미연방 기관의 온라인 보안 재수립

단순히 사이버 위협과 공격자를 뒤쫓는 데 그치지 않습니다. 사용자와 데이터를 멀웨어, 랜섬웨어, 스파이웨어 및 제로데이 공격으로부터 격리시킵니다.

eBook

MENLO SECURITY

미연방 기관에 있어 **사이버 보안은 타협의 대상이 아닙니다.**

지난 수년 간 미연방 기관에는 수많은 중대 보안 사건이 발생했으며 그 수는 현재도 계속 증가하고 있습니다. 이러한 공격은 국가 보안은 물론 전 세계 공급망을 위험에 빠뜨렸습니다.

보안 침해로 인해 사회 보장 번호, 개인 건강 기록 및 기타 HIPAA 보호 정보 등 엄청난 양의 개인 식별 정보(PII)가 노출되었습니다. 이러한 공격은 시민들을 신원 도용과 인신 공격에 취약한 상황에 노출시키며 정부 시스템의 무결성에 대해 의문을 제기하게 만듭니다.

미연방 기관에서 주로 사용하는 보안 도구와 프로토콜은 시스템과 데이터를 보호하지 못하는 경우가 많습니다. 최근의 중대 공격 사례는 위협의 위험성을 크게 부각시키고 있습니다. 일례로 2020년 9월에 일어난 공격[1]의 경우 VPN의 알려진 약점을 악용하여 연방 기관 내 여러 사용자의 액세스 자격 증명 도용이 시도되었습니다.

> 미국 회계 감사원(Government Accountability Office)은 정부 기관에서 사이버 보안 전략을 개발하고 시스템을 보호하며 지적 재산, PII와 같은 개인 정보 및 민감한 데이터와 중요 인프라를 보호하기 위해 시행해야 하는 **조치를 강조**했습니다. 그러나 민간 기구가 매년 사이버 보안에 80억 달러(USD)가 넘는 **비용을 투자**하는 상황에서도 위협은 계속되고 있습니다.

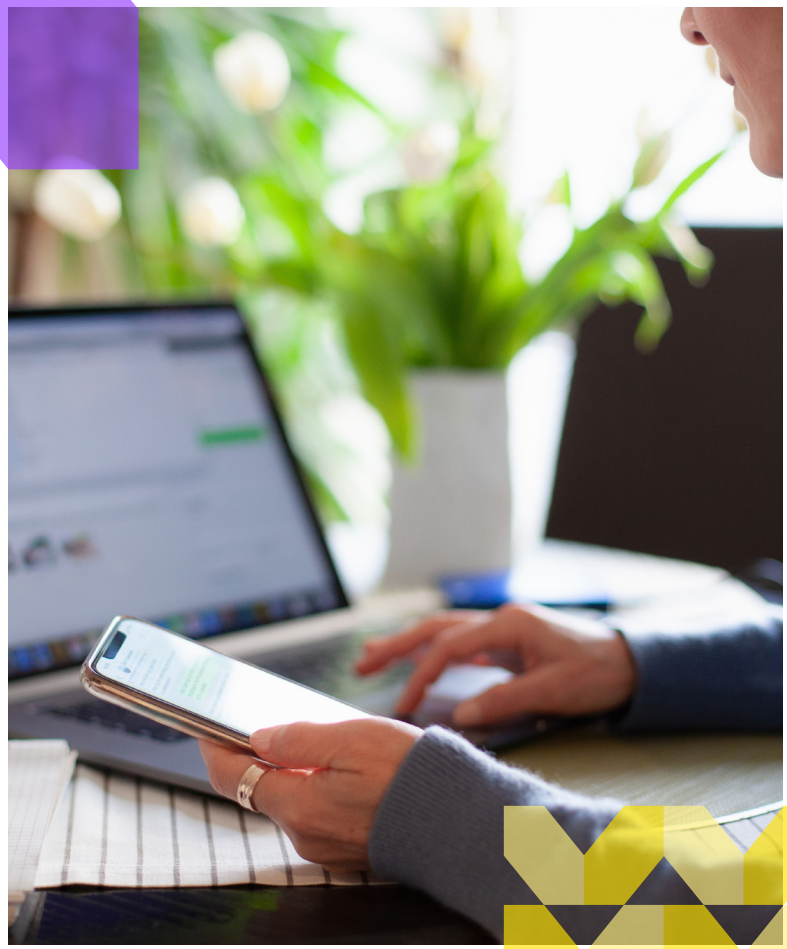
피싱 이메일, 악의적인 웹사이트 및 첨부 파일에 숨겨진 공격 코드 모두 공격자가 정부 시스템에 침투하는 데 사용하는 방법으로, 데이터를 반출하거나 정부 기관의 업무 수행 능력에 피해를 줄 수 있습니다. 제로데이 공격은 가장 큰 위협이 될 수 있습니다. 악성 코드가 수개월 동안 휴면 상태로 있다가 시스템과 데이터를 손상시키거나 하이재킹할 수 있어 감지한 시점에는 이미 너무 늦어버리기 때문입니다.

그렇다면 보안 소프트웨어와 장비에 대한 정부 기관의 대규모 투자에도 불구하고 사이버 공격이 계속 증가하는 이유는 무엇일까요?[2]

사용자의 주의가 필요합니다.

믿기지 않겠지만 정기적인 교육[3]과 반복적인 주의[4]에도 불구하고 사용자들은 계속 피싱 이메일의 링크를 클릭하거나 감염될 가능성이 있는 웹사이트에 방문합니다. Menlo Security에서 최근 미연방 정부 고객을 대상으로 수행한 연구에서 충격적인 동향이 발견되었습니다. 전체 사용자 군을 대상으로 추론한 결과에 따르면 90일 동안 해당 기관 직원이 매월 위험한 URL 100,000개 이상에 액세스하고 있습니다. 이러한 위험 상황을 정부 전체로 확대해보면 현재 도구만으로는 데이터와 시스템에 대한 사이버 위협을 차단할 수 없다는 결론이 명확해집니다.

1 https://www.nextgov.com/cybersecurity/2020/09/hackers-take-data-further-reconnaissance-breach-federal-agency/168791/
2 https://www.latimes.com/politics/story/2020-08-28/federal-work-from-home-cybersecurity
3 https://public.cyber.mil/training/phishing-awareness/
4 https://www.cio.gov/assets/resources/telework-infographic.pdf



코로나19에 따른 영향:
늘어난 단말만큼 취약점도 증가했습니다.

코로나19 대응 조치의 일환으로 시작된 재택 근무 전면 실시로 미연방 공무원들의 생산성이 유지되며 정부 조직 전체에 IT 현대화를 위한 노력이 가시화되고 있습니다. 재향 군인 병원[5]과 같은 일부 기관의 경우 이미 시행되고 있던 디지털 변환 프로그램이 "전면적인 재택 근무"로의 빠른 전환에 도움이 되었습니다.

그러나 원격 단말 수가 증가함에 따라 보안 위험도 함께 커졌습니다. 보안 팀에서 재택 근무자 시스템에 대한 가시성을 확보하는 데 한계가 있었으며 가정용 WiFi의 경우 정부 기관의 온사이트 네트워크보다 보안이 크게 취약할 수 있습니다.

6월, 팬데믹 대응 책임 위원회(Pandemic Response Accountability Committee)는 "공개 자료 업무를 수행하는 재택 근무자의 부적절한 기밀 정보 누출 및 공개[6]"에 대해 환경 보건국(Environmental Protection Agency)과 국가 정찰국(National Reconnaissance Office)에서 제기한 문제를 보고했습니다.

재택 근무 체제가 상당 기간 계속될 가능성이 높은 상황에서 기밀 데이터에 대한 원격 액세스 증가와 같은 이러한 조건은 시스템과 개인을 위험에 빠뜨리는 지속적인 공격의 토대가 될 수 있습니다.

5 https://governmentciomedia.com/va-digital-modernization-foundation-covid-19-response
6 https://www.oversight.gov/sites/default/files/oig-reports/Top%20Challenges%20Facing%20Federal%20Agencies%20-%20COVID-19%20Emergency%20Relief%20and%20Response%20Efforts_1.pdf

더 많은 비용 투자가 답이 될 수 없습니다.

기관들은 단말 보호, 엔터프라이즈 바이러스 백신, 침입 감지 및 기본적인 문제조차 해결하지 못하는 기타 기술에 계속 많은 투자를 하고 있습니다. 사용자 시스템이 감염되거나 적대적인 시스템에 직접 연결될 때마다 악성 코드를 다운로드하는 위험이 뒤따릅니다.

현재 보안 도구만으로는 에지 및 IoT 장치 등 네트워크에서 시스템과 데이터를 보호하기에 부족합니다. 이러한 도구는 사후 대응적이기 때문입니다. 즉, 기존 보안 도구는 기본적으로 공격이 실제로 발생하거나 알고 있는 서명이 나타날 때까지 아무런 조치를 취하지 않습니다.

동시에 보안 도구는 업무를 지원해야 하며 그 속도가 느려서는 안 됩니다. 사용자가 여러 게이트와 프로세스를 진행하는 데 따른 대기 시간과 시스템 오버헤드 없이 작업을 처리할 수 있도록 사이버 솔루션이 투명하게 작동해야 합니다. 또한 정부 기관의 경우 보안은 IT 현대화, 특히 확장성, 예측 가능한 SLA, 경제성을 목적으로 한 클라우드 및 SaaS 기반 운영으로의 전환을 지원해야 합니다.

2021 회계연도 대통령 예산에서 제안된 미연방 사이버 보안 자금:

188억 달러(USD)

2020 회계연도 추정 금액과는 동일하지만 2019 회계연도 실제 지출보다 **18억 달러**(USD) 많은 금액.

350,000건

매일 새롭게 생겨나는 멀웨어와 잠재적으로
바람직하지 않은 애플리케이션

7억개

2020년에 예상되는 멀웨어 수.

네트워크를 보호하려면 **가정을 바꿔야 합니다.**

대부분의 사이버 보안 제품과 서비스는 공격을 차단하는 것이 네트워크 경계에서 공격을 감지하는 것만큼 간단하다는 확신을 기반으로 합니다. 그러나 피싱 이메일은 권한 있는 사용자가 실수로 보안 프로토콜을 우회하도록 공격합니다. 반면 악성 코드 감지만으로는 부족하며 공격을 식별하려면 주목해야 하는 대상을 알아야 합니다. 많은 기관에서 사용하는 온프레미스 제품이 실패하는 주된 이유는 사용자 또는 데이터와 같은 위치에 있지 않기 때문입니다. 이 경우 보안 솔루션을 우회하는 공격의 영향을 완화시킬 수 있는 추가 제품이 필요합니다.

새로운 멀웨어 변형이 매일 나타나는 상황에서 대부분의 보안 제품은 공격 서명을 지속적으로 패치하고 업데이트해야 합니다. 업데이트가 끊임 없이 계속되는 상황에서는 기본적인 문제가 해결되지 않습니다. 즉, 권한 있는 사용자가 웹, 이메일 및 문서에 숨겨진 악의적인 소프트웨어에 연결됩니다.

이론적으로 원격 사용자를 위협으로부터 보호해야 하는 VPN도 그 답이 아닙니다. 코로나19의 기하급수적인 확산과 함께 정부 재택 근무자도 계속 증가하는 상황에서 공격자들은 특정 VPN의 취약점을 악용하여 보호 시스템에 대한 액세스를 시도하고 있습니다.[7] 여기서도 문제는 보안 제품이 네트워크 에지에서 공격을 감지하고 무력화시키는 데 완벽하지 않은 방식을 사용하며 사용자들이 온라인 커뮤니케이션, 검색 및 공동 작업하도록 계속 허용한다는 점입니다.

[7] https://us-cert.cisa.gov/ncas/alerts/aa20-099a

불완전한 보안으로 초래되는 비용은 **데이터 손실 그 이상입니다.**

대부분의 보안 운영 센터(SOC)는 과중한 업무에 시달립니다. 거짓 경보를 추적하는 데 시간과 자원이 소요되며 공격 후 이미지로 시스템 다시 설치 작업을 수행하려면 내부 및 대민 업무 모두 몇 시간에서 며칠 또는 그 이상 중단되기도 합니다. 이러한 경우 인건비(과중한 업무에 따른 피로 포함)부터 공공 기관의 신뢰도까지 모든 것이 영향을 받게 되며 기관 역할에도 문제가 발생합니다.

또한 정기적인 사이버 보안 작업에는 엄청난 시간과 노력이 필요합니다. 업데이트가 진행되는 동안 VPN 등 연중무휴 실행되어야 하는 시스템도 중단될 수 있습니다[8].

기존 보안 소프트웨어는 하드웨어 비용도 매우 높습니다. 도구에 따라 하드웨어를 정기적으로 교체해야 합니다. 이러한 경우 비용 부담이 불가피하며 소프트웨어보다 하드웨어 가격이 더 높을 수도 있습니다. 그러나 이런 투자에도 불구하고 IT 보안 팀은 오탐을 포함한 모든 경보를 평가하기 위해 고분군투할 수 밖에 없습니다. 여기서 오탐은 소프트웨어 버그나 알 수 없는 네트워크 트래픽이 그 원인으로, 담당자가 실제 위협을 파악하지 못하는 결과를 초래합니다.

AV, 멀웨어 차단 도구 및 침입 감지 도구로 시스템을 보호하던 시대는 끝났습니다. 이제 사용자를 위험한 온라인 리소스로부터 격리시켜야 합니다. 가장 많이 악용되는 공격 벡터인 피싱 이메일, 악의적인 웹사이트 및 감염된 다운로드 파일에서 비롯되는 멀웨어, 랜섬웨어, 스파이웨어 및 제로데이 공격을 100% 완벽하게 차단할 수 있는 솔루션이 필요합니다.

이제 필요한 것은 보다 직접적인 방식입니다. 즉 경계를 방어하는 것이 아니라 표적을 *다른 위치*에 격리시켜야 합니다.

8 https://us-cert.cisa.gov/ncas/alerts/aa20-073a

진정한 의미의 제로 트러스트는 인증에 그치지 않습니다.

제로 트러스트 아키텍처는 절대적으로 유효한 개념이지만 대부분의 "제로 트러스트" 모델은 특히 액세스하는 리소스가 온라인 상태인 경우에 그 역할을 다하지 못합니다. 현재 제로 트러스트 구현은 리소스에 대한 액세스만 제한할 수 있으며 여전히 사용자 장치와 공격 대상이 될 수 있는 온라인 데이터가 직접 연결됩니다.

반면에 격리는 네트워크 최종 사용자와 온라인 환경 사이에 가상의 "에어갭"을 만듭니다. 노트북 웹 브라우저에서 직접 웹사이트를 여는 방식이 아닌 클라우드 내 가상 머신이 대상 웹사이트에서 제공하는 모든 콘텐츠를 가져오고 실행합니다. 다음 단계로, 정화 버전의 웹사이트가 최종 사용자에게 전송되며 모든 악성 코드가 제거된 상태로 웹사이트는 완벽하게 작동합니다.

멀웨어가 있어도 일회용 컨테이너에만 영향을 미칠 수 있으며 클라우드 플랫폼이 피싱 웹사이트를 감지하고 읽기 전용 모드로 전환한 후 사용자에게 경고로 알려줍니다. 이것이 바로 진정한 의미의 제로 트러스트 보안입니다. 즉 어떠한 웹 리소스도 신뢰할 수 없다고 가정하며 사용자는 실제로 모든 잠재적인 위협으로부터 분리됩니다.

웹 격리는 생산성을 향상시킵니다.

격리 워크플로에서는 이메일 내 링크를 클릭하거나 웹사이트로 이동해도 멀웨어가 네트워크 환경에 유입될 수 없습니다. 사이트와 사용자 장치 간에 직접 연결되지 않기 때문입니다. 사용자에게는 대기 시간이나 성능 저하가 발생하지 않아 프로세스가 완전히 투명해집니다.

실제로 격리 모델은 생산성을 향상시킬 수 있습니다. 네트워크는 전통적으로 웹과 내부 트래픽을 모두 지원하도록 설계되었지만 SaaS 앱과 멀티미디어 사이트로의 전환에 의해 웹 수요가 광범위하게 증가했습니다. 대부분의 대역폭 제어 기술은 일부 사용자나 용도에 맞도록 성능을 조정합니다. 그러나 YouTube 및 Vimeo와 같은 동영상 사이트와 CNN과 같은 많은 뉴스 사이트는 최고의 경험을 제공하기 위해 기본적으로 고해상도 콘텐츠를 지원하며 그에 따라 대역폭 요구 사항도 증가합니다.

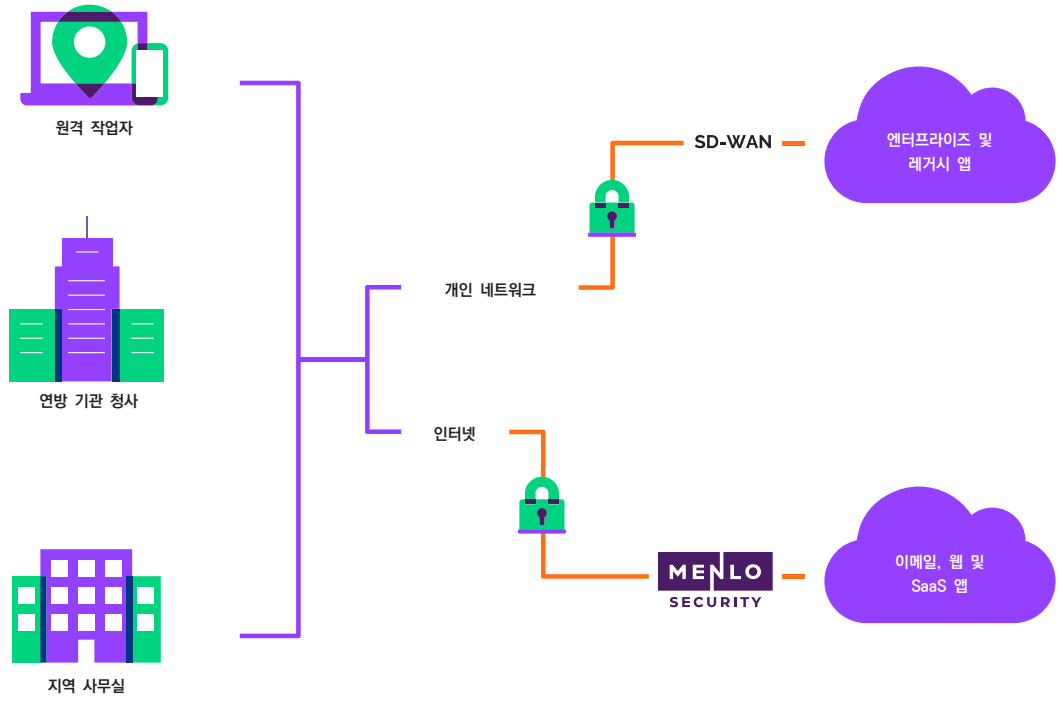
내부 네트워크에서 웹 트래픽을 분할하고 기관 정책에 따라 동영상 해상도를 표시하도록 클라우드 보안 플랫폼을 구성함으로써(즉, 해상도 자동 제한) 가상 사이트에서 눈에 띄는 품질 저하 없이 최종 사용자 장치로 콘텐츠를 빠르게 전달할 수 있습니다. 이는 또한 과거 미연방 공무원에게 불필요했던 웹의 일부분을 보다 광범위한 연결 조건에서 액세스할 수 있음을 의미합니다.

병목을 제거합니다.

생산성은 대기 시간과 직접적인 관련이 있습니다. VPN은 무선 또는 가정용 Wi-Fi를 통한 가변적인 연결뿐만 아니라 트래픽 속도를 저하시키는 오버헤드를 가중시킬 수 있습니다. 이는 결과적으로 파일 전송 속도 저하, SaaS 앱의 응답 속도 지연, 화상 회의 중 끊김 및 중단 현상으로 이어질 수 있습니다.

이러한 속도 저하는 특히 대역폭 관점에서 인터넷 연결이 제한될 수 있는 지역의 기관 시설에도 영향을 미칩니다.

그러나 클라우드 기반 격리 플랫폼은 병목을 제거합니다. 기관은 간편한 분할 터널 VPN 방식으로 분류되지 않은 트래픽을 클라우드 격리 플랫폼으로 직접 전달함으로써 대역폭 부담을 줄일 수 있습니다. 이제 더 이상 정부 네트워크를 통해 트래픽을 백홀하거나 분류되지 않은 정보를 처리할 때 인터넷 액세스 지점(IAP)이나 신뢰할 수 있는 인터넷 연결(TIC)을 거치지 않아도 되므로 DoDIN 또는 .gov 네트워크의 보안을 강화할 수 있습니다.



진화하는 보안 전략의 구성 요소

클라우드 격리 플랫폼은 조직의 IT 변환 전략을 완벽하게 지원하므로 퍼블릭, 프라이빗 및 하이브리드 클라우드 환경과 쉽게 조화될 수 있습니다. 클라우드 격리는 "전면 교체" 방식이 아닌 기존 네트워크를 계속 지원하므로 보다 안전하면서 관리가 용이한 미래로의 전환을 가능케 합니다.

IT 및 보안 관리 관점에서 클라우드 격리 방식의 또 다른 이점은 다음과 같습니다.

중앙 집중식 제어

특정 사용자나 모든 사용자에게 즉시 보안 프로토콜을 적용할 수 있으며 사용자 수십만 명을 대상으로 빠르게 웹 보안을 활성화할 수 있습니다. 사용자 연결과 웹 동작에 대한 투명성과 가시성으로 정책을 시행할 수 있습니다.

즉각적인 확장성

기능이 클라우드에 있으므로 개인 장치에 단말 소프트웨어를 설치하지 않아도 됩니다. 증가 또는 가변적인 요구 사항을 지원하도록 필요에 따라 플랫폼이 자동 확장될 수 있습니다.

데이터 손실 보호 기능 강화

클라우드 격리 모델은 부주의나 악의적 의도에 관계없이 내부자 위협으로부터 보호하는 데도 도움이 됩니다. 데이터 손실 보호(DLP) 엔진은 많이 볼 수만 있으며 데이터는 난독 처리 기법을 통해 DLP 스택에서 숨겨질 수 있습니다. 그러나 클라우드 격리는 보안 환경을 떠나는 모든 데이터(파일, 게시글, Put 매개 변수 등)에 대한 100% 완벽한 가시성을 제공하므로 현재 DLP 솔루션과 함께 보안을 강화합니다.

기관 전체에 대한 가시성

사용자가 클릭한 링크와 웹상의 목적지를 알고 있으므로 보다 효과적인 사이버 전략을 개발할 수 있습니다. 간단하면서도 포괄적인 대시보드로 문제 활동을 쉽게 찾아내고 상세하게 분석할 수 있습니다.

사용자 ID 익명화

정부 사용자의 경우 사이트 소유자가 해당 트래픽이 연방 기관에서 시작된 사실을 알지 못하는 상태에서 온라인 리소스를 사용할 수 있어야 합니다. 웹 요청 소스를 보호하는 것이 중요합니다. 상대방이 해당 정보, 즉 특정 기관의 구성원이 감염된 사이트를 브라우징하고 있다는 사실을 악용하여 공격할 수 있기 때문입니다. 클라우드 격리의 경우 요청 소스가 기관 네트워크가 아닌 가상 서버이므로 최초 IP 주소를 효과적으로 숨길 수 있습니다.

기존 인프라와의 통합

클라우드 기반 격리 솔루션이 현재 SD-WAN 구현을 강화하여 직접 인터넷 트래픽을 클라우드 서비스로 전송할 수 있습니다. 클라우드 격리는 모바일 장치 관리(MDM) 도구에도 적용되므로 스마트폰과 태블릿을 보호하고 원격 작업 전략을 완벽하게 지원합니다.

업무가 수행되는
모든 곳에서 보호합니다.

재택 근무, 현장 데이터 수집 또는 항공선 유지 관리 수행 여부에 관계없이 원격 인력은 데이터, 앱 및 공동 작업 도구에 빠르고 안정적으로 액세스할 수 있어야 합니다. 앞에서 설명한 바와 같이 TIC 또는 IAP에서 네트워크 트래픽의 상당 부분을 이동함으로써 대역폭과 처리량에 큰 이점을 가져다줄 수 있습니다.

보안 클라우드 플랫폼 모델은 Microsoft 365, G Suite, Box, Salesforce 및 ServiceNow 등 모든 생산성 및 공동 작업 도구를 지원합니다. 이제 SaaS 앱이 웹사이트처럼 가상 브라우저에서 실행되므로 이메일 첨부 파일 문서를 포함한 모든 문서를 안전하게 열고 공유할 수 있습니다.

격리 모델은 민감한 데이터에 대한 읽기 **전용 액세스**를 제공하므로 사용자가 문서를 다운로드해야 하는 횟수가 약

80%

정도 줄어듭니다.

어디서나 생산성과 보안을 지원합니다.

현재 보안 조치로는 부족합니다. 생산성과 신뢰성을 지원하지 않는 것은 물론 공격자가 새로운 위협을 만들고 보안 팀이 이에 최대한 신속하게 대응하는 상황이 계속될 뿐입니다. 보안 스택이 99.9% 효과적이더라도 시스템과 데이터가 취약해질 수 있는 가능성을 완전히 배제할 수는 없습니다.

공격자를 따라잡지 않고 격리시켜야 합니다. Isolation Core™ 기반 Menlo Security 클라우드 플랫폼은 멀웨어, 랜섬웨어 및 제로데이 공격에 대한 탁월한 보안 성능을 제공합니다. 동시에 대역폭 최적화를 통한 성능 향상이라는 실질적인 이점과 함께 관리 업무를 간편하면서도 포괄적으로 제어할 수 있습니다.

피싱 이메일과 의심스러운 웹사이트 문제를 제거함으로써 필수 시스템과 데이터에 대한 위협 대부분을 제거할 수 있습니다. 사용자에게는 투명한 환경을 제공합니다. 정부 기관은 Menlo Security 클라우드 플랫폼을 통해 리소스를 유지하고 주어진 업무에 집중할 수 있습니다.

이제 정부 기관에서 랜섬웨어, 멀웨어 및 제로데이 공격을 차단할 수 있습니다.

피싱 및 악의적인 웹사이트에서 비롯되는 위협을 제거하고 모든 사용자를 위한 온라인 성능을 향상시킬 수 있습니다.

menlosecurity.com/solutions/government

www.menlosecurity.com

(650) 614 1705 | Korea@menlosecurity.com

MENLO SECURITY