸 군터 올맨에 따르면, 안티바이러스 취약점 공격의 역사가 10년이 넘었다. 그는 이메일 인터뷰에서 고객의 요청을 받아 유명 데스크톱 안티바이러스 제품을 전문적으로 리버스엔지니어링 하는 회사들이 있다고 말했다. 이들은 기존 악성코드를 리버스엔지니어링하고, 이미 감염된 시스템을 하이재킹 하도록 만들 수 있다.

올맨에 따르면, 미국과 유럽의 정보기관들은 중국의 치후(Qihoo) 360 안티바이러스를 표적으로 하는 원격 취약점 공격에 수만 달러의 가치를 둔다. 일반적으로 국가 기관이 이런 활동을 하는 것이 알려지는 게 좋지 않기 때문에, 표적이 작고 주의 깊게 통제한다.

미국과 유럽의 정보기관들이 이런 종류의 익스플로잇에 관심이 있다면, 러시아와 중국 등 다른 사이버 강국도 마찬가지일 것으로 판단된다. 중국과 러시아의 사이버스파이 집단은 유명 애플리케이션의 알려진 취약점을 대상으로 한 익스플로잇을 개발하는 능력을 입증해왔다. 따라서 안티바이러스 제품을 표적으로도 충분히 능력을 발휘할 수 있다.

아직 직접 관찰된 적은 없지만, 안티바이러스 제품을 표적으로 한 공격이 가능하다고 인정한 안티바이러스 업체들도 있다.

카스퍼스키 랩의 안티악성코드 연구 책임자 비야체슬라프 자코제프스키는 “우리는 2016년 전망에서 보안 연구 회사와 보안 업체를 대상으로 한 공격이 미래의 트렌드로 부상할 수 있다고 내다봤다. 그러나 이런 공격이 보편화될 것으로 판단하지는 않는다. 예를 들어, 감염된 연구 도구로 보안 연구 회사를 공격할 수 있다. 또 모든 소프트웨어에 취약점이 있기 때문에 특정 표적을 대상으로 한 제한된 범위에서 보안 소프트웨어에 영향이 초래될 수 있다”고 말했다.

안티바이러스 업체인 비트디펜더(Bitdefender)는 엔드포인트 보안 프로그램을 표적으로 삼은 타깃 공격이 분명히 가능하지만, 소비자가 아닌 엔터프라이즈 환경에서 이런 일이 일어날 확률이 높다고 설명했다.

침투 테스트 전문가들은 안티바이러스 제품을 표적으로 삼은 취약점 공격이 가능하다는 사실을 오래 전부터 알고 있었다. 대형 기술 회사에서 일하고 있는 보안 연구원 한 명은 자신의 팀이 침투 테스트를 하면서 안티바이러스 관리 서버를 대상으로 취약점 공격을 시도한다고 말했다. 이런 서버들은 엔드포인트 시스템에 특수 권한을 갖고 있으며, 기업 네트워크에 수평적인 움직임에 이용할 수 있기 때문이다.

해킹 팀에서 유출된 벌너러빌리티 브로커리지 인터내셔널의 포트폴리오와 공개된 익스플로잇 데이터베이스에도 기업 안티바이러스 관리 서버를 표적으로 삼는 익스플로잇이 명단이 수록되어 있다.

안티바이러스 업체들은 소비자 제품에 이런 공격이 만연될 가능성은 크게 걱정하지 않고 있는 것으로 판단된다. 전문가들은 사이버범죄 집단이 플래시 플레이어, 자바, 실버라이트, 인터넷 익스플로러, 마이크로소프트 오피스 등 더 인기 있는 표적을 노리기 때문에 지금 당장은 이런 공격의 가능성이 낮다고 입을 모아 말했다.

그러나 이들 인기 애플리케이션 개발사가 최근 몇 년 동안 자신의 제품에 취약점 공격을 경감할 수 있는 방법을 점차 더 많이 도입하고 있는 추세이며, 보안이 강화된 새 버전으로 업데이트하는 사용자도 증가하고 있다. 즉 공격자들이 새로운 표적을 찾아 나서게 만들고 있다. 따라서 미래에는 수억 명의 소비자가 사용하는 안티바이러스 제품을 공격 대상에서 제외할 수 없다. 특히 사이버범죄자가 기존에 알려진, 이른바 제로데이 취약점을 파악하고 있는 경우가 그렇다.

지금 당장은 소비자보다는 기업이 안티바이러스 취약점을 약용한 공격 위협에 노출될 확률이 크다. 특히 사이버스파이 집단의 공격이 잦은 산업에서 직면하는 위험이 클 것이다.

### 너무 쉬운 안티바이러스 취약점 공격

안티바이러스 제품을 만드는 것은 사람이고, 사람은 실수를 한다. 따라서 버그가 전혀 없다고 가정하기 힘들다. 그러나 다른 종류의 소프트웨어보다 취약점의 수가 적고, 취약점 공격이 더 어렵다고 가정할 수 있다.

또, IT 보안 산업에 속한 회사들은 안전한 프로그래밍에 대한 가이드라인을 준수하고, 제품에 취약점 공격을 저지할 방어 체계를 도입하고, 주기적으로 코드를 감사하고, 취약점 테스트를 실시할 것이라고 가정할 수 있다. 그러나 불행히도 안티바이러스 산업에서 이런 조치들이 드문 것으로 보인다.

안티바이러스 프로그램은 웹과 이메일, 로컬 파일 시스템, 네트워크, USB 스토리지 장치 등 다양한 소스의 수 많은 데이터 및 파일을 조사할 수 있어야 한다. 또 다양한 보호 계층을 구현하는 수 많은 요소들을 보유하고 있어야 한다. 네트워크 트래픽을 가로채는 드라이버, 브라우저 및 이메일 클라이언트와 통합되는 플러그인, GUI(Graphic User Interface), 안티바이러스 엔진, 시그니처, 행동, 클라우드 기반 스캐닝을 지원하는 하위 시스템을 예로 들 수 있다.



보안 전문가들은 이를 두고 아주 큰 공격 표면이라고 표현한다. 공격자가 다양한 방법으로 악용할 취약한 코드가 많다는 의미이다. 더 나아가 안티바이러스 제품의 경우, 이들 코드 상당수가 최고 수준으로 실행될 가능성이 있다. 전문가들이 가능한 많이 피해야 한다고 주장하는 부분들이다.

구글의 보안 연구원인 타비스 오맨디는 지난 9월, 최근 몇 개월 동안 발견한 수 많은 안티바이러스 취약점 중 하나를 분석한 블로그 게시글에서 “안티바이러스 제품에는 타깃 공격에 대한 노출을 크게 높이고 쉽게 이용할 수 있는 공격 표면

이 있다”고 주장했다. 그는 “보안 제품 개발 업체들은 이런 점에서 보안 소프트웨어가 초래할 위험을 최소화하기 위해 가장 높은 수준의 기준을 적용할 책임이 있다”고 강조했다.

오맨디는 6월 이후 ESET, 카스퍼스키 랩, AVG, 어베스트 등 안티바이러스 제품에서 25개 이상의 취약점을 발견했다. 그는 과거 소포스 및 마이크로소프트 제품의 취약점을 발견했었다. 그가 발견한 취약점 가운데 상당수는 역사적으로 모든 종류의 애플리케이션에서 취약점의 근원이었던 파일 및 데이터 파싱에 뿌리를 두고 있다.

오맨디는 “우리는 미래에 시스템 권한으로 실행되지 않게 샌드박스 처리된 안티바이러스 압축해제기, 에뮬레이터, 파싱 도구를 보게 될 것이다. 오픈소스인 크로미움 샌드박스가 여러 중요 제품에서 사용된다. 네트워크 웜이 제품을 공격하고, 사용자를 표적으로 하는 공격을 받지 않도록 만들기 위해 지금 당장 샌드박스 기반의 개발 계획을 추가 수립해야 한다”고 강조했다.

오맨디 말고 다른 전문가들도 안티바이러스 제품 샌드박스 등 보안 경감책이 미흡하고, 시스템 권한에서 실행되는 요소가 너무 많다는 문제를 지적한다. 보안 연구원 작시언 코렛은 지난 2014년 로컬에서 원격으로 취약점 공격을 감행할 수 있는 14개 안티바이러스 제품과 엔진의 취약점을 밝혀냈다. 그의 주장도 오맨디와 같다.

코렛은 안티바이러스 산업이 권한 분리와 샌드박스 등의 기법을 도입해야 한다고 주장했다. 또 진짜 안전한 안티바이러스 제품이 필요하다고 강조했다. 이런 프로그램의 상당수가 중간자 공격에 취약하다. 커뮤니케이션에 SSL/TLS를 이용하지 않고, 다운로드 한 요소들에 서명을 적용하지 않는 사례가 많기 때문이다. 또 최신 브라우저에서 지원하는 취약점 공격 저지 도구를 도입해 이용하지 않으며, 실행 파일을 스캔하는 에뮬레이션을 이용하지 않고, 메모리 안전 언어를 사용하지 않는다.

더 큰 문제점도 있다. 보안 취약점을 제대로 검사하지 않는 안티바이러스 제품이 많다는 증거가 있는 것이다. 코렛은 ‘타비스 오맨디가 파악한 취약점을 살펴보면, 감사자가 첫 일주일 동안 취약점을 감지했다고 판단해 소프트웨어 감사를 전혀 하지 않고 있음을 알 수 있다’고 말했다.

취약점 인텔리전스 회사인 RBS(Risk Based Security)의 최고 연구 책임자 카스텐 에이

람은 안티바이러스 업체들이 최소한의 권한으로 제품을 실행시키고, 중요한 기능을 샌드박스 처리하고, 보안 코드를 철저히 하면서 안전하게 발전시켜야 한다고 강조했다.

RBS 자료에 따르면, 2010년 1월 이후 보안 소프트웨어와 기기에서 약 1,773개의 취약점이 발견됐다. 2015년만 372개이다. 절반 이상이 입력 조작을 통한 취약점 공격이다.

에이람은 “보안 업체들은 코딩에 있어 기준을 높여 유지해야 한다. 오랜 기간 잘 알려진 파싱 기능에서 수 많은 취약점이 발견되고 있다는 것이 당혹스러울 지경이다. 더 당혹스러운 문제도 있다. 파싱 기능에 시스템 권한이 필요하다는 것이다”고 지적했다.

안티바이러스 제품에 프로세스 샌드박스를 적용할 경우 성능이 저하된다고 생각하는 안티바이러스 업체가 많다. 일부는 권한 축소, 정기적인 보안 평가 수행, 샌드박스과 동일한 효과를 갖고 있는 다른 기술 개발 등 다른 방법을 이용해야 한다고 주장한다.

시만텍은 제품과 서비스의 공격 표면을 줄이는데 박차를 가하고 있다. 이 회사는 공격 성공 확률을 낮추기 위해 가능한 가장 낮은 권한으로 보안 구성요소를 작동시키는 방법을 추구하고 있다.

카스퍼스키 랩에 따르면, 효과적으로 취약점에 대처하는 것이 단 하나의 기술을 이용하는 것보다 복잡하다. 이 회사는 고객에게 최고 수준의 보안을 전달할 수 있다고 판단되는 기술을 구현하고 있다. 예를 들어, 획득한 수 많은 보안 정보와 지식을 활용하기 위해 머신러닝 알고리즘을 이용하고 있다. 카스퍼스키 랩의 자코제프스키는 “샌드박스 방식이 단순하지만, 성능과 효율성, 호환성에 영향을 주는 많은 중대 단점을 갖고 있다”고 지적했다.

인텔 시큐리티(맥아피)는 잠재적인 문제점을 파악하는 즉시 그 유효성, 속성, 심각성을 조사, 픽스를 개발한다고 설명했다.

안티바이러스 업체들이 발견한 취약점을 빨리 수정하지 않는다고 주장하는 사람은 없다. 일부 업체의 대응 시간은 아주 인상적이다. 또 자동으로 업데이트가 되게끔 기본값을 설정한 제품들이 많다. 문제는 이런 제품에 존재하는 취약점의 종류와 수이다.

안티바이러스 업체 비트디펜더는 구글이 제공하는 기술과 유사한 샌드박스가 보안 제품에는 효과적인 엔지니어링 솔루션이 되기 힘들다고 지적했다. 이 회사는 “안티악성코드 솔루션은 1초에 수만 시스템 이벤트를 가로채기 하고, 샌드박스 처리해야 한다. 이는 시스템 성능에 큰 영향을 준다. 운영체제 업체가 용인할 수 있는 정도를 넘어서는 영향이다”라고 설명했다.

이 회사는 안티악성코드 엔진과 ATC(Active Threat Controls) 등 로그인 사용자 권한에서 사용되는 요소들이 대부분이라고 주장했다. 또 시스템 권한에서 실행되는 요소의 수를 제한하기 위해 중개 프로세스를 이용하고 있으며, 이는 소비자 제품도 마찬가지라고 설명했다.

비즈니스 제품의 경우, 관리자가 엔드포인트가 아닌 네트워크의 여러 머신을 대상으로 스캐닝 서비스를 운영할 수 있는 그래비티 존(Gravity Zone)이라는 솔루션을 개발했다고 말했다. 또 최근에는 안티악성코드 솔루션을 운영 시스템 외부의 타입 1 하이퍼바이저에 완벽하게 분리 배치하는 HVMI(Hypervisor-based Memory Introspection) 기술을 도입했다고 덧붙였다. 이 회사는 “이는 안티악성코드를 사용자 환경에서 실행되는 루트킷, 익스플로잇과 분리하는 기술이다”고 설명했다.

안티바이러스 제품의 취약점 공격이 쉽고, 그 공격 표면이 넓다는 점과 타깃화된 공격의 발생 가능성이 높다는 점을 감안하면, 일부 기업 환경에 이런 프로그램을 설치할 가치 자체가 있는지 의문이 제기된다.

일부 전문가는 사이버스파이 집단 등이 사용하는 정교하게 개발된 악성코드 프로그램의 경우, 엔드포인트 안티바이러스 제품의 효과성을 의심하고 있다. 위협 대비 보상이 거의 없다고 판단하는 것이다. 특히 이런 공격에서 자주 표적이 되는 산업이 그렇다.

코렛은 “소규모 사업체와 일반 사용자들의 보호 도구로만 적합한 것이 안티바이러스 제품이라고 생각한다”고 말했다. 코렛의 설명에 따르면, 안티바이러스는 광고와 달리 알려지지 않은 위협은 감지하지 못한다. 또, 안티바이러스의 감지를 회피하는 것이 어렵지 않다. 대부분의 악성코드 개발자는 악성코드 개발에 앞서 이를 테스트한다.

오랜 기간 엔드포인트 안티바이러스 제품을 비판해온 올맨은 운영체제에 보안 기능이 탑재되는 사례가 증가하면서 안티바이러스 프로그램이 점차 쓸모 없게 될 것이라고 내다봤다.

현재 일부 안티바이러스 업체들은 자신의 제품이 제 기능을 하도록 만들기 위해 운영체제에 탑재된 보안 메커니즘을 손상시켜야 한다. 그런데 이는 시스템 감염 위험을 높인다.

최근 이스라엘의 데이터 침입 방지 기술 개발사인 엔사일로(enSilo)는 카스퍼스키 랩, AVG에 다른 애플리케이션을 위해 운영체제에 탑재된 취약점 방어 기술을 무력화시키는 취약점이 있다고 공개했다.

엔사일로 연구원들이 블로그 게시글에 공개한 내용에 따르면, 이들 안티바이러스 제품은 읽기, 쓰기, 실행 권한 메모리 페이지를 어도비 리더와 웹 브라우저 등 다른 애플리케이션에 귀속된 사용자 모드 프로세스에 할당하는 문제점이 있다. 이는 공격자가 윈도우에서 드파티 애플리케이션용으로 탑재된 ASLR(Address Space Layout Randomization) 및 DEP(Data Execution Prevention) 등 취약점 경감 도구를 회피, 더 손쉽게 취약점을 악용할 수 있도록 만든다.

에리암은 안티바이러스 제품에 존재 가치가 있다고 말했다. 그는 가정과 기업 환경의 많은 사용자들이 각자의 행동, 즉 위험한 소프트웨어를 다운로드 받거나, 악성 링크를 클릭하는 행동에서 스스로를 보호할 필요가 있다고 말했다.

그리고 엔드포인트 안티바이러스 프로그램은 이와 관련된 위협을 줄이는데 도움을 준다. 그러나 이런 장점이 안티바이러스 제품을 표적으로 삼는 공격 위험을 상쇄할 정도일까? 이는 위협이 발생하는 형태, 설치한 안티바이러스 제품의 보안이 좌우할 문제이다.

사용자는 자신의 환경에 적합한 보안 소프트웨어, 정말 필요한 기능과 특징을 주의 깊게 검토해야 한다. 안티바이러스 구매자는 업체의 보안과 관련된 평판, 제품에 영향을 초래하는 취약점에 대처하는 속도, 취약점의 종류와 중대성을 점검해야 한다. 에리암은 “더 전해질 수 있다는 생각에서 무조건 보안 소프트웨어를 설치해서는 안 된다. 이는 좋은 방법이 아니다”고 말했다.


자코제프스키는 “우리는 악성코드의 발전 속도를 과소 평가하지 않는다. 그러나 이와 동시에 안티바이러스 제품이 효과적이지 않다는 주장에도 동의하지 않는다. 기업을 표적으로 삼는 정교한 위협과 공격을 감지할 종합적인 전략을 개발할 능력을 갖추기 전에 일반 악

성코드를 걸러 차단해야 한다”고 강조했다.

그는 기업과 개인 데이터 침해 위협과 위험을 줄이는 유일한 방법은 전통적인 안티바이러스 소프트웨어, 차세대 보호 도구, 정보 공유, 보안 서비스, IT 직종 종사자 교육, 정기적인 소프트웨어, 하드웨어, 애플리케이션 평가 등을 결합한 다계층 전략을 수립해 실천하는 것이라고 말했다.

비트디펜더는 안티바이러스 제품이 악성코드를 놓치는 사례가 있다고 인정했다. 그러나 이런 경우는 극히 예외라는 점을 강조했다. “결론적으로 안티바이러스는 기회를 노리는 공격을 필터링 하는 것이다. 이는 알려진 취약점, 악성코드에 기반을 두고 있다. 이런 안티악성코드 솔루션을 보안 인식 제고 프로그램 등으로 보완하는 방법을 사용해야 한다”고 말했다.

위험이 아주 높은 환경에서 안티바이러스 프로그램을 보완하거나, 대체할 수 있는 기술 중 하나는 사전에 승인한 애플리케이션만 실행을 허용하는 애플리케이션 화이트리스트 기술이다. 미국 NIST(National Institute of Standards and Technology)는 일부 운영체제에 기본 탑재된 화이트리스트 보호 메커니즘을 사용할 것을 장려하고 있다. 또 최근에는 이에 관한 권장 가이드를 발표하기도 했다.

기업 환경을 데이터 유출 등 내부와 외부의 위협에서 방어하는데 중요한 역할을 하는 또 다른 보호 수단은 네트워크 경계선 방어이다. 그러나 네트워크 수준의 보안 어플라이언스에도 취약점이 있을 수 있다는 점에 유념해야 한다. 실제 보안 전문가들은 이들 제품에서 수 많은 취약점을 발견했으며, 암시장에서 이런 취약점이 판매되고 있는 실정이다. 



## IT 트렌드 종합 정보센터

# IDG Tech Library

IDG Tech Library는 IDG 글로벌 네트워크를 통해 축적된 전문 정보를 재구성하여 최신 기술의 기본 개념부터 현황, 전략 및 도입 가이드까지 다양한 프리미엄 IT 정보를 제공합니다. Computer World, Info World, CIO, Network World 등의 세계적 IT 유명 매체의 심도 깊은 정보를 무료로 만나보세요

IDG Deep Dive, Tech Focus, Summary, World Update 등의 다양한 콘텐츠를 제공 받을 수 있습니다.



한국IDG(주) 서울시 중구 봉래동 1가 108번지 창화빌딩 4층 100-161 Tel : 02-558-6950 Fax : 02-558-6955  
[www.itworld.co.kr](http://www.itworld.co.kr)   [www.twitter.com/ITWorldKR](https://www.twitter.com/ITWorldKR)   [www.facebook.com/ITworld.Korea](https://www.facebook.com/ITworld.Korea)

# “예외없는” 보안 위협... 공격 형태별 비율은?

Maria Korolov | CSO

**최** 근 40개 기업의 25만 개 엔드포인트 기기를 분석한 결과, 모든 기업 네트워크에서 침투 증거가 발견되었다. 공격의 가장 위험한 단계인 ‘데이터 유출’까지 이른 것은 드물었지만, 완전히 안심할 순 없다는 것이 이번 조사를 진행한 벡트라 네트워크(Vectra Networks)의 의견이다.

네트워크 모니터링 기술 제공업체인 벡트라는 이번 보고서를 통해 모든 기업의 네트워크에는 주변 방어를 염탐하는 일종의 위협이 있다고 밝히고, 각 위협들의 비율과 공격 형태를 공유했다.

위협의 32%를 차지하는 첫 번째 단계는 ‘지휘 통제’다. 공격자들이 진입로를 마련하고 감염 경로 확보 결과를 알린다. 이런 활동이 모두 자동화된 것은 아니다. 벡트라 네트워크의 제품 마케팅 디렉터 웨이드 윌리엄슨은 “대부분의 경우 네트워크에 더 깊이 파고들어 갈수록 키보드를 손으로 입력할 필요가 있다. 아마도 어떤 사용자 자격을 획득해서 이 시스템 혹은 저 시스템에 로그인할 수 있을 것이다. 공격을 지휘하는 것”이라고 설명했다.

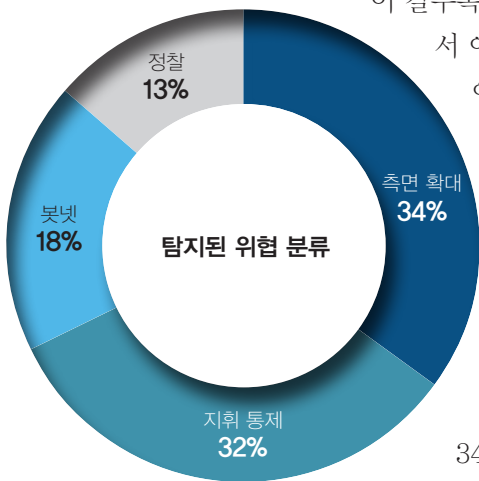
이 시점 후 공격은 두 가지 다른 방향으로 뻗어나갈 수 있다. 하나는 ‘봇넷’이다. 벡트라에 따르면, 활동중인 확인된 위협 가운데 18%가 봇넷 기반의 형태다. 봇넷 기반의 위협 가운데 클릭 사기(click fraud)가 85%로 압도적으로 많으며, 무차별 대입(brute-force) 공격이 5%, 서비스 거부(denial-of-service) 공격이 4%로 나타났다.

공격의 다른 경로는 기업 내부로 더욱 들어가는 것이다. 이 공격의 다음 단계는 ‘정찰(reconnaissance)’로 위협 활동의 13%를 차지한다. 이 다음은 34%를 차지하는 측면 확대(lateral movement)다. 측면 확대의 56%는 무차별 대입 공격이며, 22%는 자동화 응답, 그리고 탈취된 자격(credential)과 계정을 활용한 커베로스(Kerberos) 공격이 측면 확대 활동의 16%를 차지한다.

봇넷 관련 위협의 수는 분석된 네트워크의 증가와 같은 비율로 증가한 반면, 정찰 활동의 성장세는 거의 4배 높았고, 측면 확대는 거의 7배 높았다.

마지막 단계는 ‘데이터 유출(data exfiltration)’로 기업에게는 가장 위험하지만 확인된 위협의 단 3%만 차지한다. 이는 기업이 피해를 입기 전 이런 공격들을 감지하고 파악할 기회가 있다는 의미다. 그러나 동시에 공격자들이 적발되기 전까지 기업 네트워크 내에서 몇 달씩 시간을 보낼 수 있는 이유도 설명해준다.

윌리엄슨은 단 3%의 공격만 데이터 유출 단계에 있다고 해서 이 단계에 머무르는 시간이 이만큼 짧은 것은 아니라고 경고했다. 그는 “한번 유출 채널을 만들어두면 오랫동안 데



출처 : Vectra Networks



이터를 훔칠 수 있도록 열어둘 수도 있다”고 설명했다.

### 공격자가 숨는 기법

벡트라는 공격자들이 숨어있는 방식도 분석했다. 공격자들이 그들의 커뮤니케이션을 숨기는데 가장 흔하게 사용한 기법은 가짜 브라우저 활동으로 36%를 차지했고, 새로 생성된 도메인은 25% 경우에 쓰였다. 익명 토르(TOR) 네트워크는 14%에서 쓰였고, 13%의 외부 원격 접속이 뒤를 이었다.


가장 드물게 쓰인 기법들로는 풀링 인스트럭션(pulling instructions), 스텔스 HTTP 포스트, 히든 HTTPS 터널, 악성코드 업데이트, P2P 네트워크, 히든 HTTP 터널 등이 있었다.

히든 터널은 공격자들이 텍스트필드, 헤더, 혹은 보통 트래픽의 기타 세션 파라미터 속에 코딩된 메시지를 임베드 할 수 있으므로 특히 감지하기 어렵다. 게다가 공격자들이 암호화된 트래픽을 활용하게 되면 감지는 더욱 어려워진다.

벡트라는 행동 분석을 통해 숨겨진 터널을 찾아냈는데, 조사 결과 공격자들은 암호화된 채널을 하이재킹하는 것을 선호하는 것으로 나타났다. 예를 들어 암호화된 HTTPS 커뮤니케이션은 비암호화된 HTTP 지휘와 통제 커뮤니케이션에 비해 두 배 이상 선호되었다.

이번 보고서에서 최고의 뉴스는 유출에 관련된 위협의 비율 즉 3%가 작년에 비해 절반으로 줄어들었다는 점이다. 하지만 이는 벡트라 고객들이 공격이 실제 감행되기 전에 이를 차단하기 위해 그들의 네트워크 분석을 활용했기 때문일 수 있다.

윌리엄슨은 “고객들은 업스트림 보안을 지나가는 위협을 감지 식별하기 위해 벡트라 솔루션을 활용한다. 이 정보를 가지고 위협 대응에 활용할 것이다”고 설명했다.

한편, 이번 조사는 1,000명 이하의 중형급 기업부터 5만 명 이상의 대기업을 모두 대상으로 했다. 분석 대상 기업의 수는 이전 보고서의 2배인데, 기존 벡트라 솔루션 사용자뿐만 아니라, 이런 유형의 스캔 솔루션을 처음 도입할 잠재 고객까지 포함되었다. 

# 정보 보안 프레임워크 구축을 위한 베스트 프랙티스

Michelle Drolet | Networkworld

**사**이버 공격으로 인한 기업 비용이 연간 4,000~5,000억 달러에 달하고 있다. 사이버 보안은 그 어느 때보다도 높은 관심을 받고 있다. M&M(Markets and Markets)은 사이버 보안 시장이 올해 1,060억 달러에서 2020년에는 1,700억 달러 규모로 성장할 것으로 전망했다. 개선, 미준수 벌금, 브랜드 이미지 피해 등을 고려했을 때 데이터 유출의 평균 비용은 정확하게 계산하긴 어렵지만, 매우 높으며 계속 증가하고 있다.

허트블리드(Heartbleed) 취약성은 2014년에 발생한 비극적인 보안 버그로 그 영향이 광범위했다. 기업들이 보안 서비스와 플랫폼에 더 많은 돈을 쏟아 붓고 있지만, 많은 서버에서 여전히 익스플로잇 공격이 발생하고 있다. IoT로 인해 새로운 위협이 발생하면서 기업 내 대응이 복합적으로 나타나고 있다. 일부 영역에서의 ‘훌륭한 프랙티스(good practice)’가 다른 영역에서는 그렇지 않을 수도 있다.

## 탄탄한 기반 구축

모래 위에 지은 집이 오래 지속되지 않는 것과 마찬가지로 탄탄한 기초가 없는 정보 보안 전략은 쏟아 붓는 돈의 액수에 상관없이 실패하게 될 것이다. 우리는 소프트웨어 취약성 증가, 악성코드 및 랜섬웨어의 등장, 위협 간과의 위협에 관해 많은 이야기를 듣고 있지만 대체 무엇을 해야 할까?

정보 보안 프레임워크를 구축하기 위해서는 우선 CIS(Center for Internet Security)의 CSC(Critical Security Control)을 활용하는 것이 좋다. 이 베스트 프랙티스는 정부와 사법 기관이 마련한 것으로 사이버 방어를 강화하기 위한 실행 가능한 방법에 초점을 맞추고 있다.

베스트 프랙티스에 나열된 20가지 조치 중 아무것이나 선택해도 보안 상태에 긍정적인 영향을 끼치지만, 전체 범위를 포괄하는 것이 현명하다 할 수 있다. 이것들은 단순하고 상식적인 규칙이지만 이것들이 얼마나 간과되고 있는지 알게 된다면 놀라게 될 것이다. 먼저 도입부를 살펴보자.

### 1. 승인 및 미승인 기기 인벤토리

양호한 보안 기반을 구축하는 것의 핵심은 적절한 질문을 던지고 자신의 지식 공백을 확인하는 것이다. 이 첫 번째 통제는 분명 보안에 근본적이지만 많은 조직들이 다음과 같은 질문에 답하기 위해 몸부림칠 것이다.

- 총 몇 대의 서버를 보유하고 있는가?
- 네트워크에 연결된 장치는 총 몇 대인가?
- 방화벽, 스위치, 라우터는 어떠한가?
- 네트워크에 접근하는 것을 통제할 수 있는가?

자신이 보유하고 있는 하드웨어에 대해 정확히 모르는 상태에서 완전한 지도를 갖거나 잠재적인 취약성을 표시할 방법은 없다. 최신의 포괄적인 하드웨어 인벤토리는 필수적이다.

## 2. 승인 및 미승인 소프트웨어 인벤토리

첫 번째 통제와 함께 취하고 사용 중인 모든 시스템과 장치를 아우르는 승인된 소프트웨어 목록을 작성해야 한다. 실시간으로 소프트웨어를 모니터링하여 버전을 검증하고 승인되지 않은 앱을 차단하거나 최소한 표시할 수 있어야 한다.

취약성과 익스플로잇 공격을 시의 적절하게 처리하기 위해 어떤 운영 체제와 소프트웨어 버전을 사용하고 있는지 파악하고 발생하는 새로운 위협에 기초하여 필요한 업데이트를 표시할 수 있는 시스템을 보유해야 한다.

알고 있겠지만 정확한 하드웨어 및 소프트웨어 인벤토리를 구축하는 것이 어려울 수 있다. 로마는 하루아침에 건설되지 않았고 좋은 정보 보안 프레임워크를 구축하기 위해서도 시간과 자원이 소요된다는 사실을 알게 될 것이다. 중요한 것은 전체적인 관점에서 계획을 세우는 것이다. CSC에서 개요한 단계를 따라 시작하고 각 단계를 밟을 때마다 방어력이 강화될 것이다.

팀을 훈련하거나 새로운 CISO를 고용하거나 보안 컨설팅 서비스를 구매하는지 여부에 상관없이 이 목록을 통해 자신의 노력을 비교 측정할 수 있는 탄탄한 프레임워크를 갖출 수 있다. 매우 유용하고 실행 가능한 기준이며 개별적인 보안을 개선할 뿐 아니라 전체적인 온라인 보안을 강화할 수 있다. 모든 기업은 이를 탄탄한 보안 기초를 구축하기 위한 시작점으로 삼아야 한다.

## 실시간 취약점, 권한, 로그 모니터링

이제 지속적으로 취약점들을 처리 해결하는 중요성, 운영 권한의 치밀한 제어 유지의 중요성, 감사 로그 모니터링의 중요성에 대해 살펴보자. 이런 개념들은 CSC 4, 5, 6에 압축되어 있다.

엄중한 정책을 개발하고 자원을 적절히 순환시키고 직원들을 교육시키기 위해 자원을 충당하는 것을 고려하고, 지속적으로 그들의 효과를 측정해 필요한 변화를 취해야 한다.

## 4. 지속적인 취약점 평가와 개선

새로운 취약점들이 매일 등장한다. 만약 이런 취약점을 지속적으로 스캔 하지 않으면 사이버범죄자들이 이득을 취할 수 있게 된다. 보안을 갖춰두면 담당자는 실 수 있다는 생각은 위험하다. 취약점 식별만으로는 부족하고 담당자 역시 행동을 취해야 한다.

만약 담당자가 취약점을 찾고 제대로 처리하지 않으면 공격자들에게는 아주 손쉬운 공

격 대상이 되는 것이다.

기업이 취약점을 해결하는데 평균적으로 176일이 소요되었지만 사이버 범죄자들은 이를 공략하는데 평균 7일이 걸린다고 노섹(NopSec)의 2015년 취약점 리스크 관리 현황 보고서(State of Vulnerability Risk Management)에서는 밝히고 있다. 취약점을 뿌리 뽑고 이를 능동적으로 해결하는 게 중요하고 그렇지 못하면 침투 당하게 될 것이다.

다음은 고려해보자.

- 인텔리전스 업데이트를 갖춘 자동화된 실시간 취약점 스캐닝
- 모든 소프트웨어의 자동화된 패치 관리
- 취약점이 패치 되었는지 확인하기 위한 결과 비교

테스트 환경 속에서 패치 평가를 통해 비즈니스 기능에 악영향이 없음을 확인하는 것도 고려해야 할 것이다. 몇몇 사례에서는 취약점에 대처하기 위한 대안적 대책이 필수적일 수 있다. 또한 가장 위험한 취약점에 대해 패치를 우선화하고 혼돈을 최소화하기 위해 패치를 순차적으로 적용하는 것도 좋은 생각이다.

## 5. 운영 권한의 통제된 활용

직원이 방어 체계에서 가장 약한 부분이 되는 경우가 흔하다. 버라이즌의 2015년 데이터 유출 조사 보고서(Data breach Investigation Report)에서는 사이버 스파이 사건의 2/3 이상이 피싱으로 인해 일어난 것으로 나타났다. 사이버 범죄자들에게는 암호를 해킹하거나 직원들이 자신도 모르는 사이 악성코드를 다운로드 하도록 운영 권한을 쓰게 하는 게 훨씬 쉽다. 제대로 된 도구로 내부자 공격을 차단할 수 있지만 일반적인 정책을 강화하는 게 효과가 있다.

- 운영 권한 최소화
- 계정들을 인증하고 권한이 확실히 인가된 것인지 확인하기
- 복잡한 암호와 암호화 강제화
- 새로운 계정과 로그인 시도 경보

운영 권한에 대해 밀접한 제어를 유지하면 데이터 유출 리스크를 큰 폭으로 줄일 수 있다.

## 6. 유지관리, 모니터링, 감사 로그 분석

만약 감사 로그 시스템을 유지하지 않으면 공격 당한지도 파악하기 힘들어질 수 있다. 2015 트러스트웨이브 글로벌 보안 보고서(Trustwave Global Security Report)에 의하면 2014년 데이터 유출의 단 19%만 피해 조직에 의해 감지되었다고 한다. 회사들이 로그를 수집하는 것은 드문 것은 아니지만 확인하지 않고 유출을 몇 달간 감지하지 못하는 일은 발생한다. 많은 회사들은 모든 준수 사항을 지키기 위해 기록을 유지하지만, 이를 모니터링하고 전체적으로 분석하지 않는다면 제대로 활용하지 못하는 셈이다.

- 지속적인 타임스탬프를 위해 최소한 두 개의 동기화 시간 소스가 필요하다.
- 감사 로그는 표준화된 포맷으로 인증 기록되어야 한다.
- 스토리지 공간을 갖추고 상당 기간 동안의 로그를 보유 유지하라.
- 공격자들의 로그 조작을 방지하기 위해 별도의 로깅 서버 활용을 고려하라.
- 로그를 정기적으로 수집, 집계, 분석하라.

적절한 분석은 공격을 감지, 이해, 복구하는데 도움을 줄 것이다.

취약점, 권한, 로그를 실시간으로 모니터링할 때 필요한 데이터를 수집하고 잠재적 문제를 끄집어내기 위해 자동화된 소프트웨어 시스템에 의존하는 경우가 있을 것이다. 그 시스템의 효과를 정기적으로 테스트해야 한다. 가상 공격은 약점을 식별하고 방어 체계의 결점을 찾는 데 도움이 될 수 있다.

시간이 생명이다. 취약점을 더 빨리 해결하고 수상한 행동을 더 빨리 식별하고 공격을 드러낼수록 더 좋다. 성과에 대한 벤치마크를 설정하고 측정 단위를 수립해서 보안 성과가 기대치를 실제로 충족시키고 있는지 확인할 수 있다. 그 성과를 향상시키기 위해 지속적으로 작업하면 잠재적 공격자들의 침투를 훨씬 어렵게 만들 수 있을 것이다.

### 악성코드 방어선 구축

이메일 프로그램과 웹 브라우저는 여전히 공격자들의 가장 흔한 공격점인데, 너무 많은 회사들이 안타까울 정도로 부적절한 악성코드 방비를 갖추고 있으며, 포트 제어와 서비스 제한 실패는 마치 사이버 범죄자들에게 들어오라고 문을 열어주는 것과도 같다.

### 7. 이메일과 웹 브라우저 보호

인간 행동은 여전히 사이버 범죄자들에게는 가장 저항이 적은 경로이고 이들은 종종 시스템에 접속하기 위해 소셜 엔지니어링 기법을 사용한다. 버라이즌의 2015 데이터 유출 조사 보고서(Data Breach Investigations Report)에 따르면, 피싱의 증가에도 불구하고 수신자의 23%는 피싱 메시지를 열어보고 11%는 첨부물을 클릭한다. 의심스러운 첨부물, 수상한 웹사이트, 취약한 플러그인들은 모두 공격자들의 침투에 사용될 수 있다.

웹브라우저와 이메일 프로그램을 모두 최신으로 유지하는 게 중요하다. 직원들이 지원되지 않는 브라우저나 이메일 프로그램을 사용하지 않도록 하고 이들이 불필요한 플러그인과 애드온을 설치하지 못하게 한다. 모든 URL 요청은 로그 되어야 하고 인증되지 않은 웹사이트로의 접속을 차단하는 필터를 갖춰야 한다. 모든 이메일 첨부물은 사업에 불필요한 경우 스캔하고 차단되어야 한다.

웹 브라우저와 이메일에 대해 강력하게 통제하는 것은 피싱의 위협을 줄일 뿐 아니라 스팸을 줄이고 시간 낭비 방지에도 도움이 된다.



### 8. 악성코드 방어

비라이즌의 2015 데이터 유출 조사보고서에 의하면 매초마다 5건의 악성코드 사건이 발생하고 있으며 악성코드는 이메일, 클라우드 서비스, 웹페이지, 스마트폰, 심지어 USB 드라이브 등 모든 종류의 소스로부터 기업의 시스템에 들어올 수 있다.

진입 시점에 감지하는 게 항상 가능하진 않겠지만 제대로 된 방어를 쳐놓음으로써 피해가 너무 커지기 전에 감지하고 막을 수 있다.

실시간 모니터링과 위협 산정을 위한 자동화된 도구 채용은 의무화 되어야 한다. 기업 시스템 전반에 악성코드 방어를 배치시킬 필요가 있다. 안타깝게도 포네몬 인스티튜트(Ponemon Institute) 보고서에서는 응답자의 겨우 41%만이 인텔리전스를 캡처하고 악성코드의 진정한 위협을 평가하는 자동화된 도구가 있었던 것으로 나왔다. 반면 자동화된 도구가 있는 조직들은 인간의 개입 없이도 악성코드 감염의 60%를 처리할 수 있어서 많은 시간과 자원을 절약했다고 한다.

외부 기기의 활용을 제한하고 트래픽 흐름에서 악성 콘텐츠를 집어내고 보안 시스템이 자동화되도록 업데이트 해주는 네트워크 기반의 안티악성코드 도구를 활용하는 것이 좋다.

악성코드 사고 조사는 비용이 많이 들고 부정확한 인텔리전스가 흔하다는 것은 알고 있어야 한다. 인텔리전스와 자동화된 방지 개선에 돈을 쓰면 보안 직원 조사에서는 큰 돈을 쓰지 않아도 될 것이다.

### 9. 제약과 네트워크 포트, 프로토콜, 서비스 제어


설정 오류, 원격 접속, 새로 설치된 소프트웨어의 기본 설정 서비스는 잠재적 공격자들에게 창문을 열어두는 격이다. 네트워크화된 기기상 모든 포트, 프로토콜, 서비스는 제대로 관리되어야 한다. 이는 이들을 추적, 제어하고 필요한 곳에서는 수정하는 것을 의미한다.

기업의 IT 담당자는 무엇이 필요하고 무엇이 안 필요한지 분명히 파악해야 한다. 초기부터 분명한 설정 계획을 짜면 앞으로 문제 해결에 걸리는 시간을 많이 아낄 수 있다.

포트를 스캔하고 서비스를 검토하고 비즈니스 운영에 불필요한 모든 것을 닫아라. 트래픽 승인을 위해 방화벽을 설치하고 서버를 확인시켜야 한다. 이들은 공격자들이 침투하기 단순한 취약점들이지만 역시 막아야 할 틈새이기도 하다. 그러므로 꼭 잠그자.

### 미루지 말라

이런 문제들에 대해 직원들을 교육시키고 이들이 취약점이 되지 않게 하는 알맞은 시스템을 구축해야 한다. 자동화된 시스템의 효과를 측정하는 것을 기억하고 실수와 실패를 통해 확실히 배울 수 있어야 한다.

피싱, 악성코드, 취약점 공격에 대한 가장 효과적인 방어는 보안 전문성, 교육된 직원, 자동화된 실시간 시스템, 입증된 분명하고 간결한 정책을 포함하는 다각적인 전략이다. 

# “보안, 생산성, 비용” 세 마리 토끼를 잡는 Dell Data Protection

Dell Korea



기업이 데스크톱과 노트북, 태블릿, 기타 기기를 교체해야 하는 데에는 여러 가지 이유가 있다. 더 작고 가벼우며, 에너지 효율성이 높은 시스템에서 최신 운영체제와 애플리케이션, 무선 기술을 이용해서 한층 미래에 준비된 업무 환경을 구현하고, 모바일 생산성을 높이는 것이 하나의 이유다. 시대에 뒤떨어진 하드웨어 및 소프트웨어를 지원하는데 드는 비용과 시간을 절감하는 것도 또 다른 이유가 될 수 있다.

그러나 하드웨어를 교체해야 하는 더 강력한 이유가 있다. 하드웨어와 운영체제, 애플리케이션의 보안을 강화해야 한다는 점이다. 직원들이 계속 새로운 방식으로 일을 하게 되면서, 중요한 데이터를 보호하고, 양적 질적으로 진화하고 있는 보안 위협에서 보호를 받을 수 있는 강력한 도구가 필요하다. 복잡성이 크게 가중되지 않으면서, 다양한 대규모의 시스템을 보호하고, 보안을 강화할 수 있는 올바른 도구가 있어야 한다.

하드웨어 교체 프로세스의 일환으로 엔드포인트 데이터 솔루션을 도입해 구현하면 고급 인증, 종합적인 암호화, 최첨단 악성코드 보호 기능을 제공할 수 있다. 또한, 사용자 생산성을 높이고, 미래에 대비된 업무 환경을 구현하고, 기업의 주요 정보를 보호하고, IT를 더욱 간소하게 관리할 수 있다.

## 현대적인 업무 환경 구현을 위한 도전 과제와 해결책

현대에는 모든 산업의 기업과 기관이 새로운 업무 방식을 수용해야 한다. 직원들은 거주지 인근의 커피숍, 공항, 가정에서 일하며, 전 세계 곳곳에서 끊임없이 로그인한다. 기업에서 지급한 데스크톱과 노트북에서 개인 소유의 스마트폰, 태블릿에 이르기까지 다양한 기기를 이용하며, 업무에 하나 이상의 기기를 사용하는 경우도 많다.

직원들이 상시 어디에서나 정보와 리소스를 이용할 수 있도록 만들면 생산성을 높이고, 협업을 촉진하고, 고객에게 더 나은 서비스를 제공할 수 있다. 그러나 보안을 훼손하지 않으면서 이런 업무 방식을 지원하기는 쉽지 않다. 직원들이 특정 기기, 애플리케이션, 업무 방식을 이용하지 못하게 하는 것은 해결책이 될 수 없다. 목표는 직원들이 필요에 따라서 승인되지 않은 도구를 이용할 수 있게 하는 것이 아니라, 통제를 하면서도 생산성을 높이

는 것이 되어야 한다.

보안 위협의 수와 범위가 증가하고 있는 만큼, 직원들이 사용하는 시스템 보안에 어려움이 커졌다. 공격자들은 네트워크에 침입해 정보를 훔치기 위해 직원들이 반복하는 행동, 일상 업무에 대한 정보를 획득한다. 이 때문에 직원들은 인터넷을 이용하거나, 이메일 첨부 파일을 여는 단순한 행위만으로 데이터 침해 사고의 공범이 될 수 있다.

보안 침해 사고 보도도 이어지고 있는데, 알려지지 않은 사고는 더 많다. 10개 국가를 대상으로 한 조사에 따르면, 지난 12개월 동안 보안 침해를 경험했다고 대답한 비율이 73%에 달했다.

이런 공격으로부터 직원과 데이터를 보호하기 위해 엔드포인트에 탄탄한 방어 체계를 구축할 필요가 있다. 현재 최상의 엔드포인트 방어책은 암호화, 인증, 지능형 위협에 대한 보호가 포함된 애플 내다보는 다계층 보호 시스템이다. 이와 동시에 다양한 기기를 표적으로 삼는 위협에 대처해야 하면서 복잡성이 증가할 소지가 있다. 이 때문에 정책 설정, 관리, 사용자 권한, 비밀번호, 인증 원격 관리에 이르기까지 다양한 관리자의 보안 작업을 간소화할 방법이 필요하다.

### 통합적이고 주도적인 보안 체계 도입

Dell은 보안 문제를 극복하면서 비즈니스 프로세스와 새로운 업무 방식을 효율적으로 지원, 기업과 기관의 보호와 준수, 구현에 도움을 줄 수 있는 데이터 보안 솔루션을 만들었다.

- **보호** : 기업과 기관은 내부와 외부 등 전체 조직을 효율적이면서도 한발 앞서 보호할 수 있어야 한다.
- **준수** : 기업과 기관은 정부와 업계의 규정, 기업 정책을 준수해 일관성 있으면서도 신뢰도 높은 거버넌스를 확보해야 한다.
- **구현** : 조직이 새로운 업무 방식을 수용하고, 최신 기술 구현을 앞당길 수 있게끔 새로운 전략과 데이터 보안 솔루션으로 비즈니스 프로세스를 지원해야 한다.

정보를 보호하고 규제를 준수하는 것이 아주 중요하지만, 보안을 생산성 향상의 대가로 사용해서는 안 된다. 직원이 자신이 선호하는 방식으로 업무를 수행하고, 원할 때 데이터에 액세스하고, 생산성을 유지하는 데 필요한 기기와 도구를 사용할 수 있게끔 데이터를 보호해야 한다. 직원들의 일상 워크플로우를 방해하지 않는 방식으로, 뒤에서 조용히 지능형 데이터 보안 기술을 운영해야 한다.

데이터 보안 솔루션은 IT의 효율성을 높이고, 관리 비용을 줄일 수 있도록 구현되어야 한다. 내부의 전문성이 제한된 기업과 기관조차도 데이터 보안 준수 여부를 빠르게 증명할 수 있어야 한다.

### 새로운 시스템에 기반을 둔 보호

데스크톱과 노트북, 태블릿, 기타 기기를 업데이트하면 최신 보안 기술을 적용할 기회가 생긴다. 새 시스템으로 보안을 구현하면, 하드웨어의 최소 권장사항을 충족할 확률이 높아지고, 최신 보안 소프트웨어를 십분 활용할 수 있다. 또 오래된 운영체제에 새 소프트웨어



를 배포할 때 발생할 수 있는 많은 문제를 피할 수 있다.

동일 업체로부터 새 시스템과 보안 솔루션을 선택하면 더 큰 장점이 있다. Dell은 하드웨어와 보안 소프트웨어 모두를 지원하는데, 이는 IT의 생산성을 높여준다. Dell에서 하드웨어 지원을 받고, 다른 곳에서 보안 소프트웨어 지원을 받을 필요가 없다.

Dell에서 하드웨어와 보안 소프트웨어를 모두 조달할 경우 조달 프로세스를 간소화할 수도 있다. 사전에 원하는 보안 솔루션을 탑재해서, 여러 시스템에 솔루션을 배포할 때 초래되는 비용과 시간 낭비를 없앨 수 있기 때문이다. 검증과 테스트를 마쳤기 때문에 도입 첫 날부터 안심하고 사용할 수 있다.

더불어, 보안 소프트웨어와 하드웨어를 함께 구입하면 소프트웨어 라이선싱을 오펙스(Opex)에서 카펙스(Capex)로 옮길 수 있다. 즉, 고정 비용으로 감가상각 할 수 있다는 의미다.

### Dell Data Protection으로 종합적인 엔드포인트 보안 구현

데이터를 보호하고, 규제 준수에 도움을 받고, 생산성을 높이기 위해서는 인증과 암호화, 위협 보호라는 3가지 필수 요소를 포괄하는 종합적인 엔드포인트 보안이 필요하다.

- 승인된 사용자만 데이터에 액세스 할 수 있도록 하는 인증
- 데이터가 어디에 있든 이를 보호하는 암호화
- 신뢰할 수 없는 콘텐츠로부터 사용자와 데이터를 보호하는 위협 보호

Dell 데이터 보호 솔루션 제품군은 이런 핵심 요소를 포괄하는 종합적인 기능을 제공한다(그림1 참조). Dell은 데이터에 중점을 둔 방법으로 보안을 강화하고, 사용자의 생산성을 향상시킨다. 이를 위해 모든 기기와 클라우드에 최고 수준의 암호화를 적용한다. Dell Data Protection(DDP)은 암호화, 지능형 위협 보호, 인증 도구를 통합하고, 엔터프라이즈 컴플라이언스 준수 보고 기능과 함께 하나의 관리 콘솔로 구현한 것이 특징이다.

### Dell Data Protection 포트폴리오

오직 Dell만 완전한 엔드포인트 보안 솔루션 제품군을 공급한다.

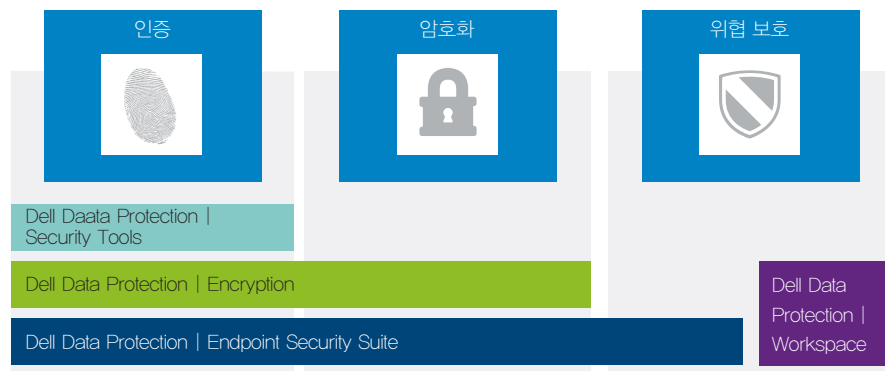


그림1 | Dell Data Protection 제품군은 인증과 암호화, 위협 보호에 필요한 사항을 해결한다.

### 최종 사용자 인증

인증은 보안 프레임워크의 초석 역할을 한다. Dell Data Protection|Security Tools (DDP|ST)는 Dell 프리시전(Precision), 래티튜드(Latitude), 옵티플렉스(OptiPlex) 시스템에 포함된 로컬 관리 인증 솔루션으로, Dell은 이를 통해 세계 최고 수준의 보안 기능을 갖춘 비즈니스 노트북을 공급하고있다.

DDP|ST의 고급 인증 옵션은 미승인 사용자와 데이터의 침입을 방지한다. 하드웨어 인증은 안전한 액세스 관리 기능을 제공하는데, 이를 위해 스마트카드와 지문 리더기를 사용한다. 또 FIPS(Federal Information Processing Standards) 201 인증서와 옵션으로 무접촉 스마트카드 리더기를 지원한다.

DDP|ST는 윈도우의 부팅 전 로그인과 SSO(Single Sign-On)을 지원, 사용자 경험을 간소화한다. 또한, 스마트폰 앱에서 셀프서비스 윈도우 비밀번호 재설정 기능을 지원한다. 이 앱은 안전한 일회용 비밀번호 토큰을 생성해서 헬프 데스크의 도움이 필요한 비밀번호 재설정 문제를 줄여준다. 이 앱은 iOS, 구글 안드로이드, 윈도우 모바일(Windows Mobile)을 지원한다.

### 지능형 암호화

기존 암호화 소프트웨어 솔루션은 배포와 관리가 어렵고, 여러 플랫폼으로의 확장성이 미흡했으며, 사용자의 생산성을 떨어뜨리는 요소였다. Dell Data Protection|Encryption(DDP|E)는 이런 문제점을 줄여서 기기, 외장 미디어, 퍼블릭 파일 동기화 및 공유 서비스 등 위치에 상관없이 데이터를 보호한다.

기기를 도난 당하거나 잃어버렸을 경우, 암호화가 데이터 액세스를 방지한다. 기기 유실과 관련된 규제 위반에 따른 벌금, 보고 등의 부담을 없애주는 경우도 많다. 단순화된 마이크로소프트 비트로커(BitLocker) 관리에서 풀 디스크 및 다중키 암호화에 이르기까지 다양하면서도 유연한 암호화 옵션을 제공한다. DDP|E와 옵션인 DDP Hardware Crypto Accelerator는 최고 수준인 FIPS 140-3 보호를 지원한다. 오직 Dell만 FIPS 140-2 인증을 획득하고, 추가 보안 계층을 위해 하드웨어에서 권한을 처리하는 TPM(Trusted Platform Module)을 공급하고 있다.

### 고급 위협 보호

Dell Data Protection|Protected Workspace (DDP|PW)는 지능형 공격에서 실시간으로 사용자와 데이터를 보호하기 위해 정교한 악성코드 방지 기법을 이용한다. APT(Advanced Persis-

## 모든 플랫폼의 IT 보안 취약점을 방지하는 Dell Data Protection

직원들은 다양한 기기를 사용하고 있으며, 하나 이상을 사용하는 경우가 많다. Dell Data Protection은 Dell 노트북과 데스크톱, 서버, 태블릿은 물론 스마트폰과 다른 기기 등 모든 엔드포인트를 지원한다. 구글 안드로이드, 애플 iOS와 OS X, 윈도우 등 다양한 운영체제 및 프로세스 플랫폼과 호환되기 때문이다.

이는 다음과 같은 장점이 있다.

- 업계 최고 수준의 전사적인 엔드포인트 보안
- 다양한 시스템 지원에 따른 IT의 복잡성 감소
- BYOD 프로그램 지원
- 패치 및 시스템 관리 단순화
- 사용자가 자유롭게 자신이 선호하는 도구를 이용해 업무를 수행할 수 있음

tent Threat)과 제로데이 취약점을 포함, 신뢰할 수 없는 콘텐츠로부터 사용자를 보호한다. 그리고 사용자가 상시 인터넷에 액세스하거나, 마이크로소프트 오피스 또는 어도비 아크로벳 등 위협이 큰 애플리케이션을 이용할 수 있는 안전한 환경을 구현한다.

DDP|PW는 행동 기반 탐지(behavior-based detection)를 이용한다. 악성코드 공격 시, 악성코드가 호스트 운영 시스템, 메모리, 네트워크 통신에 액세스를 못하도록 방지하고, 데스크톱 이미지를 다시 만드는 시간 낭비 없이 시스템을 재빨리 복원한다. 악성코드가 사용자 데이터 및 호스트 OS에 접근하지 못했기 때문에, 단 몇 초 만에 복구가 완료된다. DDP|PW는 또 IT 관리자가 전사적인 보안을 개선할 수 있도록 상세한 포렌식 데이터를 제공한다.

### Dell의 차별점

Dell의 새 클라이언트 시스템과 보안 솔루션을 선택하면 교체 프로세스를 간소화하는데 도움이 된다.


여러 업체와의 관계를 관리할 필요 없이, 한 업체에서 제품을 구입하고 지원받을 수 있다. Dell의 보안 솔루션은 Dell 시스템상에서 완전한 테스트와 검증 과정을 거쳤기 때문에, 모든 것이 제대로 작동한다고 확신해도 된다. 이러한 엔드 투 엔드(End to end) 솔루션은 복잡성과 위협을 경감하는데 도움이 된다.

또한, 인텔® 코어™ v프로™ 프로세서 제품군을 탑재한 신형 디바이스의 경우는 인텔의 AMT(Active Management Technology)와 원격 KVM(Keyboard, Video, and Mouse) 기능으로 포괄적인 원격 관리 환경을 제공한다. 관리자는 이들 기능을 이용해 장애를 해결하거나 업데이트를 배포할 수 있으며, 원격으로 시스템을 재가동하거나 전원이 꺼진 시스템에 액세스하고 운영체제를 사용하지 못하도록 할 수도 있다. 이런 높은 수준의 관리성과 액세스는 지원 비용의 절감은 물론, 높은 가동시간과 사용자 만족도로 이어진다.

과거 어느 때보다 공격이 정교해지고 있다. 따라서 기업의 상황에 맞게 데이터를 보호할 수 있는 추가적인 지원이 필요할 수 있다. Dell은 기업의 환경에 가장 잘 부합하는 방식을 판단하는 데 도움이 되는 광범위한 보안 전문성을 보유하고 있다.

### 결론

기업과 기관에는 IT 시스템을 교체해야 하는 이유가 많다. 그러나 가장 중요한 이유 중 하나는 새로운 보안 위협으로부터 스스로를 보호하고, 다양한 업무 방식을 지원하는 것이다. 어떤 엔드포인트 기기에서나 데이터를 보호해야 한다. 사무실, 가정, 공항, 다른 국가 등 직원이 어디에 있든 보호할 수 있어야 한다.

새롭게 도입한 시스템에 Dell Data Protection을 구현하면, 사전 설치, 검증, 테스트가 완료된 업계 최고 수준의 엔드포인트 보안 솔루션을 사용할 수 있다. 이러한 전략으로 보안을 강화하고 생산성을 높이는 동시에 TCO 절감이 가능하다. 



# 비즈니스 급 노트북을 재정의하다.



CES 2016 혁신상에 빛나는 Latitude 13 7000 시리즈 비즈니스 노트북



## Latitude 13 7000 시리즈 비즈니스 노트북

인텔® 코어™ 프로세서 및 13.3" Full HD 또는 QHD+ 터치 지원 인피니티 에지 디스플레이를 갖추고도 단지 1.43cm 두께, 1.12Kg에 불과한 가벼운 무게로 세계에서 가장 작은 13.3" 비즈니스 급 노트북 새로운 Latitude 13 7000 시리즈를 만나보십시오.

[www.dell.co.kr](http://www.dell.co.kr)에서 지금 구매하실 수 있습니다.

울트라북, 셀러론, 셀러론 인사이트, 코어 인사이트, 인텔, 인텔 로고, 인텔 아톰, 인텔 아톰 인사이트, 인텔 코어, 인텔 인사이트, 인텔 인사이트 로고, 인텔 바이브, 인텔 v프로, 아이테니엄, 아이테니엄 인사이트, 펜티엄, 펜티엄 인사이트, 바이브 인사이트, v프로 인사이트, 제온, 제온 Phi 및 제온 인사이트는 미국과 다른 나라에서 인텔사의 등록상표입니다.

• 제품 사진의 크기 비율은 동일하지 않습니다. • 표시 화면은 합성 이미지입니다. • 제품의 실제 색상은 인쇄 관계로 다를 수 있습니다. • 이 광고에 사용된 제품 사진은 출하시의 제품과 일부 다를 수 있습니다. • 구성이나 사양에 따라 제공이 제한되는 경우가 있습니다. 상세한 내용은 당사 영업부로 문의하시기 바랍니다. • Dell Precision, DELL 로고는 미국 Dell Inc.의 상표 또는 등록 상표입니다. • 기타 회사명 및 제품명은 각 회사의 상표 또는 등록 상표입니다.

인텔 인사이트®. 더 강력한 솔루션 아웃사이드.

