
SONICWALL®
사이버 공격 전략의
유형과 대응 방법
E-BOOK

서론

최근의 사이버 범죄자들은 다양한 동기, 특히 금전적 이득을 노리고 한층 복잡해진 수법을 사용하여 탐지를 피하고 네트워크에 조용히 잠입합니다. 이러한 위협 행위자들은 지적 재산을 훔치고, 중요 정보를 훔쳐 보고, 프로세스를 망치거나 파일을 인질로 잡는 등 다양한 범죄를 저지릅니다. 이들을 최신 기술을 채택하여 탐지를 회피하고 발각 없이 긴 시간 액세스하여 악성 활동을 수행하려고 합니다.

공격자가 공격할 취약점을 찾아내면 침입한 시스템에 맬웨어 다운로드 및 설치를 시도합니다. 대부분의 경우 아직 전통적인 안티바이러스 솔루션이 파악하지 못한 신종 변종 맬웨어가 사용됩니다.

이 eBook은 사이버 범죄자가 네트워크에 침투하기 위해 사용하는 사이버 공격 전략과 도구를 상세히 설명하고, 이러한 전략에 제대로 반격해 사이버 범죄자의 공격 과정을 중단시키는 방법을 자세히 소개하겠습니다.

사이버 공격 전략 #1
24시간 내내 맬웨어로 네트워크 무차별 융단폭격

맬웨어의 총 건수가 증가 추세이며, 몇몇 국가에서는 수백만 건의 시도로 기록적인 수치를 보이고 있습니다. 공격은 어떤 벡터를 통해서도 들어와 네트워크에 침투할 수 있습니다. 이메일, 모바일 디바이스, 웹 트래픽 등이 모두 표적이며, 해커는 자동 취약점 공격을 통해 그 누구라도 희생양으로 삼습니다. 꼭 염두에 둘 사실은 회사 규모는 중요하지 않다는 것입니다. 누구든 해커에게는 IP 주소이자 이메일 주소, 즉, 빈틈을 노려 공격할 먹잇감에 불과합니다. 공격자는 자동화된 도구로 밤낮없이 취약점 공격을 퍼붓고 피싱 이메일을 발송합니다.

많은 조직의 문제는 바로 여기에 제대로 대응할 수 있는 도구가 없다는 점입니다. 트래픽을 걸러내고, 엔드포인트를 보호하고, 악성 이메일을 필터링하는 도구는 자동화가 부족한 경우가 많습니다. 숨겨진 위협을 찾기 위해 암호화된 트래픽 내에 보이지 않는 방화벽을 실행하거나 제한된 온보드 시스템 메모리에 맬웨어 서명을 저장하는 경우도 많습니다.

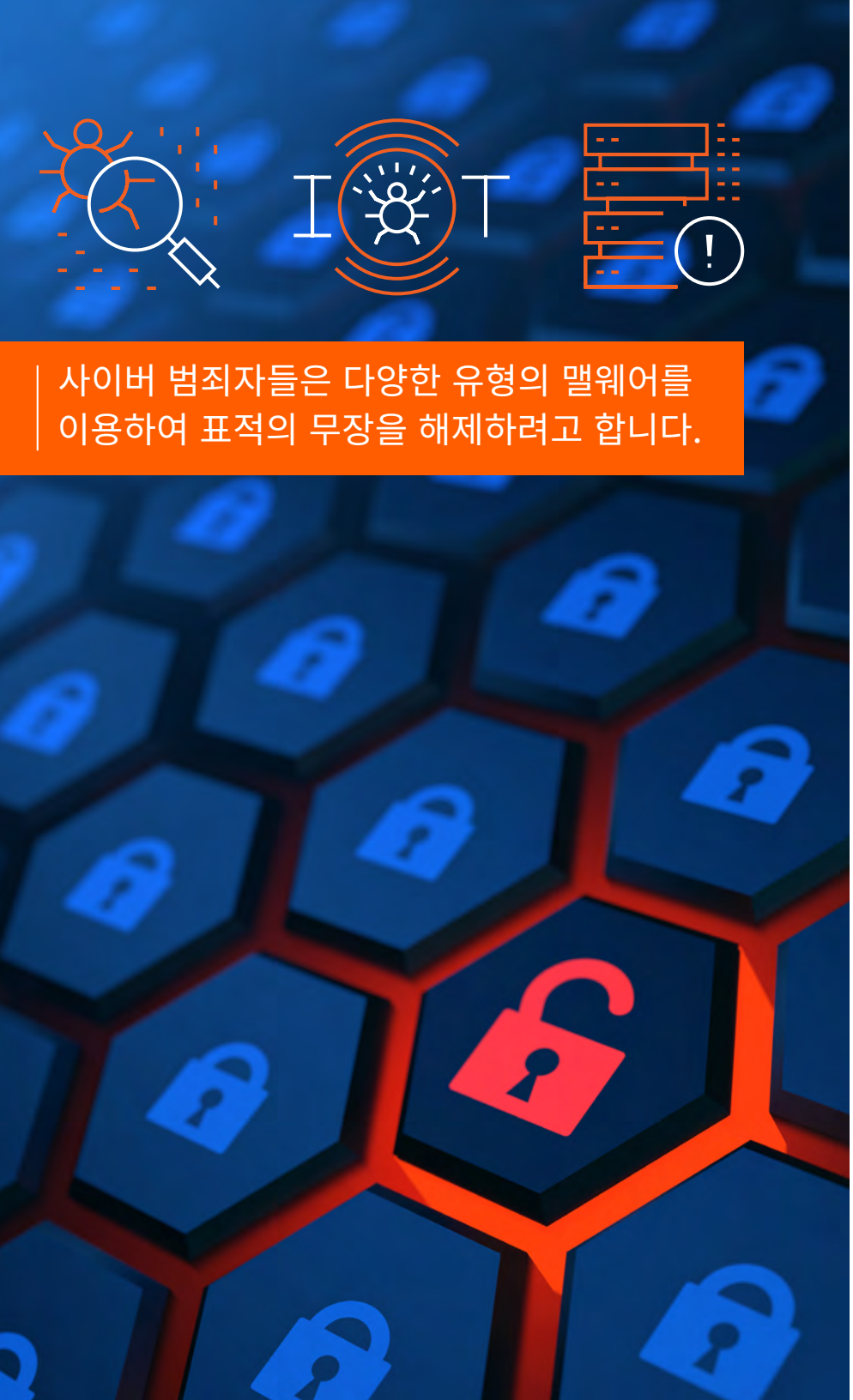
365일/
24시간

반격 #1
매일, 매 순간 네트워크 보호

기존에 없었던 맬웨어 변종이 매시간 수백 개는 넘게 개발되고 있으므로, 이러한 신종 위협에 맞서 최신의 실시간 보호책을 강구해야 합니다. 효과적인 보안 솔루션이라면 실시간으로 위협을 탐지하고, 조직을 한 해 내내 24시간 보호해줄 수 있는 최신 기술을 갖추고 있어야 합니다. 각종 유형의 맬웨어와 변종이 대규모로 쏟아져 들어오므로 어떤 방화벽이라도 쉽게 가용 메모리를 초과하게 됩니다. 실시간 심층 메모리 검사(Real-Time Deep Memory Inspection, RTDMI™)와 같은 기술이 적용된 보안 서비스 솔루션은 불특정 다수를 겨냥한 제로데이 위협과 알려지지 않은 맬웨어 변종을 선제적으로 탐지하여 차단합니다.

방화벽이 최대한 거시적인 시각에서 맬웨어를 모니터링하고 완전히 새로운 변종을 발견해 식별하려면 클라우드 기반 샌드박스를 사용해야 합니다. 사물인터넷(IoT) 디바이스가 공격자의 진입점 역할을 할 수 있으므로, 동적으로 업데이트되어 방화벽 게이트웨이뿐 아니라 모바일 및 원격 엔드포인트도 보호할 수 있는 보안 솔루션을 갖추는 것이 매우 중요합니다.

최신 악성 소프트웨어 위협에 대응하기 위해 클라우드의 힘을 활용한 실시간 침입 감지 및 예방을 자동으로 제공하는 보안 플랫폼을 요구하세요.



사이버 범죄자들은 다양한 유형의 맬웨어를 이용하여 표적의 무장을 해제하려고 합니다.

사이버 공격 전략 #2 다양한 형태의 맬웨어로 네트워크 감염시키기

사이버 범죄자들은 다양한 공격 벡터와 맬웨어 변종을 이용하여 네트워크에 침입하려 합니다. 주로 이용되는 다섯 가지는 바이러스, 웜, 트로이 목마, 스파이웨어, 랜섬웨어입니다.

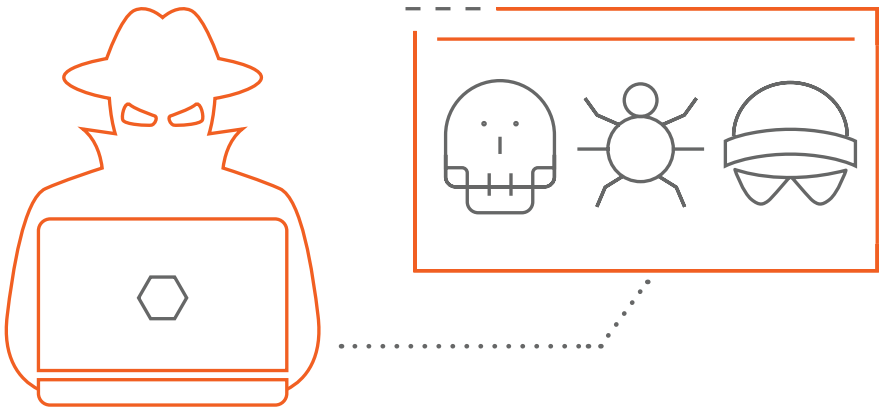
과거 컴퓨터 바이러스는 감염된 미디어의 공유를 통해 확산되었습니다. 기술이 발전함에 따라 배포 방식도 진화했습니다. 현재 바이러스는 흔히 불법 프로그램, 파일 공유, 웹 다운로드, 이메일 첨부파일을 통해 확산됩니다. 열거나 실행하면 데이터 손상부터 시스템 다운까지, 매우 다양한 악성 증상을 발현시킵니다.

컴퓨터 웜은 1980년대 말부터 존재했으나 조직 내 네트워킹 인프라가 대중화되기 전까지는 널리 확산되지 못했습니다. 컴퓨터 바이러스와 달리 웜은 자가 증식하여 인간의 개입 없이도 네트워크를 통해 번져 나갈 수 있습니다. 그래서 감염 속도가 빠르고 네트워크 트래픽 과부하를 유발합니다.

트로이 목마는 합법적인 소프트웨어나 파일을 가장하여 네트워크로부터 민감한 데이터를 추출하도록 고안된 악성 프로그램입니다. 감염된 시스템은 다양한 종류의 트로이목마가 제어하고 공격자가 접근하도록 백도어를 열어둡니다. 트로이목마는 봇넷을 만드는 데에도 사용됩니다.

스파이웨어는 본질적으로 악성인 것은 아니지만 웹브라우저를 감염시켜 사용하기 아주 불편하게 만들기 때문에 상당히 성가십니다. 스파이웨어는 합법적인 애플리케이션의 탈을 쓰고 사용자에게 약간의 혜택을 제공하면서 몰래 키 입력과 브라우징 내역을 기록하고, 개인 데이터를 훔치고, 사용자의 행동이나 사용 패턴을 추적합니다. 훔친 데이터는 공격자에게 전송되어 사용자의 프라이버시 및 보안을 침해하는 데 활용됩니다.

랜섬웨어는 엔드포인트나 서버 전체의 파일을 암호화하여 액세스할 수 없게 변형시키는 공격입니다. 사이버 범죄자들은 희생양에게 복호화 키를 건네주는 조건으로 비트코인 등의 몸값을 요구합니다. 랜섬웨어가 비즈니스에 중요한 시스템에까지 확산되게 되면 해결하기 위한 비용이 수십억 원 이상에 달할 수도 있습니다.



위협을 선제적으로 차단하려면 맬웨어에 맞서 보호하는 층을 여러 겹 두르는 것이 좋습니다.

반격 #2
모든 유형의 맬웨어로부터 네트워크가 보호될 수 있게 조치

방화벽이라면 모든 유형의 사이버 위협으로부터 조직을 안전하게 보호해야 합니다. 기존 보호 범위였던 게이트웨이를 넘어 엔드포인트까지 한 곳에서, 저지연으로 공격 벡터를 차단할 수 있는 보호 기능이 통합되어 있어야 소기의 목적을 제대로 달성할 수 있습니다. 다음과 같은 기능이 갖춰져 있는지 살펴보십시오.

- 네트워크 기반 맬웨어 보호 - 공격자가 맬웨어를 다운로드하거나 전송하여 시스템에 침입하지 못하게 차단
- 지속적이고 시기 적절한 업데이트 - 수많은 신종 맬웨어 변종을 즉각 발견하여 24시간 내내 네트워크를 안전하게 보호
- 침입 방지 서비스(IPS) - 공격자가 취약점을 공략할 수 없도록 방지
- 샌드박싱 의심스러운 코드를 클라우드 기반 격리 환경으로 보내 파훼하고 분석함으로써 기존에 없었던 맬웨어 발견
- 액세스 보안 - 모바일 및 원격 엔드포인트가 네트워크 범위 내부에 있든 외부에 있든 사용자 액세스 제어 대책 적용
- 이메일 보안 - 이메일을 통해 전송되는 피싱, 스팸, 트로이 목마, 소셜 엔지니어링 공격 차단

네트워크에 액세스하는 모든 디바이스에 최신 안티바이러스 보호 소프트웨어가 설치되어 있어야 네트워크 맬웨어 보호를 위한 추가 계층이 확보됩니다. 조직 내 PC에서는 종합 안티바이러스를 실행하고 네트워크에는 방화벽을 실행하면 사이버 범죄자가 네트워크에 침입하기 위해 사용하는 많은 도구를 중지시킬 수 있습니다.

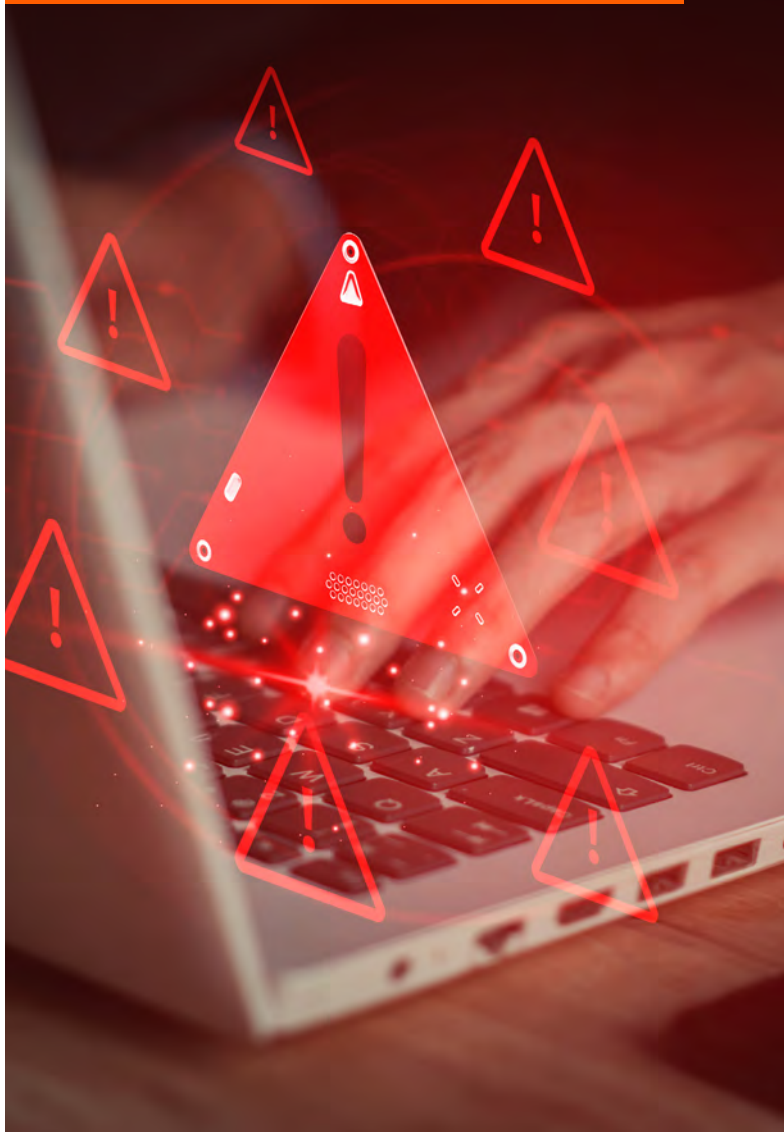
사이버 공격 전략 #3
가장 약한 네트워크를 찾아 침투

대다수의 방화벽 업체가 우수한 위협 보호 성능을 주장하지만 솔루션의 효과를 입증할 수 있는 곳은 일부에 불과합니다. 기존의 방화벽을 사용하는 조직은 네트워크가 보호되고 있다 믿지만 숙련된 사이버 범죄자는 복잡한 알고리즘을 사용하여 탐지를 회피하여 적절한 보안 조치가 부족한 구식 방화벽을 쉽게 우회함으로써 네트워크에 침투할 수 있습니다.

몇몇 방화벽은 보안을 위해 성능을 희생시키므로 높은 네트워크 성능을 이용해야 할 때 보안 조치를 꺼버리고 싶은 유혹을 느끼기 쉽습니다. 이는 절대 해서는 안 될 매우 위험한 관행입니다.

네트워크 보안의 다른 취약점은 인적 요인에서 발생합니다. 범죄자들은 사람의 행위나 행동으로 네트워크의 무결성, 기밀성, 가용성이 실수로 침해될 수 있는 가능성을 호시탐탐 엿봅니다. 위험성을 초래하고 보안 조치를 약화시킬 수 있는 행위에는 피싱 사기, 소셜 엔지니어링, 시스템 오구성, 소프트웨어 패치 미적용, 보안 정책 무시 등이 있습니다. 위협 행위자는 이러한 전술로 취약점을 공략해 로그인 정보 등 인증 정보를 얻어 내부에서 공격을 유도함으로써 방화벽 보호를 간단히 우회합니다. 그리고 적절한 보안 조치 없이 개인 디바이스를 회사 네트워크에 연결하는 직원들도 있습니다. 이 경우, 조직의 네트워크 보안 범위 밖에서 개인 디바이스를 분실하거나 방치하고 자리를 뜨면 미승인 액세스가 발생하여 회사의 보안이 심각하게 침해될 수 있습니다.

사이버 범죄자들은 그들이 찾아낸 네트워크 취약점을 기반으로 희생자를 표적화 합니다.



> 방화벽이라면 성능 저하 없이 내부 및 외부의 모든 공격으로부터 네트워크를 보호해주는 엔진이 갖춰져 있어야 합니다.

반격 #3
우수한 위협 보호, 높은 성능, 중앙집중식 관리가능한 통합적인 보안 플랙폼을 선택하세요.

독립적인 테스트로 네트워크 기반 맬웨어 보호 성능을 인증받은 보안 솔루션을 선택합니다.

멀티코어 플랫폼 설계로 크기와 유형에 관계없이 파일을 스캔하여 변화하는 트래픽 흐름에 대응할 수 있는지 확인하는 것이 좋습니다. 방화벽이라면 성능 저하 없이 내부 및 외부의 모든 공격으로부터 네트워크를 보호해주는 엔진이 갖춰져 있어야 합니다.

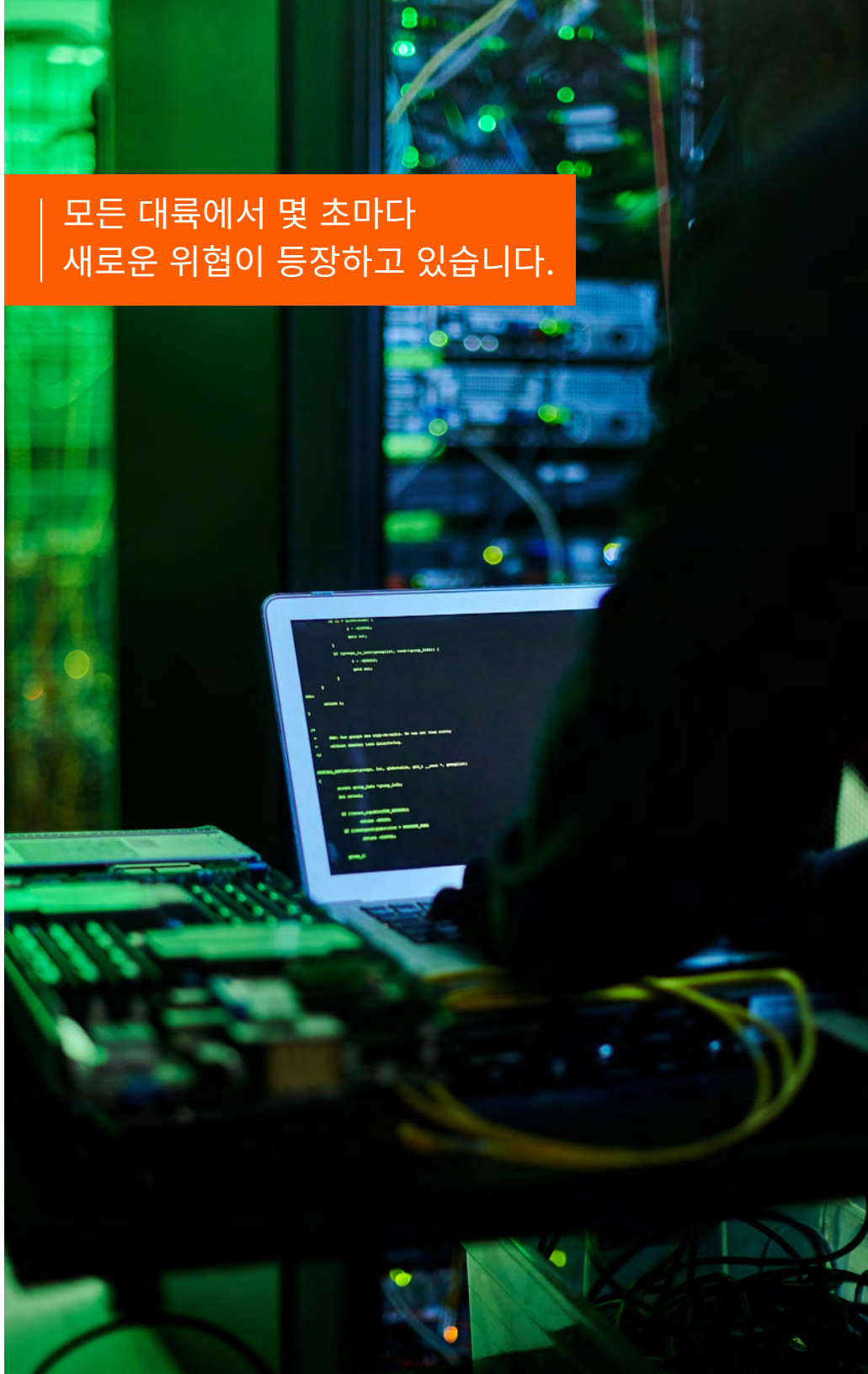
클라우드 기반 샌드박스를 갖춰, 귀사의 환경을 표적으로 삼는 완전히 새로운 맬웨어를 발견할 수 있는 방화벽을 선택하십시오. 이런 선택이 미래의 하루가 일상적인 근무일이 될지, 사이버 범죄자가 디지털 자산을 인질로 협박하는 날이 될지 가를 수 있습니다.

보안 전략은 보안 모바일 액세스 범위 내부는 물론 외부의 모바일 및 원격 엔드포인트도 보호할 수 있어야 합니다.

적절한 이메일 보안을 갖춰 피싱, 스팸, 바이러스, 소셜 엔지니어링 등 이메일로 전송되는 위협으로부터 보호하는 것도 중요합니다. 무료 SonicWall 피싱 퀴즈 등의 도구를 활용하여 직원들을 교육하십시오.

사이버 공격 전략 #4 수시로 모습을 바꾸고 전 세계적으로 공격

많은 사이버 범죄자들은 신종 맬웨어를 지속적으로 개발하고 세계 곳곳의 범죄자에게 공유합니다. 그래서 모든 대륙에서 몇 초마다 새로운 위협이 등장하고 있습니다. 많은 범죄자들은 "치고 빠지기" 접근법으로 공격합니다. 즉, 침투하여 가능한 많은 것을 취하고 알람이 울리기 전에 빠져 나갑니다. 여러분이 무슨 일이 일어났는지 인지하기도 전에 이미 들어왔다 나갈 수 있습니다. 더 많은 데이터를 장기간 은밀하게 빼내기 위해 아주 조심스럽고 천천히 공략하는 공격자도 있습니다. 웹을 통해 진행되는 공격도 있고, 이메일을 통해 진행되는 것도 있으며, 네트워크 보안 범위 밖에 있는 동안 감염된 디바이스를 통해 네트워크에 직접 침투하기도 합니다.



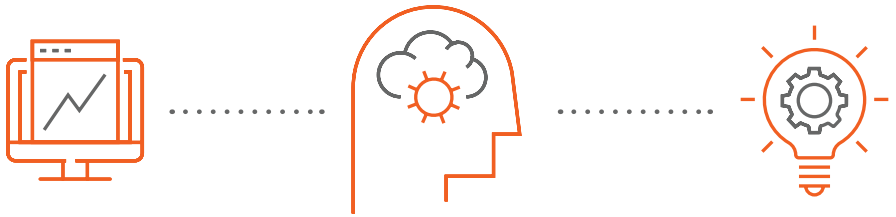
최신 글로벌 위협을 차단하려면 글로벌 위협 인텔리전스를 갖춘 보안 솔루션에 투자해야 합니다.

반격 #4
글로벌 위협으로부터 보호해주는 방화벽 선택

위협에 신속하게 대응해야 보호력을 극대화할 수 있습니다. 신종 위협에 맞선 대응책을 신속하게 배포하려면 자체 위협 인텔리전스와 연구팀, 대책팀을 보유한 보안 솔루션 업체를 선정하는 것이 좋습니다. 많은 사람이 참여하는 보안 커뮤니티와 협력하여 SonicWall 사이버 위협 보고서와 같은 유용한 자료를 발행할 역량이 있는 곳이면 더욱 좋습니다.

스펙트럼이 넓은 솔루션은 전 세계적 규모의 포괄적인 클라우드 기반 맬웨어 카탈로그를 활용하여 로컬 방화벽 분석 성능이 뛰어납니다.

간단한 방화벽은 지역에 한정된 위협을 식별하고 차단할 수 있으나, 더욱 정교한 차세대 방화벽은 봇넷 필터링 기능이 추가되어 위험한 도메인에서 흘러드는 트래픽과 악성 위치를 오가는 연결을 차단함으로써 알려진 글로벌 위협에 노출될 가능성을 줄여줍니다.



결론

네트워크 기반 사이버 공격을 효과적으로 방어하는 전략을 개발하려면 강력한 보안 관행을 통합하고, 성능 저하 없이도 비정상적인 네트워크 동작을 탐지하여 대응할 수 있는 효과적인 보안 도구를 사용한 총체적인 접근법을 택해야 합니다. 진화하는 위협에 능동적으로 대체함으로써 알려지지 않은 위협으로부터 여러분 개인과 조직을 보호하십시오.

평가를 통해 귀사의 필요에 정확히 맞는 솔루션을 추천받고 싶다면 SonicWall 영업 담당자에게 문의하거나 SonicWall 차세대 방화벽(NGFW) 온라인 페이지를 방문하여 자세히 알아보십시오.

자세한 내용을 알고 싶으십니까?

문의해주시면 SonicWall 보안 전문가가 연락을 드리겠습니다.

SonicWall 제품군 라이브 데모도 마련되어 있습니다.

웹페이지에서 차세대 방화벽에 대해 자세히 알아보실 수 있습니다.

최신 공격이 어디서 자주 일어나는지 Capture Labs Security Center에서 확인해보십시오.

SonicWall 소개

SonicWall은 초분산 시대와 모든 사람이 원격, 모바일 및 비보안 상태인 업무 현실을 위한 경계 없는 사이버 보안(Boundless Cybersecurity) 서비스를 제공합니다. SonicWall은 알려지지 않은 정보에 대한 실시간 가시성을 제공하며 혁신적인 경제성으로 전 세계 기업, 정부, 중소기업 간 사이버 보안 비즈니스 격차를 해소합니다. 자세한 정보는 www.sonicwall.com을 방문해 주십시오.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
기타 정보는 웹 사이트에서 확인할 수 있습니다.
www.sonicwall.com

Ebook-TypesofCyberattacks-JK-8854