요약

# MARSH가 CYBER CATALYST℠로 지정한 ARUBA POLICY ENFORCEMENT FIREWALL

네트워크가 디지털 혁신의 촉매제가 되면서 이제 기존의 경계 보안 방어로는 충분하지 않게 되었습니다. 모바일과 IoT 디바이스는 조직 내 어디에서나 직원, 파트너, 고객 및 게스트에 의해 연결되고 있으므로 특정 IT 액세스 권한에 기반한 트래픽 세분화 개선의필요성이 커지고 있습니다.

IP 주소에 기반을 둔 표준 보안 방화벽 규칙과 물리적 네트워크 구성으로는 이제 충분하지 않습니다. 이제 조직은 사용자 역할, 디바이스 유형 또는 위치에 상관없이 동적으로 적용되는 에지 기반 보호가 필요합니다.

아루바는 특히 이 문제를 해결하는 데 도움이 되는 Policy Enforcement Firewall(PEF)이라는 포괄적인 역할 기반 액세스 제어 솔루션을 최초로 개발하였습니다. 이 입증된 기술은 액세스 시점에 "제로 트러스트" 경계를 제공하는 유일한 사용자 및 디바이스 중심 방화벽으로서, Marsh가 위험 저감 효과를 인정하여 Cyber Catalyst℠로 지정하였습니다.

## 잠재적 비즈니스 손실 및 영향 방지

인터넷 및 클라우드를 통한 모바일 기술 및 트랜잭션은 조직이 현재 비즈니스를 수행하고 잠재 고객을 발굴하는 방법에 중요한 역할을 하고있습니다. 안타깝게도 이것은 공격 영역에 추가됩니다. 조직은 적절한 보안 상세, 수용가능하거나 피할 수 있는 위험,재정적 책임에 감수할 의사가 있는지에 대해결정을 내려야 합니다.

기술, 프로세스 및 사람 외에도 사이버 보험은 조직의 규모를 막론하고 사이버 보안의 핵심 요소가 되었습니다. 실제로 버라이존(Verizon)이 최근에 배포한 보고서에 따르면 전체 사이버 공격의 약 43%는 중소기업(SMB)이 대상인 것으로 나타났습니다.
또한 조직은 기밀 정보 유출이나 랜섬웨어로 인한 강탈 비용과 관련된 소송과 싸워야합니다.

## MARSH 프로그램의 CYBER CATALYST℠란?

Cyber Catalyst℠ 프로그램의 일환으로 선도적인 사이버 보험사는 사이버 위험을 줄이는 데 효과적이라고 생각하는 솔루션을 평가하고 식별합니다. 참여 보험사는 Allianz, AXIS, AXA XL(AXA의 사업 부문), Beazley, CFC, Munich Re, Sompo International, Zurich North America입니다. Microsoft는 이 프로그램의 기술 자문입니다.

사이버 위험을 줄이는 데 효과적인 것으로 간주되는 사이버 보안 제품 및 서비스는 “Cyber Catalyst℠”로 지정됩니다. Cyber Catalyst로 지정된 솔루션을 채택하는 조직은 참여 보험사의 강화된 사이버 보험 정책 약관에 합당한 자격을 갖출 수 있습니다.

Aruba Policy Enforcement Firewall 및 HPE 서버 Silicon Root of Trust (SiROT) 는 Cyber Catalyst℠로 지정되었습니다.

## 제로 트러스트 보호를 위한 역할 기반 제어

제어를 위해 IP 기반 VLAN을 활용하는 기존 방화벽은 사용자 또는 디바이스가 네트워크의 승인을 받은 후에만 활성화되므로 지능형 공격의 좋은 먹잇감이 됩니다.
아루바의 PEF 기술은 ID, 트래픽 속성, 기타 컨텍스트를 사용하여 초기 연결 시점에 중앙에서 액세스 권한을 시행합니다. 이것이 중요한 이유는 공격자가 널리 개방된 네트워크에 연결될 때마다 수천 개의 악성프로그램패킷을 방출하여 사용자 자격증명을 획득하고 악성프로그램 공간 및 기타 파괴적인 활동을 확장할 수 있기 때문입니다.
디바이스가 연결될 때와 정책이 시행될 때 사이의 간격을 메우는 것이 필수적입니다.

아루바의 유무선 인프라를 사용할 때 각 사용자 또는 디바이스의 ID를 확인한 후 네트워크 또는 리소스에 액세스할 수 있는 권한을 부여합니다. 미리 정의된 규칙에 따라 역할이 할당되고 권한이 부여됩니다. 이로써 사용자 또는 디바이스가 접근하거나 커뮤니케이션할 수 있는 애플리케이션 및 데이터가 제한됩니다. 예를 들어 감시 카메라는 콘텐츠 다운로드 시 비디오 서버와만 커뮤니케이션하도록 허용됩니다.

데이터 반출 또는 랜섬웨어와 같은 공격이 감지되면 PEF는 역할 및 권한부여 권한을 업데이트하여 사용자 또는 디바이스와 연결된 권한을 자동으로 변경할 수 있습니다. 공격 대응에는 대역폭 축소, 검역에서 전면 차단에 이르는 다양한 조치가 포함될 수 있습니다. 공격에 대한 경고는 단순 API 통합에 따라 조직의 보안 생태계 내 어느 보안 제품에서도 트리거될 수 있습니다.

PEF는 온프레미스 또는 클라우드 기반 관리 콘솔에서 관리되며 Aruba 네트워킹 인프라와 함께, 또는 독립형 보안 게이트웨이를 통해 번들로 제공됩니다.

Aruba Policy Enforcement Firewall은 조직이 제로 트러스트 역할 기반 액세스 제어를 구현할 수 있게 지원함으로써 위험을 효과적으로 줄일 수 있는 능력에 근거하여 “Cyber Catalysts℠”로 지정되었습니다. 자세한 내용은 Cyber Catalyst 프로그램, Aruba PEF 및 HPE SiROT에 관한 다음 리소스를 참조하십시오.

## 추가 리소스

- Aruba Policy Enforcement Firewall
- HPE 서버
- Marsh가 Cyber Catalyst로 지정

Cyber Catalyst℠ 프로그램에서 선도적인 사이버 보험사는 사이버 위험을 줄이는 데 효과적이라고 생각하는 솔루션을 평가하고 식별합니다. 참여 보험사는 Allianz, AXIS, AXA XL(AXA의 사업 부문), Beazley, CFC, Munich Re, Sompo International, Zurich North America입니다. Microsoft는 이 프로그램의 기술 자문입니다.

a Hewlett Packard Enterprise company



AAG_CyberCatalyst_090919 a50000156enw