방화벽 개요

Palo Alto Networks 차세대 방화벽

애플리케이션 사용, 사용자 행동 및 복잡하고 뒤얽힌 네트워크 인프라의 근본적인 변화로 인해 전통적인 포트 기반 네트워크 보안에 취약점을 노출시키는 위협 환경이 조성되고 있습니다. 사용자는 업무 관련성 및 보안 리스크를 고려하지 않은 채 다양한 유형의 디바이스에서 실행되는 수많은 애플리케이션을 이용하고자 합니다. 한편 데이터센터 확장, 네트워크 세분화, 가상화 및 이동성 전략은 전통적인 보안 메커니즘을 우회하는 보다 정교해지고 진화한 새로운 위협으로부터 네트워크를 보호하는 동시에 애플리케이션 및 데이터에 대한 안전한 액세스를 구현할 방법을 찾기를 요구하고 있습니다.

과거에는 네트워크 보안을 위해 모든 것을 차단하거나 업무 편의를 위해 모든 것을 허용하는 두 가지 방안 중 하나를 선택해야 했습니다. 이러한 선택에는 타협의 여지가 거의 없었습니다. Palo Alto Networks®의 차세대 보안 플랫폼은 사이버 위협을 예방하면서 액세스를 허용하는 방식을 통해 사용자가 필요로 하는 애플리케이션을 안전하게 이용할 수 있도록 하는 방법을 제공합니다.

Palo Alto Networks의 차세대 방화벽은 차세대 보안 플랫폼의 핵심으로, 가장 정교한 위협도 처리할 수 있도록 근본적으로 설계된 제품입니다. 차세대 방화벽은 애플리케이션, 위협 및 콘텐츠를 포함하여 모든 트래픽을 검사하여 장소 및 디바이스 유형에 상관없이 이를 사용자와 연계시킵니다. 업무의 필수 요소인 애플리케이션, 콘텐츠 및 사용자가 기업 보안 정책의 일부가 되는 것입니다. 따라서 보안을 주요 업무 계획에 맞게 조율할 수 있습니다. Palo Alto Networks의 차세대 보안 플랫폼을 사용하면 사고 대응 시간을 단축하고, 알려지지 않은 위협을 발견하고, 보안 네트워크 구축을 원활하게 수행할 수 있습니다.

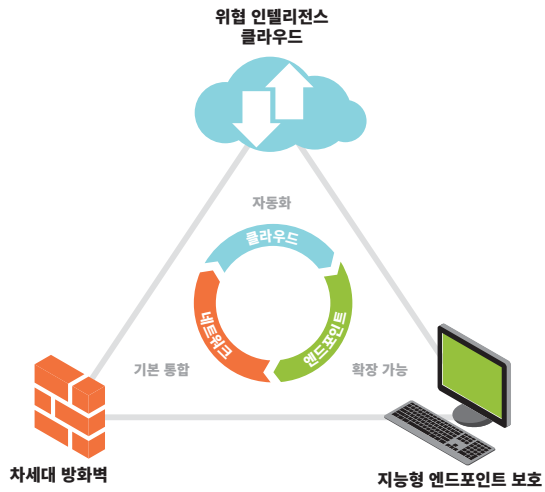

그림 1: Palo Alto Networks 차세대 보안 플랫폼

- 모든 트래픽을 분류하고, 업무상 사용 사례를 판단하고, 해당 애플리케이션(Software as a Service(서비스로서의 소프트웨어, SaaS) 애플리케이션 포함)에 대한 액세스 허용 및 보호가 이루어지도록 정책을 적용함으로써 애플리케이션, 사용자 및 콘텐츠를 안전하게 보호합니다.
- 불필요한 애플리케이션을 삭제하여 위협 대상을 줄임으로써 위협을 방지하고 표적 보안 정책을 적용하여 취약점 공격, 바이러스, 스파이웨어, 봇넷 및 알려지지 않은 멀웨어(APT)를 차단합니다.
- 애플리케이션 유효성 검증, 데이터 격리, 악성 애플리케이션 통제 및 신속한 위협 방지를 통해 데이터센터를 보호합니다.
- 가시성 및 통제 강화를 통해 퍼블릭 및 프라이빗 클라우드 컴퓨팅을 안전하게 보호하고, 가상 머신 채택에 맞춰 보안 정책을 배포, 시행 및 유지합니다.
- 차세대 보안 플랫폼을 장소에 상관없이 사용자 및 디바이스로 확장함으로써 안전한 모바일 컴퓨팅 환경을 구현합니다.
- 귀사의 구조에 맞춤화된 직관적인 관리 기능과 함께 디바이스, 네트워크 및 정책의 관리를 원활하게 합니다.

차세대 보안 플랫폼은 공통 보안 원칙을 바탕으로 광범위한 보안 요건을 충족하도록 돕습니다. 네트워크 보안과 GTI(global threat intelligence) 및 엔드포인트 보호를 균형 있게 조합하여 전반적인 보안 상태를 강화하고 보안 사고 대응 시간을 단축하는 동시에 업무 계획을 뒷받침할 수 있습니다.

보안을 통해 비즈니스의 자율권 강화

Palo Alto Networks의 차세대 보안 플랫폼을 통해 애플리케이션, 사용자 및 콘텐츠를 바탕으로 하는 정책을 통해 비즈니스의 자율권을 강화할 수 있습니다. 또한 당사 플랫폼 전용으로 설계된 포지티브 제어 모델을 통해 특정 애플리케이션이나 기능은 활성화하고 다른 것은 모두 차단할 수 있습니다(명시적 또는 묵시적). 차세대 방화벽은 전체 포트에 걸쳐 풀 스택(full stack) 싱글 패스 방식의 검사를 수행하기 때문에 보안 정책 결정의 토대가 되는 애플리케이션, 관련 콘텐츠 및 사용자 ID에 관한 완전한 컨텍스트를 제공합니다.

- 항상 모든 포트를 통과하는 애플리케이션을 모두 분류합니다. 오늘날 애플리케이션과 그 콘텐츠는 다양한 기법을 사용해 포트 기반 방화벽을 쉽게 우회할 수 있습니다. Palo Alto Networks의 차세대 보안 플랫폼은 기본적으로 복수의 분류 메커니즘을 트래픽 흐름에 적용하여 애플리케이션, 위협 및 멀웨어를 식별합니다. 포트, 암호화(SSL 또는 SSH) 혹은 채택한 회피 기법에 상관없이 모든 트래픽이 분류됩니다. 일반적으로 트래픽에서 적은 비중을 차지하나 잠재적 위험이 높은 식별되지 않은 애플리케이션은 체계적 관리 대상으로 자동으로 분류됩니다.
- 위협 대상을 줄이는 방식으로 사이버 공격을 예방합니다. 트래픽이 완전히 분류되면 특정 애플리케이션만 허용하고 나머지는 모두 거부하는 방식으로 네트워크상의 위협 대상을 줄일 수 있습니다. 그런 다음 조율된 사이버 공격 예방 기능을 적용하여 알려진 멀웨어 사이트를 차단하고 익스플로잇, 바이러스, 스파이웨어 및 악성 DNS 쿼리를 방지할 수 있습니다. 알려지지 않았거나 맞춤화된 멀웨어는 가상화 샌드박스 환경으로 보낸 후 파일을 실행해서 악성 행위를 직접 관찰함으로써 분석하고 식별합니다. 새로운 멀웨어가 발견되면 감염 파일 및 관련 멀웨어 트래픽에 대한 시그니처가 자동으로 생성되어 귀하에게 전달됩니다.
- 애플리케이션 트래픽 및 관련 위협을 사용자 및 디바이스에 매핑합니다. 기업의 보안 상태를 강화하고 사고 대응 시간을 단축하기 위해서는 애플리케이션 사용을 사용자 및 디바이스 유형에 대해 매핑하고 그 결과로 얻은 컨텍스트를 보안 정책에 적용할 수 있어야 합니다. 기업 사용자 리포지토리와의 통합을 통해 애플리케이션에 액세스하는 Microsoft® Windows®, Mac® OS X®, Linux®, Android® 또는 iOS 사용자 및 디바이스의 ID를 식별합니다. 사용자 및 디바이스의 ID 식별과 통제의 통합으로 사용자가 어디에서 어떤 디바이스를 사용하든지, 회사 네트워크상의 모든 애플리케이션이 안전하게 사용되도록 할 수 있습니다.

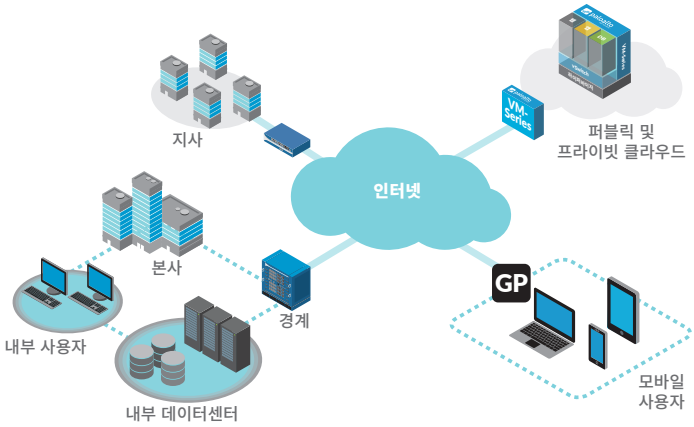

그림 1: 기업 전체에 걸쳐 안전한 지원 정책 배포

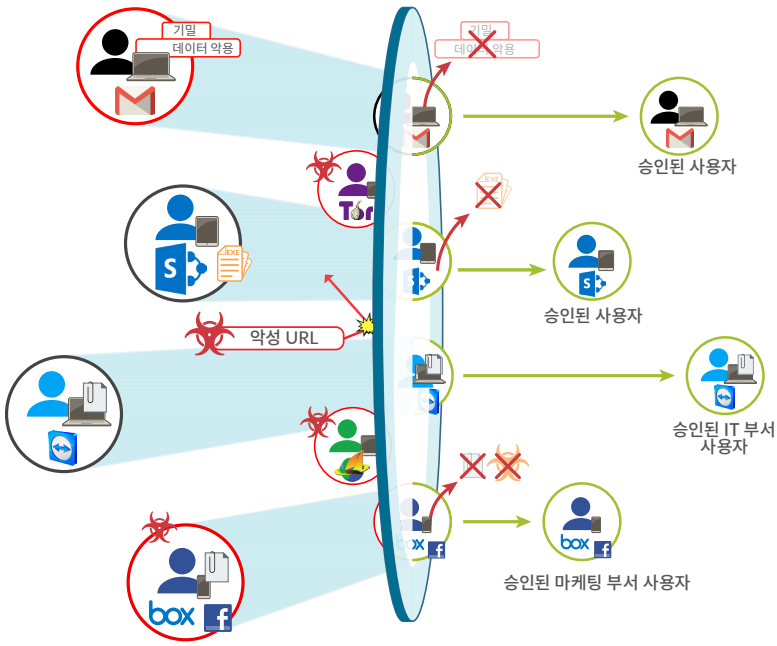

그림 2: 완벽한 통제 범위에 있는 애플리케이션, 콘텐츠, 사용자 및 디바이스

그림 3: 애플리케이션 활동을 명확하고 쉽게 파악할 수 있는 형식으로 보여 주는 인터페이스. 애플리케이션, 애플리케이션의 기능 및 사용 중인 사람에 대해 자세히 알아보려면 필터를 추가하거나 제거합니다.

사용 중인 특정 애플리케이션, 애플리케이션이 수반할 수 있는 콘텐츠 및 위협, 관련된 사용자 및 디바이스에 대한 컨텍스트를 구축하면 정책 관리를 능률적으로 수행하고, 기업의 보안 상태를 강화하고, 사고 조사를 가속화하는 데 도움이 됩니다.

완전한 컨텍스트 - 보다 엄격한 보안 정책

보안 관련 모범 사례를 살펴보면 정책 관련 결정, 네트워크 활동에 대한 보고 능력, 포렌식 역량은 컨텍스트에 좌우됩니다. 사용 중인 애플리케이션, 방문 웹사이트, 관련 페이로드 및 사용자에 관한 컨텍스트는 모두 네트워크 보호에 있어 가치 있는 데이터입니다. 인터넷 게이트웨이를 통과하고, 데이터센터 또는 클라우드 환경 내에서 작동하고, 원격 사용자에 의해 사용되고 있는 애플리케이션을 정확히 파악하고 있다면 위협 방지와 조율된 구체적인 세부 정책을 그와 같은 애플리케이션에 적용할 수 있습니다. IP 주소뿐만 아니라 사용자가 누군지 파악할 경우, 보다 정밀한 정책 할당을 가능하게 하는 또 다른 컨텍스트 요소를 확보할 수 있습니다.

상호 작용이 뛰어난 가상화 및 로그 필터링 도구가 애플리케이션 활동, 관련 콘텐츠 또는 위협, 사용자, 사용되는 디바이스 유형에 관한 컨텍스트를 제공합니다. 이러한 데이터 항목 각각은 그 자체로 네트워크의 일부를 파악하는 데 유용하지만, 전체적인 컨텍스트를 알 수 있다면 잠재적 보안 위험을 포괄적으로 파악해 더욱 현명한 정책 결정을 내릴 수 있습니다. 모든 트래픽이 끊임없이 분류됩니다. 상태가 변하면 변경 사항이 분석을 위해 기록되고 그래픽 요약이 동적으로 업데이트되어, 사용이 간편한 웹 기반 인터페이스상에 정보가 표시됩니다.

- 인터넷 게이트웨이에서 신규 혹은 낯선 애플리케이션을 조사하여 애플리케이션 설명, 동작 특성 및 사용자를 신속하게 판단합니다. URL 범주, 위협, 데이터 패턴을 그래픽으로 자세히 보여주므로 게이트웨이를 통과하는 네트워크 트래픽을 보다 다각적으로 파악할 수 있습니다.
- WildFire™에 의해 알려지지 않은 멀웨어 존재 여부가 분석된 모든 파일은 세부 항목(사용된 애플리케이션, 사용자, 파일 형식, 표적 OS, 관찰된 악성 행위 등)과 함께 가시성 도구에 기록됩니다.
- 데이터센터 내에서, 사용 중인 모든 애플리케이션을 검증하고 권한 있는 사용자에 의해서만 애플리케이션이 사용되고 있는지 확인합니다. 데이터센터 활동에 대한 가시성 강화로 잘못 구성된 애플리케이션이 있는지 혹은 SSH 또는 RDP의 악의적 사용이 있는지 확인할 수 있습니다.
- AutoFocus™ 위협 인텔리전스 서비스로 위협 분석, 포렌식 및 위협 헌팅 워크플로가 가속화되고, 디바이스로부터 PAN-OS®에 고유한 맥락적 위협 데이터가 직접 제공됩니다.
- 퍼블릭 및 프라이빗 클라우드 환경에서, 가상 서버의 생성 및 이전에 보조를 맞추면서 차세대 보안 플랫폼을 통해 정책을 적용하고 애플리케이션을 보호합니다.
- 모든 구축 시나리오에서 알려지지 않은 애플리케이션(일반적으로 네트워크 트래픽에서 차지하는 비중 작음)을 분석 및 체계적 관리를 위해 분류할 수 있습니다.

어떤 애플리케이션이 사용되고 있는지, 얼마나 많이 사용되고 있는지, 누구에 의해 사용되고 있는지 완전히 파악하지 못하는 경우가 많습니다. 네트워크 트래픽(애플리케이션, 콘텐츠 및 사용자)의 업무 관련 측면을 완전히 파악하는 것이 더욱 현명한 정책적 통제를 위한 첫 번째 단계입니다.

애플리케이션 구현을 통한 위험 감소

과거에는 위험 감소 프로세스는 네트워크 서비스 이용 제한과 잠재적인 업무 방해를 의미했습니다. 오늘날에는 위험 감소는 기존의 '모든 것을 거부'하는 접근 방식과 '모든 것을 허용'하는 접근 방식 간에 균형을 이루는 데 도움이 되는 업무 중심 접근 방식을 통해 애플리케이션을 안전하게 구현함을 의미합니다.

- 애플리케이션 그룹 및 SSL 복호화를 통해 몇몇 변종 애플리케이션에 대한 웹메일 및 인스턴트 메시지 전송을 제한하고, 모든 위협에 대해 검사하고 알려지지 않은 의심스러운 파일(EXE, DLL, ZIP 파일, PDF 문서, Office 문서, Java®, Android® APK)을 분석 및 시그니처 개발을 위해 WildFire로 업로드합니다.

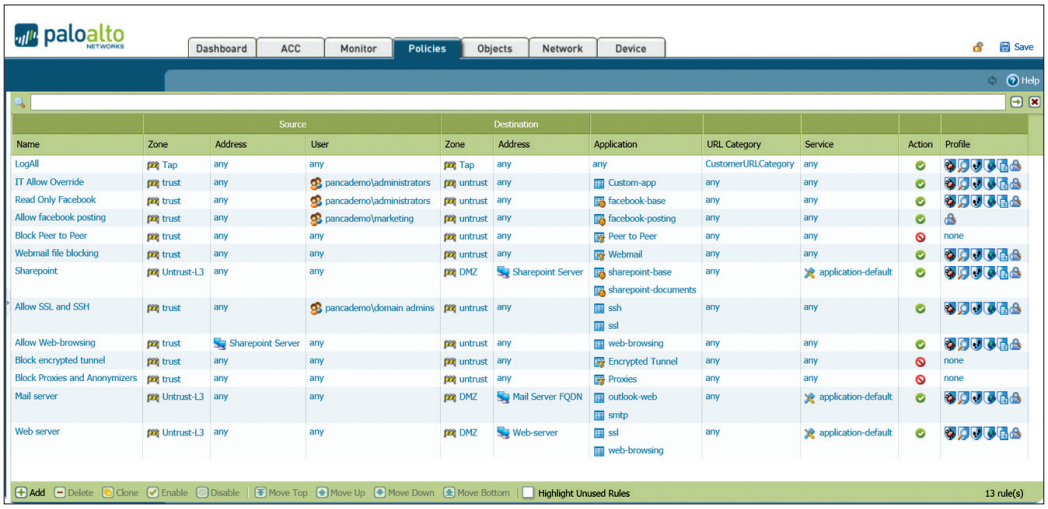

그림 4: 애플리케이션, 사용자 및 콘텐츠의 통제 정책을 신속하게 수립하고 배포할 수 있는 통합 정책 편집기

- 업무 관련 웹사이트에 대한 트래픽을 허용하고 감시하여 사용자의 웹 서핑을 통제하는 한편, 업무와 무관한 것이 확실한 웹사이트에 대한 액세스를 차단합니다. 의심스러운 웹사이트에 대한 액세스는 맞춤형 차단 페이지를 통해 지도합니다.
- P2P(peer-to-peer) 파일 전송 애플리케이션은 모두 동적 애플리케이션 필터를 통해 명시적으로 차단합니다.
- 귀사 내에서 사용되는 SaaS 애플리케이션을 파악하고, 각 애플리케이션에 대해 정밀한 액세스 및 이용 통제 수단을 구축하고, 이와 같은 애플리케이션을 통한 멀웨어 전송을 차단합니다.
- GlobalProtect™ 모바일 보안 서비스를 통해 인터넷 게이트웨이 정책 및 위협 방지 기능을 원격 사용자까지 확대하여 모바일 디바이스를 안전하게 사용할 수 있도록 합니다.

데이터센터에서 컨텍스트를 활용하여 데이터센터 애플리케이션이 표준 포트 상에서 실행되고 있는지 확인하고, 악성 애플리케이션을 찾고, 사용자를 검증하고, 데이터를 격리하고, 업무적으로 중요한 데이터를 위협으로부터 보호합니다. 예를 들면 다음과 같습니다.

- 보안 존을 사용하여 Oracle® 기반 신용카드 번호 리포지토리를 격리하여 Oracle 트래픽이 Oracle 표준 포트를 통해서만 이동하도록 하고, 트래픽을 검사하여 인바운드 위협이 존재하는지 확인하고 액세스를 금융 그룹으로 제한합니다.
- IT 부서만 데이터센터 내에서 사용할 수 있는 원격 관리 애플리케이션 그룹(예: SSH, RDP, Telnet)을 생성합니다.
- 가상 데이터센터에서, SharePoint® 가상 머신이 구축되거나 해체되거나 가상 환경에서 이전되는 경우 동적 개체를 사용하여 보안 정책 생성을 자동화합니다.

사용 가능한 애플리케이션 및 콘텐츠 보호

위협 방지 및 콘텐츠 검사 정책을 적용할 때, 애플리케이션 및 사용자 컨텍스트가 보안 정책의 필수 구성 요소가 됩니다. 위협 방지 정책에 컨텍스트를 전면적으로 적용함으로써 포트 호핑 및 터널링과 같은 우회 전술을 무력화합니다. 선택적 애플리케이션 사용을 구현하여 위협 표적 표면 영역을 축소하고 위협 방지 및 콘텐츠 검사 정책을 해당 트래픽에 적용합니다.

정책에 적용할 수 있는 위협 방지 및 콘텐츠 검사 요소는 다음과 같습니다.

- **IPS 및 네트워크 안티바이러스/안티-스파이웨어로 알려진 위협 방지.** 광범위한 알려진 위협으로부터의 보호는 통합 시그니처 형식 및 스트림 기반 검사 엔진을 사용하는 싱글 패스 검사를 통해 이루어집니다. Intrusion Prevention System(IPS) 기능으로 네트워크 및 애플리케이션 레이어 취약점 공격, 버퍼 오버플로, DoS 공격 및 포트 검사를 차단합니다. 안티바이러스/안티-스파이웨어 방지 기능을 통해 알려진 PDF 바이러스뿐만 아니라 압축 파일 또는 웹 트래픽(압축 HTTP/HTTPS)에 숨겨진 수백만 종의 멀웨어를 차단합니다. SSL로 암호화된 트래픽의 경우 정책 기반 복호화를 선택적으로 적용한 다음 포트에 상관없이 트래픽에 위협이 존재하는지 검사합니다.
- **WildFire로 알려지지 않은 멀웨어 및 표적형 멀웨어 차단.** 클라우드 내 가상화 샌드박스 환경이나 WF-500 어플라이언스에서 알려지지 않은 파일을 직접 관찰하고 실행하는 WildFire를 사용해 복수의 운영 체제 및 어플라이언스 버전에서 파일에 숨겨진, 알려지지 않았거나 표적형인 멀웨어(예: Advanced Persistent Threat(지능형 지속 위협, APT))를 식별하고 분석할 수 있습니다. WildFire는 420가지가 넘는 악성 행위를 감시하고, 멀웨어가 발견되는 경우 5분 이내에 시그니처가 자동으로 생성되어 귀하에게 전송됩니다. WildFire는 모든 주요 파일 형식을 지원합니다 (PE 파일, Microsoft Office의 .doc, .xls 및 .ppt 파일, PDF 파일, Java Applet(jar 및 class) 및 Android Application Package(APK)). 이에 더해, 이메일에 포함된 링크를 분석하여 잠재적 피싱 공격을 차단합니다.
- **봇 감염 호스트를 식별하고 멀웨어의 네트워크 활동 저지.** 네트워크를 이상 현상 및 위협에 노출시킬 수 있는 알 수 없는 트래픽을 포함한 모든 애플리케이션을 모든 포트에 걸쳐 상황에 맞게 완전하게 분류합니다. C2(Command and Control) App-ID™, 봇넷 거동 보고서, DNS 싱크홀링, 패시브 DNS를 통해 알려지지 않은 트래픽, 의심스러운 DNS 및 URL 쿼리와 감염된 호스트 간의 상관관계를 신속하게 파악합니다. 글로벌 위협 인텔리전스를 적용하여 악성 도메인에 대한 DNS 쿼리를 가로채 싱크홀링을 실행합니다.

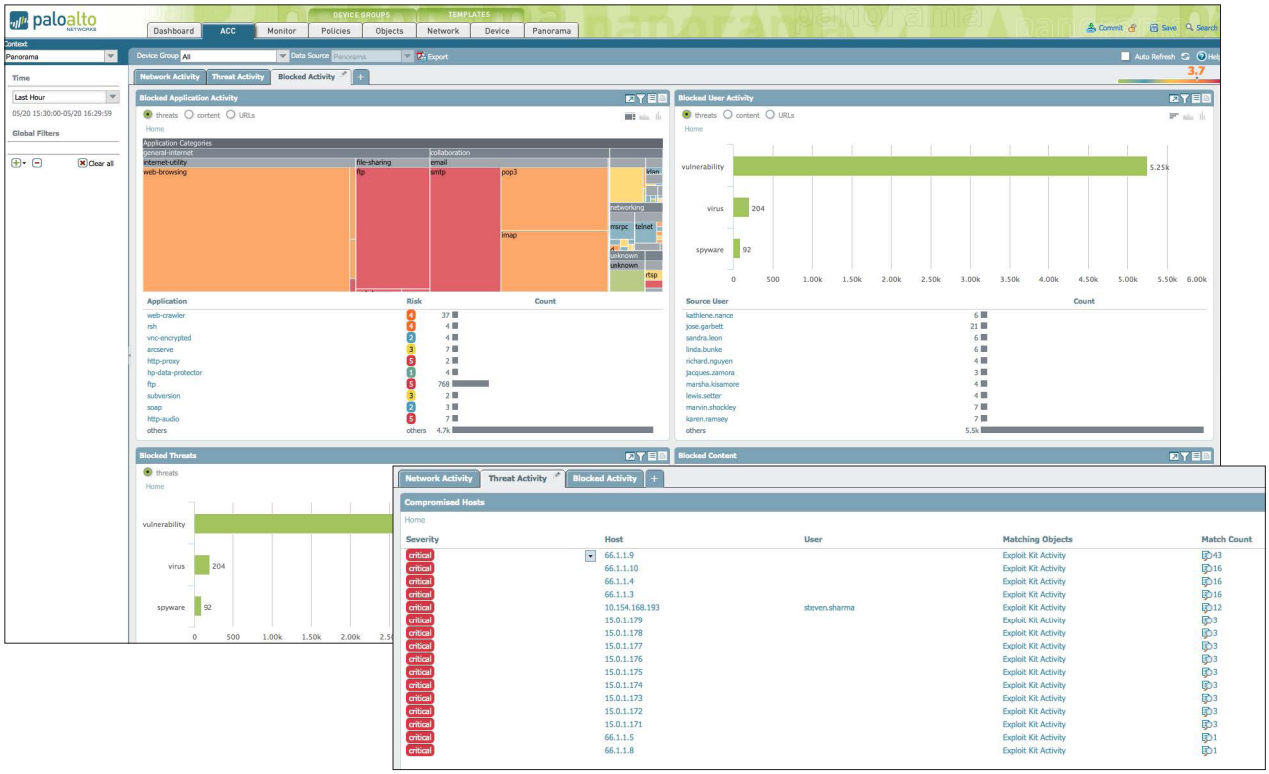

그림 5: 콘텐츠 및 위협 가시성 – 감염된 호스트와 더불어 URL, 위협 및 파일/데이터 전송 활동을 명확하고 파악하기 쉬우며 간편하게 맞춤화할 수 있는 형식으로 표시. 개별 요소에 대해 자세히 알아보려면 필터를 추가하거나 제거합니다.

- **인증되지 않은 파일 및 데이터 전송 제한.** 관리자는 데이터 필터링 기능을 사용하여 인증되지 않은 파일 및 데이터 전송에 수반되는 위험을 줄이는 정책을 구현할 수 있습니다. 단순히 파일 확장자만 검사하는 것이 아니라 파일 내용을 검사하여 전송 허용 여부를 결정함으로써 파일 전송을 통제할 수 있습니다. 일반적으로 드라이브 바이(drive-by) 다운로드에서 발견되는 실행 파일을 차단하여 미확인 멀웨어가 네트워크에 확산되지 않도록 막을 수 있습니다. 데이터 필터링 기능을 사용하면 기밀 데이터 패턴(신용 카드 번호 또는 주민등록번호, 사용자 정의 패턴 등)의 흐름을 탐지하고 제어할 수 있습니다.
- **웹 서핑 통제.** 관리자는 사용자 지정이 가능한 완전 통합형 URL Filtering 엔진을 사용하여 세부적인 웹 브라우징 정책을 적용함으로써 애플리케이션 가시성 및 제어 정책을 보완하고 법적 위험, 규제 위험, 생산성 위험으로부터 기업을 완벽하게 보호할 수 있습니다.
- **디바이스 기반 애플리케이션 액세스 정책.** GlobalProtect를 통해 세부 정책을 설정하여 특정 애플리케이션 및 네트워크 리소스에 액세스할 수 있는 디바이스를 통제할 수 있습니다. 예를 들어, 노트북 컴퓨터가 기업 이미지에 부합하는지 확인한 다음 데이터센터 액세스를 허용합니다. 모바일 디바이스가 민감한 데이터에 액세스할 때 먼저 해당 디바이스가 최신 상태인지, 회사 소유인지, 패치가 완전히 이루어졌는지 확인합니다.
- **감염된 호스트를 자동으로 확인.** 자동 연관성 확인 엔진이 네트워크 전반에 걸쳐 사전에 정의된 침해 지표를 확인하고, 일치 여부를 판단한 다음, 감염된 호스트를 자동으로 표시하여 수동 데이터 마이닝 작업의 필요성을 줄입니다.

네트워크 보안 관리

차세대 보안 플랫폼은 CLI(command-line interface)나 기능 일체가 탑재된 브라우저 기반 인터페이스를 통해 개별적으로 관리할 수 있습니다. 대규모 구축의 경우 Panorama™를 사용하여 모든 하드웨어 및 가상 어플라이언스 방화벽에 대해 가시성, 정책 편집, 보고 및 로깅 기능을 전체적으로 이용할 수 있습니다. Panorama는 전역 구축에 대해 단일 어플라이언스의 경우와 동일한 상황별 통제 수준을 제공합니다.

사전 및 사후 규칙과 통합된 역할 기반 관리 기능을 통해 중앙 집중식 통제와 로컬 수준에서의 편집 및 디바이스 구성 유연성 간에 균형을 도모할 수 있습니다. 디바이스의 웹 인터페이스와 Panorama의 웹 인터페이스가 모양과 느낌이 동일하므로 인터페이스를 전환할 때 시행착오를 겪지 않아도 됩니다. 관리자는 제공된 인터페이스를 사용하여 동기화 문제에 대한 걱정 없이 언제든지 변경할 수 있습니다. 또한 SNMP 및 REST 기반 API와 같은 표준 기반 도구가 추가로 지원되므로 타사 관리 도구와 연동할 수 있습니다.

보고 및 로깅

보안 모범 사례에 의하면 지속적인 관리와 대응(보안 사고 조사 및 분석, 일일 보고서 생성 등) 간에 균형을 이루는 것이 중요합니다.

- **보고:** 사전 정의 보고서를 그대로 사용하거나, 구체적인 요건에 따라 사용자 지정하거나, 하나의 보고서로 묶을 수 있습니다. 모든 보고서는 CSV 또는 PDF 형식으로 내보낼 수 있으며 예약 실행 및 이메일 전송이 가능합니다.
- **로깅:** 실시간 로그 필터링으로 네트워크의 모든 세션에 대해 간편하고도 신속하게 포렌식 검사를 할 수 있습니다.

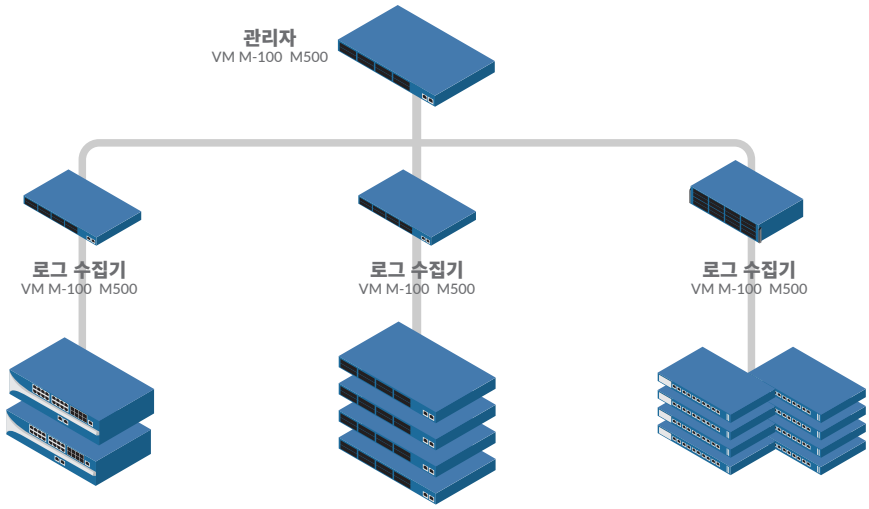

그림 6: 전용 어플라이언스에 또는 분산 방식으로 구축하여 확장성을 극대화할 수 있는 Panorama

애플리케이션, 콘텐츠(WildFire에 의해 탐지된 멀웨어 포함) 및 사용자 전체 컨텍스트를 필터 기준으로 사용하고, 그 결과를 오프라인 아카이브 저장 또는 추가 분석을 위해 CSV 파일로 내보내거나 syslog 서버로 전송할 수 있습니다. Panorama에 의해 취합된 로그 또한 추가 분석 또는 아카이브 보관을 위해 syslog 서버로 전송할 수 있습니다.

- **위협 헌팅:** PAN-OS에서 AutoFocus 서비스의 위협 인텔리전스에 직접 액세스할 수 있으므로, 추가적인 리소스 없이 위협 분석 및 위협 헌팅 워크플로를 가속화할 수 있습니다. 추가 분석이 요구되는 경우 사용자가 두 시스템에 대해 사전에 입력한 조사 결과를 바탕으로 AutoFocus와 PAN-OS 간에 스윕을 수행할 수 있습니다.

Palo Alto Networks의 차세대 보안 플랫폼에서 제공하는 보고 및 로깅 기능 이외에 Splunk®와 같은 타사 SIEM 도구와 Palo Alto Networks 솔루션의 통합 기능을 이용할 수 있습니다. 이와 같은 도구는 보고 및 데이터 시각화 기능을 보완해 주며 사내의 복수 시스템에 걸쳐 보안 이벤트의 상관성을 연결하도록 돕습니다.

특수 목적용 하드웨어 또는 가상화 플랫폼

Palo Alto Networks의 차세대 방화벽은 기업 지사에서부터 고속 데이터센터까지 확장할 수 있는 특수 목적용 하드웨어 플랫폼이나 클라우드 기반 컴퓨팅을 지원하는 가상화 폼 팩터 형태로 이용할 수 있습니다. Palo Alto Networks는 가상화 데이터센터, 퍼블릭 및 프라이빗 클라우드를 망라하는 가장 광범위한 가상 플랫폼을 지원합니다. VM-Series 방화벽 플랫폼은 VMware® ESXi™, NSX™, Citrix® SDX™, Microsoft Hyper-V®, Amazon® Web Services(AWS), Microsoft Azure™ 및 KVM 하이퍼바이저를 지원합니다. Palo Alto Networks 플랫폼을 하드웨어 또는 가상 폼 팩터 형태로 구축하는 경우 Panorama를 중앙식 관리 도구로 사용할 수 있습니다.

4401 Great America Parkway
Santa Clara, CA 95054

본사: +1.408.753.4000
영업 부서: +1.866.320.4788
고객 지원: +1.866.898.9087

www.paloaltonetworks.com

pan-next-generation-firewall-overview-ds-050616