Hewlett Packard Enterprise

비즈니스 백서

IT 인프라 보안에 대한 종합적인 시각

목차

2016년 사이버 공격으로 인한 기업의 비용은 4,500억 달러에 달했습니다. 인프라 및 DC 시스템, 데이터 스토리지 및 백업, 인텔리전트 에지를 위한 네트워크 액세스, 공급망, 서비스 등 기술 스택 전체에 HPE의 표준 기반 보호 정책과 통합 제어를 사용하면 걱정할 일이 전혀 없습니다.

사이버 위협 때문에 불안하십니까? 실리콘과 펌웨어 계층에서 시작하여 공급망, 제조 공정, 개발 환경, 하드웨어, 데이터 센터, 클라우드를 거치는 HPE의 보안 접근 방식으로 탁월한 대응 능력을 갖추십시오.

소개

HPE 인프라 기술 및 서비스는 기업이 데이터와 애플리케이션에서 수익을 창출하는 시간을 앞당겨 줍니다. 기업들은 HPE 서버와 스토리지 시스템, 네트워크 액세스 제품을 이용하여 온프레미스 및 하이브리드 클라우드 환경에 미션 크리티컬 워크로드를 배포하고 관리합니다.

이 백서에서 HPE가 애플리케이션과 고객 데이터를 보호하는 방법을 Jaikumar Vijayan이 설명합니다. HPE는 실리콘과 펌웨어 계층에서 시작하여 공급망, 제조 공정, 개발 환경, 하드웨어, 데이터 센터, 클라우드로 이동하는 접근 방식을 취합니다.

디지털 인프라가 손상되거나 중단되지 않도록 보호해야 한다는 고객과 소비자, 규제 당국의 압력은 날로 커지고 있습니다. 공격은 갈수록 정교해지고 위협 요인은 더욱 영리하면서도 조직적으로 접근하고 있으므로 정보 보안 실패가 미치는 영향은 정보 및 재정적 손실 측면에서 훨씬 더 중요해졌습니다.

2016년에는 사이버 공격으로 인해 발생한 기업 비용이 전 세계적으로 4,500억 달러에 이르렀으며,[1] 20억 건이 넘는 개인 정보가 도난당했습니다. 2016년 Cybersecurity Ventures의 보고서에 따르면 2021년에는 사이버 범죄로 인한 손실액이 6조 달러에 달할 전망입니다.[2] 여기에는 데이터 파기와 도난, 생산성 손실, 지적재산 분실, 개인정보와 재무 정보의 도난, 침해 복구 비용, 명성 손상 등이 포함됩니다.

Ponemon Institute의 연구 결과 사이버 범죄로 인한 기업의 평균 비용은 2015년 380만 달러에서 2016년 400만 달러로 늘었습니다.[3] 혁신적인 기업일수록 손실액이 큰 경향이 있는데, 이런 기업들의 2016년 평균 손실액은 950만 달러입니다.[4]

사이버 공격은 이제 더 이상 OS와 애플리케이션만을 대상으로 삼고 있지 않습니다. 데이터베이스, 펌웨어, 커널 및 하드웨어 수준에서도 공격이 발생하고 있는데, 펌웨어 수준의 공격이 특히 문제입니다. 오늘날 대부분의 하드웨어에서는 OS가 부팅을 하기도 전에 수백만 줄의 펌웨어가 작동합니다. 공급망 펌웨어나 런타임 시 혹은 물리적인 액세스를 통해 악성 코드를 두 줄만 심어도 데이터를 훔치고 서비스 거부 상황을 초래하며 전체 시스템의 무결성을 손상시킬 수 있습니다.

본 백서는 여러 부분으로 나누어 HPE가 다음 계층에서 실행하는 보안 관리를 설명합니다.

1. 인프라 및 데이터 센터 시스템
2. 미션 크리티컬 솔루션
3. 데이터 스토리지 및 백업
4. 인텔리전트 에지에서 보안 네트워크 액세스
5. 공급망
6. HPE Pointnext

이 백서는 실리콘 계층에서 시작하는 기술 스택이 인터넷 규모 워크로드의 구축, 배포, 실행, 관리에 대한 표준 기반 보안을 지원하도록 보장하는 HPE의 노력을 알릴 목적으로 제작되었습니다. 국립 표준기술원(NIST) 사이버 보안 프레임워크에서 규정한 방식으로 조직이 보안 사건을 식별, 보호, 탐지, 대응 및 복구할 수 있도록 제품에 통합된 통제 측면에 중점을 둡니다.

[1] "**Cybercrime costs the global economy $450 billion: CEO**," CNBC, 2017

[2] "**Hackerpocalypse: A Cybercrime Revelation**," Cybersecurity Ventures, 2016

[3] "**Data Breaches Now Cost $4 Million on Average**," Fortune.com, Time Inc., 2016

[4] "**2016 Cost of Cyber Crime Study & the Risk of Business Innovation**," Sponsored by Hewlett Packard Enterprise, conducted by Ponemon Institute, 2016

인프라 및 데이터 센터 시스템

하이브리드 IT 환경을 위한 HPE 클라우드 중심 시스템

하이브리드 IT 환경은 퍼블릭 클라우드 인프라 및 서비스를 온프레미스 프라이빗 클라우드 및 전용 컴퓨팅 리소스와 결합하여 사용합니다. 기업들은 하이브리드 IT 환경에서 퍼블릭 클라우드의 경제성과 유연성, 그리고 온프레미스 인프라의 보안과 통제를 모두 누리면서 미션 크리티컬 워크로드를 제공할 수 있습니다.

HPE ProLiant Gen10 시스템을 비롯한 HPE의 업계 표준 서버 포트폴리오는 하이브리드 IT와 기존 인프라의 보안을 책임지는 방식을 나타냅니다. 하이브리드 클라우드 설정에서 중요한 엔터프라이즈 워크로드를 보안 위협으로부터 보호하고 보안 위협을 탐지하며 대응 및 복구하기 위해 서버가 실리콘 수준부터 시작하여 다양한 기술을 통합합니다.

다음 내용에서는 이러한 일부 통제 방법에 대해 설명하고 있습니다.

- **실리콘 RoT**—HPE 서버는 각 서버의 실리콘에 실리콘 RoT(Root of Trust)라 부르는 고유한 디지털 지문이 포함된 업계 표준 시스템입니다. RoT는 특정 보안 기능을 확인하고 다른 기능의 무결성을 테스트 및 확인할 수 있는 기능을 제공합니다. 이렇게 하면 펌웨어가 손상되었거나 조작된 경우 서버가 부팅되지 않습니다. 시스템 펌웨어는 RoT에 기반하므로 공격하는 쪽에서 전체 UEFI(Unified Extensible Firmware Interface)와 HPE iLO(Integrated Lights Out) 코드를 대체하더라도 시스템이 부팅되지 않습니다. 오늘날의 많은 컴퓨터에서는 시스템 부팅 시 실행되는 첫 번째 모듈로 UEFI가 BIOS를 대체했습니다. iLO는 HPE의 원격 서버 관리 기술입니다.
- **런타임 펌웨어 검증**—HPE Gen10 서버는 주요 시스템 펌웨어를 런타임 보호하는 위협 탐지 기능을 지원합니다. 부팅 중에 보안 점검 과정을 수행하는 HPE iLO 칩셋은 서버가 작동하는 동안에도 지속적으로 동일한 검증 작업을 계속합니다. 실리콘 RoT가 적용된 HPE iLO 칩셋이 매일 HPE iLO 펌웨어와 UEFI BIOS를 점검하므로 고객이 펌웨어 손상을 신속하게 탐지할 수 있습니다.

- **손상된 펌웨어에서 안전하게 복구**—펌웨어 문제가 탐지될 경우 관리자는 해당 펌웨어를 마지막으로 알고 있는 정상 상태 또는 공장 기본 설정으로 복원할 수 있습니다. 드물지만 펌웨어가 손상된 경우에는 HPE iLO 칩셋이 비휘발성 메모리에 저장된 통합 백업에서 인증된 펌웨어를 자동으로 로드합니다. 시스템 펌웨어가 손상된 경우 HPE iLO는 백업본에서 복구를 시도하거나 관리자에게 알립니다.
- **데이터 보호**—Hewlett Packard Enterprise는 CNSA(Commercial National Security Algorithms)를 지원합니다. CNSA는 미국 연방기관이 일급비밀을 비롯한 국가보안시스템(NSS)을 보호하는 데 사용하는 암호화 알고리즘 모음으로, NSS에 사용할 제품을 개발하는 업체에서도 사용합니다. 가장 민감한 데이터를 보호하도록 설계된 높은 수준의 보안입니다. 과거에 미국 국가안전국(NSA)이 NSS 보호에 사용하던 Suite B 암호도 CNSA로 대체되었습니다.[5]
- **TPM**—HPE 서버는 암호화 키와 디지털 인증서, 플랫폼 인증과 플랫폼 실행 소프트웨어 확인에 사용되는 암호를 저장하기 위해 TPM(Trusted Platform Module) 1.2 및 2.0 기술을 지원합니다. 또한 TPM 모듈과 계획된 부팅 프로세스는 OS 초기화 과정을 모니터링하고 OS를 안전하게 시작하기 위해 함께 사용됩니다.
- **물리적 손상으로부터 보호**—섀시 침입 탐지 및 랙 캐비닛 도어 탐지 제어를 통해 물리적으로 조작하려고 하거나 허가 없이 서버에 액세스하는 경우 경고합니다. 섀시 보드와 후드에 물리적으로 연결되어 있어 섀시에 대한 물리적인 침입을 탐지하며 HPE 시스템의 출고, 입고, 유통, 작동 중에도 보안을 제공합니다.
- **제품 무결성과 품질 보증**—HPE 서버와 스토리지, 네트워크 제품에 적용되는 업계 최고의 보안 관리 및 보안 혁신 사항은 FIPS 140-2, 연방 정보보안관리법(FISMA), 연방 위험 및 인증관리 프로그램(FedRAMP), Common Criteria 인증과 같은 연방 표준을 준수합니다.

  HPE 하드웨어 제품에 적용된 업계 표준은 UEFI Secure Boot, CRTM(Core Root of Trust Measurement), TPM 1.2 및 2.0 등입니다.
- **참조 아키텍처와 구성**—Hewlett Packard Enterprise는 참조 아키텍처와 구성을 사용하여 다양한 하이브리드 IT 플랫폼에 완전하고 믿을 수 있으며 완벽하게 검증된 인프라 구성을 구현합니다.

  안전하고 규정에 맞는 백업 및 복제를 위한 HPE 참조 아키텍처와 **Micro Focus SecureData를 사용한 HPE Helion CloudSystem Enterprise 보안용 HPE 참조 구성** 참조 아키텍처는 워크로드 테스트를 거친 반복 가능한 구성을 제공합니다. 엔터프라이즈 고객 환경에서 수년 간의 경험을 통해 개발한 보안 기능이 함께 제공됩니다.

  참조 아키텍처를 사용하면 다양한 워크로드 요건에 맞게 인프라를 계획하고 실행해야 하는 기술적 복잡성이 크게 줄어듭니다.

[5] cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf

미션 크리티컬 솔루션

조직에서는 HPE 미션 크리티컬 시스템을 사용하여 대규모 트랜잭션 처리, 일괄 처리, 데이터베이스 및 분석 애플리케이션을 실행합니다. HPE의 미션 크리티컬 시스템 포트폴리오는 HPE NonStop, HP-UX, OpenVMS, Linux®, Windows®, VMware® 운영 환경이 실행되는 HPE Integrity 서버에 구축되었습니다.

HPE NonStop

HPE NonStop 시스템은 은행, 통신사, 운송업체, 기타 다양한 부문에서 내결함성 컴퓨팅 성능을 제공합니다. 이 시스템은 고가용성, 기밀성, 무결성 요건이 높은 중요한 워크로드를 실행합니다. HPE NonStop 고객들은 데이터 보호 권한이 복잡하고 엄격한 규제가 적용되는 업종인 경우가 많습니다. HPE NonStop 서버는 다음과 같이 다양한 방법으로 이러한 요구사항을 충족합니다.

- **강력한 액세스 관리**—HPE NonStop OS의 Platform과 Safeguard 계층은 시스템 최하위 수준에서도 인증과 권한 부여, 사용자 관리, 액세스 관리 서비스를 제공합니다. 사용자와 그룹, 개체가 최소한의 필수 액세스만으로 데이터와 시스템 리소스를 이용하도록 만들어 내부자에 의한 도난과 데이터 오용을 방지합니다. 모든 사용자 암호는 자격 증명 도난과 오용을 방지하도록 암호화 형식으로 저장됩니다. 또한 역할 기반 액세스 제어(RBAC) 또는 SEEP(Security Event Exit Process) 지원과 같은 확장 기능도 있습니다.
- **시스템 수준의 피해 방지**—애플리케이션은 권한이 없는 사용자 모드에서 실행됩니다. 시스템에서 인증되지 않은 애플리케이션이나 루트킷, 기타 맬웨어가 실행될 위험을 줄이기 위해 정해진 절차를 통해서만 권한 있는 커널 기능을 호출할 수 있습니다.
- **허가되지 않은 시스템 액세스 및 설정 변경 제어**—Safeguard 구성요소가 로그인 시도, 개체 액세스, 보안 설정 변경, 기타 중요한 보안 이벤트를 모니터링하고 감사합니다. 보안 관리자와 감사자는 이러한 툴을 사용하여 포렌식 활동을 모니터링하고 수행하여 보안 이벤트를 조사할 수 있습니다.
- **저장 및 전송 데이터 암호화**—HPE의 VLE(Volume Level Encryption)와 Secure Tape 제품은 디스크나 백업 스토리지 장치에 저장된 데이터도 암호화합니다. NonStop 시스템이 제공하는 디스크 삭제 툴로 필요할 때 데이터를 스토리지 장치에서 삭제할 수 있습니다. 전송 계층에 있는 데이터의 엔드 투 엔드 암호화에 SSH(secure shell) 및 SSL(Secure Sockets Layer) 프로토콜을 이용합니다.

  엄격한 감사 관리와 사용자 인증 같은 보안 요건을 충족하기 위해 ISV와 긴밀하게 협력합니다.
- **규정 준수 보고 지원**—HPE의 XYGATE Compliance PRO는 PCI와 같은 규정 요건을 준수함을 입증하는 GUI 기반의 인터페이스 및 보고 템플릿입니다. 위 제품 외에도 HPE NonStop의 다른 보안 제품을 통해 키 입력 로깅, 다중 인증, 통합 애플리케이션 로그, NonStop 환경을 보호하는 기타 솔루션 등 여러 메커니즘을 통해 고객 환경을 안전하게 보호합니다.

HP-UX를 실행하는 HPE Integrity 서버

글로벌 은행과 제약사, 통신사 및 기타 많은 조직에서는 HP-UX를 실행하는 HPE Integrity 서버를 사용하여 미션 크리티컬 워크로드를 실행합니다. HPE Integrity 서버는 다양한 기술로 위협을 방어하고 탐지하며 대응합니다.

- **파일 및 디스크 수준 암호화**—Hewlett Packard Enterprise는 허가된 애플리케이션만 사용자 파일 및 데이터에 액세스할 수 있도록 다양한 암호화 기술을 제공합니다. 파일 수준 및 디스크 수준의 암호화뿐만 아니라 데이터에 대한 위협이 제기되기 전에 손상된 애플리케이션을 격리하는 HP–UX 11i Security Containment 기술을 허용하는 HP-UX 화이트리스팅 기능도 지원합니다.
- **호스트 침입 탐지**—관리자는 HP-UX HIDS(Host Intrusion Detection System)를 사용하여 HP-UX 시스템의 공격과 침입을 모니터링하고 탐지하며 대응할 수 있습니다. 예를 들어 HP-UX HIDS는 시스템 활동을 모니터링하다가 의심스럽거나 악의적인 행동을 암시하는 패턴을 탐지하면 해당 활동에 대한 경고를 생성합니다.
- **역할 기반 액세스 제어**—HP-UX 환경에서 신원을 보호하기 위해 역할 기반 액세스 제어, 기존 LDAP(Lightweight Directory Access Protocol) 기반 ID 관리 인프라와의 통합, 중앙 인증, 권한 부여, RADIUS(Remote Authentication Dial-In User Service) 프로토콜을 사용하는 미들웨어 및 애플리케이션을 통한 계정 관리를 지원합니다.
- **Common Criteria 인증**—Common Criteria 인증을 비롯한 업계 인증은 HP-UX 보안 모델을 독립적으로 검증하고 HP-UX 사용자의 보안 요건을 해결하기 위한 HPE 전략의 네 번째 구성요소입니다.

HPE Integrity Superdome X

글로벌 제조사와 리테일, 통신사, 의료, 금융기업은 Superdome X를 통해 중요한 비즈니스 처리 및 분석 워크로드를 수행합니다. 이 서버에서 처리하는 민감한 데이터와 프로세스를 보호하기 위해 Superdome X는 다양한 보안 기술을 갖추고 있습니다.

- 인증된 업데이트: 시스템을 업데이트하기 전에 펌웨어 업데이트가 디지털 서명을 확인합니다. Superdome X 펌웨어 업데이트 과정은 완전히 안전하며, 보안 프로토콜로 보호되고 Superdome X 엔클로저의 모든 구성요소용 펌웨어가 디지털 서명 번들에 포함되어 있어 보호 기능을 극대화합니다. 펌웨어 업데이트에 보안 HPE 서명과 서명 확인을 사용합니다. 검증 작업이 실패하면 업데이트가 중단되고 프로그래밍된 펌웨어는 변경되지 않은 상태로 남습니다.
- 신뢰할 수 있는 호스트 기능과 역할 기반 액세스 제어: Superdome X Onboard Administrator 네트워크의 액세스 권한을 IPv4 주소 5개 이하로 제한할 수 있으며, 하드웨어와 파티션에 액세스하는 역할 기반 액세스 제어가 있습니다. 구성 가능한 강력한 암호 수행과 최소 암호 길이가 포함됩니다.
- 안전한 개발: 프로덕션 공정을 지원하는 모든 인프라는 맬웨어 침입 위험을 최소화하기 위해 동적으로 관리되는 바이러스 검사 소프트웨어를 사용합니다. 제조 공정 중에 펌웨어와 소프트웨어 패키지에서 맬웨어 및 바이러스 검사를 수행한 다음 HPE 사이버 보안 과정에서 디지털로 서명하여 펌웨어 또는 소프트웨어 조작이 불가능함을 확인합니다.
- 기타 보안 기능에는 인증서 관리, 중앙 암호화 설정, 중앙 사용자 관리, 보안 툴(Secure Out-of-Box), 감사 로그, 이중 보안 등이 있습니다.

데이터 스토리지 및 백업

이 단원에서는 엔터프라이즈의 데이터 스토리지 및 백업 보안 요건을 충족하기 위해 HPE 3PAR StoreServ 스토리지 어레이 시스템과 HPE StoreOnce 중복 제거 어플라이언스가 실행하는 조치를 설명합니다.

HPE 3PAR StoreServ 스토리지 어레이 시스템

HPE 3PAR StoreServ 블록 스토리지는 권한 부여, 인증, 가용성, 암호화, 무결성, 감사 용이성의 6가지 요인을 기준으로 구축됩니다.

- HPE 3PAR에는 이러한 보안 원칙과 기능이 모두 포함되어 있습니다. HPE 3PAR의 중요한 몇 가지 보안 기능은 다음과 같습니다.
  - **자체 암호화 드라이브**—HPE 3PAR StoreServ 시스템은 데이터를 확실히 보호하기 위해 사용자 개입 없이 드라이브에 쓰는 데이터를 암호화하는 자체 암호화 드라이브로 구성됩니다.
  - **저장 데이터 암호화 인증**—엔드 투 엔드 T10-DIF 오류 검사와 함께 FIPS 140-2 레벨 검증 암호화로 저장 데이터의 무결성을 보호합니다.
  - **FIPS 인증 키 관리**—HPE 3PAR StoreServ 스토리지는 온프레미스와 클라우드에서 모두 엔터프라이즈 데이터 보호 요건을 충족하기 위해 로컬 및 외부 FIPS 인증 키 관리를 지원합니다.
  - **인증서 기반 사용자 인증**—HPE 3PAR StoreServ 스토리지 시스템은 스토리지에 액세스하는 사용자 및 애플리케이션에 대한 LDAP 및 X.509 인증서 기반 인증을 지원합니다.
- **HPE StoreOnce 시스템**—HPE StoreOnce 시스템은 중요한 엔터프라이즈 데이터를 안전하게 백업하고 공격이나 다른 중단 문제가 발생할 경우 쉽게 복구할 수 있도록 합니다.

  HPE StoreOnce 시스템은 저장 데이터를 보호하기 위해 NIST FF1 AES-256비트 암호화를 구현합니다. 일부 모델은 IPSec을 통한 전송 데이터 암호화를 지원합니다. 또한 HPE StoreOnce의 보안 삭제 기능은 NIST SP 800-88 미디어 삭제 가이드라인을 준수하며 최대 7단계를 통해 민감한 데이터 삭제를 지원합니다.
- **확장 가능 암호화**—HPE 확장 가능 암호화 기술은 서버에 저장된 데이터를 보호하는 차별화된 기능입니다. 각 드라이브에서 별도의 키를 관리해야 하는 자체 암호화 드라이브를 사용하는 경쟁 업체의 서버와 달리 Hewlett Packard Enterprise는 암호화 카드가 포함되고 대규모로 관리할 수 있는 HPE Smart Array 컨트롤러 카드를 통해 신뢰할 수 있는 암호화를 제공합니다.
- **전략적 파트너십**—파트너와의 협력을 통해 데이터 스토리지 및 백업 기능을 확장하고 개선합니다. 전략적 파트너십의 예는 다음과 같습니다.
  - **Veeam**—HPE 3PAR StoreServ와 Veeam Backup & Replication 소프트웨어 통합을 통해 가상화된 미션 크리티컬 환경의 데이터 보호와 복구 시간을 개선합니다.
  - **Veritas**—HPE StoreOnce와 Veritas NetBackup의 통합으로 고속 데이터의 고가용성 복원 및 재해 복구성이 개선됩니다.
  - **Arista**—Arista 데이터 센터 스위치는 HPE 스토리지, 서버, 관리 제품에서 작동하여 컨버지드 인프라 구현을 지원합니다.
  - **Scality**—미디어, 금융, 정부, 기타 부문에서 소프트웨어 정의 개체 스토리지를 최적화합니다.
  - **Cohesity**—2차 워크플로를 통합하려는 조직에게 사전 검증과 사전 구성이 완료된 웹 규모의 스토리지 옵션을 제공합니다.
  - **Micro Focus**—Micro Focus는 기존의 비즈니스 로직과 애플리케이션을 신기술로 통합하는 IT 시스템을 구축, 운영 및 보호하는 글로벌 소프트웨어 회사입니다.

인텔리전트 에지에서 보안 네트워크 액세스

Hewlett Packard Enterprise 솔루션을 이용하는 조직은 IoT와 엔터프라이즈 모빌리티의 비즈니스 장점을 안전하게 활용할 수 있습니다.

Aruba 360 Secure Fabric의 소프트웨어 구성요소인 HPE Aruba IntroSpect UEBA(User and Entity Behavior Analytics) 기술과 HPE Aruba ClearPass 툴을 통해 사용자와 시스템, 스마트폰, 태블릿, 기타 IoT 장치를 식별, 연결, 보호, 관리할 수 있습니다.

HPE의 360 Secure Fabric 기능은 가시성, 제어 및 모니터링을 네트워크 에지에서 공격 탐지, 경고 및 대응력과 결합합니다. 엔드포인트 장치가 안전하게 네트워크에 액세스하는 방법을 몇 가지 예로 설명하겠습니다.

HPE Aruba ClearPass를 이용한 보안 액세스 제어
HPE Aruba ClearPass는 멀티벤더 IoT 세계에 역할 기반, 장치 기반 네트워크 액세스 제어를 제공합니다.

장치 인증 및 권한 부여
HPE Aruba ClearPass는 유무선 네트워크에서 사용 중인 장치를 식별하고 인증하며 권한을 부여합니다. 네트워크에 연결된 개별 장치의 종류와 OS, 기타 속성 같은 정보를 실시간으로 수집합니다.

정책 적용
HPE Aruba ClearPass Policy Manager를 통해 네트워크에서 사용하는 장치에 대해 보안 위반이 발생할 경우 완전 격리와 같은 매우 세분화된 상황 인식 보안 정책을 적용합니다.

HPE Aruba IntroSpect를 사용한 고급 공격 탐지
HPE Aruba IntroSpect는 온프레미스 및 클라우드 호스팅 UEBA 기능을 제공하여 기존의 보안 툴을 피한 사용자, 시스템, 장치에 대한 공격을 나타내는 비정상적인 행동을 탐지합니다.

엔드포인트 위협 탐지
HPE Aruba IntroSpect는 감시 방식과 자율식 기계 학습을 사용하여 내부자 위협과 외부 공격을 탐지하고 네트워크에서 정상적인 사용자 및 엔터티 동작을 기준으로 판단한 다음 이러한 동작의 차이를 확인합니다.

HPE Aruba IntroSpect 독립 UEBA 기술은 네트워크와 IT 로그 정보를 모두 사용하고 분석하여 네트워크에서 변칙적이며 잠재적으로 유해할 수 있는 행동을 식별합니다.

다층 엔드포인트 보호
HPE Aruba ClearPass와 HPE Aruba IntroSpect를 같이 사용하면 IoT 환경에 대한 취약성과 위협을 완화하는 고급 공격 탐지와 신속 대응 기능을 제공할 수 있습니다.

HPE Aruba IntroSpect는 IT 환경의 내부와 외부 위협을 탐지합니다. HPE Aruba ClearPass는 지정된 정책과 HPE Aruba IntroSpect의 공격 경고 데이터, 보안 생태계의 기타 제품을 기반으로 네트워크에 대한 엔드포인트 액세스를 제어합니다.

공급망

공급망이 취약하면 제조, 창고 보관, 운송, 사전 배포 단계에 위조 부품이나 악성 소프트웨어가 들어올 수 있습니다. 위협 범위에는 공급망에 유입된 손상된 장치를 통해 간첩 행위를 하는 민족 국가 행위자와 서비스 거부 캠페인이 포함됩니다.[6]

한 가지만 취약해도 재앙으로 이어질 수 있습니다. 예를 들어 2016년 Apple은 맬웨어에 감염된 펌웨어가 최소 하나의 서버에 로드되었다는 사실을 발견한 후 타 벤더에서 공급한 여러 서버로 구성된 데이터 센터를 제거해야 했습니다.[7]

HPE는 이러한 조작을 방지하고 공급망 수명주기에 걸쳐 제품 무결성을 유지하기 위해 다음과 같은 여러 가지 대책을 시행하고 있습니다.

표준 및 평가

HPE 제품 및 서비스의 공급자는 정책과 업계 관행을 바탕으로 한 여러 표준과 자체 평가를 따라야 합니다. DFARS(Defense Federal Acquisition Regulation Supplement)와 ISO가 이러한 표준에 해당합니다.

컴플라이언스에 대한 증거로는 위험 기반 보안 감사, 정기적인 프로그램 모니터링 및 보고, 전자 부품의 검사 및 시험, 구성 부품 추적 가능성, 오염 부품의 격리 및 제거가 포함된 원료 관리 공정 등이 있습니다. 공급자의 배송 및 물류 공정은 C-TPAT(Customs—Trade Partnership Against Terrorism) 또는 Hewlett Packard Enterprise에서 정한 유사 프로세스를 충족해야 합니다.

펌웨어 보호 표준

Hewlett Packard Enterprise는 NIST BIOS 서버 보호 가이드라인과 ISO 공급망 보안 관리 시스템 사양 등의 표준을 채택하고 준수하여 펌웨어 오염, 손상, 위조, 대체 등의 위험을 완화합니다.

출처, 조달, 원산지, 추적 가능성

Hewlett Packard Enterprise 하드웨어의 프로그래밍형 논리 구성요소는 원산지, 공급자 이름, 적합성 인증 등을 비롯하여 완전한 제품 및 부품 추적이 가능합니다. 그리고 공급자에게도 동일하게 요구합니다.

맞춤형 실리콘과 HPE iLO 펌웨어 제어

HPE는 실리콘 RoT의 핵심인 맞춤형 HPE 실리콘과 HPE iLO 펌웨어를 구축하여 완전한 제어권을 갖습니다. 이를 통해 공급망에서 조작될 가능성이 크게 줄어듭니다.

보안 클린룸

HPE는 보호된 클린룸을 사용하여 시스템에 들어가는 모든 펌웨어에 디지털로 서명합니다.

하드웨어 섀시를 완전히 제작한 다음 뚜껑을 닫고 밀봉합니다. 섀시가 열렸는지 여부를 내부 스위치가 기록하기 때문에 최근 몇 년 동안 일부 국가와 정부에서 논란이 되었던 은밀한 조작을 탐지하지 못하는 일이 없어집니다.

드라이브와 메모리 같은 고위험 구성요소에는 위조 제품인지 쉽게 알아볼 수 있도록 복제 불가능한 라벨을 붙입니다.

[6] "**Cyber Supply Chain Security and Potential Vulnerabilities within U.S. Government Networks**," National Conference of State Legislatures, 2016

[7] "**Apple Severed Ties with Server Supplier After Security Concern**," The Information, 2017

HPE Pointnext

HPE Pointnext는 엔터프라이즈 고객을 대상으로 하는 자문, 전문가 및 운영 서비스를 제공합니다. HPE Pointnext의 전문가들이 하이브리드 IT 환경으로의 전환 및 최적화를 지원하며 에지에서 코어, 코어에서 클라우드로 전환하도록 도와줍니다.

HPE Pointnext는 고객들이 디지털 경제에서 경쟁우위를 차지하는 데 필요한 적응형 디지털 보호를 구현할 수 있도록 조언하고, 전략과 로드맵을 정의하며, 아키텍처 및 설계 서비스를 제공하고, 통합 및 혁신을 지원합니다. HPE의 유연한 방법론과 청사진을 통해 전체적인 관점에서 바라보는 전환뿐만 아니라 격차를 줄이거나 현재 보안 통제, 연속성, 보안 운영을 개선하기 위한 구체적인 솔루션도 구현할 수 있습니다.

다음 내용에서 각 서비스가 조직의 보안을 어떻게 개선할 수 있는지 확인해 보십시오.

위험과 연속성, 컴플라이언스 관리

HPE Pointnext 서비스를 이용하는 조직은 위험과 연속성, 컴플라이언스 관리 프로그램을 비즈니스 목표, 위험 수용 범위, 복구 요건, 규정 요구사항과 일치시킬 수 있습니다. 예를 들어 HPE Pointnext는 조직의 컴플라이언스, 아키텍처와 취약성 평가, 비즈니스 영향력 평가 수행을 지원합니다. 재해 복구와 비즈니스 연속성 계획 서비스도 제공합니다.

인프라 및 액세스 제어

HPE Pointnext는 조직이 안전한 인프라와 액세스 제어를 설계하고 구현하여 비즈니스 요건에 부합하도록 지원합니다. HPE Pointnext의 맞춤형 참조 아키텍처는 고객이 클라우드와 IoT, 모바일, 기타 환경에 보안을 설계하고 통합하는 데 도움이 됩니다.

HPE 플랫폼 보호 및 컴플라이언스 서비스를 통해 조직은 IT 인프라를 평가하고 보안 대비력을 개선할 수 있습니다. HPE Aruba ClearPass, 타사의 네트워크 액세스 제어 제품 등의 기술을 통합할 수 있는 서비스가 제공됩니다.

데이터 보호 및 개인정보 보호 평가

HPE Pointnext는 조직이 개인식별정보(PII), 지적재산권, 기타 민감한 데이터에 대한 위험을 평가하고 이해하도록 지원합니다. 위험 방지에 적절하고 예산에 맞춘 제어 방법을 설계하여 디지털 자산의 기밀성과 무결성, 가용성을 보호합니다. HPE Pointnext는 사람, 정책, 프로세스, 제품, 증명(People, Policy, Process, Product, Proof)으로 구성된 5P 원칙을 통해 종합적인 데이터 보안 및 보호를 수행합니다.

본 비즈니스 백서 작성에 기여한 사람:

Boliek, Lois H.

Bradley, Chris

Brockelman, Ken

Church, Nigel

Dasari, Shiva R.

De Clercq, Jan

Kapoor, Vikas

Leech, Simon

Lepore, Mark

Lunetta, Larry

Malik, Rashmi

Mayes, Brad

Moore, Bob

Young, Greg

HPE Pointnext의 백업, 복구, 아카이빙(BURA) 기술을 통해 데이터 백업 및 복구에 전략적 이니셔티브를 구현할 수 있습니다. HPE 데이터 삭제 서비스를 통해 스토리지와 다른 시스템에서 민감한 데이터를 삭제할 수 있습니다. 또한 패치 관리 서비스를 사용하여 알려졌거나 새로운 맬웨어 위협으로부터 보호합니다.

운영 보안 및 사이버 방어

인프라 보안 통제로 보안 수준을 향상할 수 있습니다. 그러나 이러한 통제가 실제로 효과를 발휘하려면 조직에 무엇이 필요한지, 기존 통제의 실제 효과가 어느 정도인지 평가하여 위험을 완전히 파악해야 합니다.

HPE의 운영 보안(OPSEC) 프레임워크와 운영 보안 서비스 제품군을 사용하면 위협 관리, 취약성 관리, 보안 모니터링 같은 영역을 제어할 수 있습니다. OPSEC 서비스에는 HPE Gen10 보안 기능을 위한 HPE Foundational Care, HPE 데이터 삭제 서비스, HPE 자산 복구 서비스, 직원 보안 프로그램 등이 있습니다.

ITIL®을 이용한 보안 요건 준수

HPE의 ITIL(IT Infrastructure Library) 프로세스는 IT 보안 요건을 비즈니스 니즈에 맞게 평가하고 조정하며 보안이 장애물이 아닌 디지털 전환의 원동력임을 보장합니다. HPE는 공통 목표를 정의하고 비즈니스 니즈에 대응하는 방식으로 엔터프라이즈 위험 지표를 식별하는 것을 지원합니다.

자동화를 통한 사건 탐지 및 대응력 개선

HPE는 보안 관리자가 SIEM(보안 정보 및 이벤트 관리)과 HPE Aruba IntroSpect 같은 행동 분석 툴을 사용하여 전사적으로 보안 정보를 중앙 집중화하고 연관성을 찾을 수 있는 방법을 제공합니다.

결론

HPE가 기술 스택에 구현하는 보안 통제는 조직이 내부에서 보안 사건을 식별, 보호, 탐지, 대응, 복구하도록 설계되었습니다. 복잡한 IT 공급망으로 인해 제기되는 보안 위험도 인식하고 있습니다. HPE가 소프트웨어 및 구성요소의 무결성을 보호하기 위해 취한 조치는 IT 업계에서 독보적입니다.

Hewlett Packard Enterprise는 실리콘과 펌웨어 계층에서 시작하여 하드웨어, 데이터 센터, 클라우드를 통과하는 기술 스택을 통해 인터넷 규모의 워크로드를 구축, 배포, 실행, 관리하는 표준 기반의 보호 기능을 제공합니다.

업계 표준과 성공 사례 기반의 HPE의 보안 접근 방식은 최고 수준의 미국 정부 및 국제 표준의 인증을 받았습니다. 고객의 워크로드가 온프레미스나 클라우드, 하이브리드 환경, 네트워크 에지에서 안정적으로 실행되도록 하는 것이 HPE의 목표입니다.

자세히 알아보기:

hpe.com/security

지금 업데이트 받기

© Copyright 2017 Hewlett Packard Enterprise Development LP. 본 안내서의 내용은 사전 통지 없이 변경될 수 있습니다. Hewlett Packard Enterprise 제품 및 서비스에 대한 보증의 경우, 해당 제품 및 서비스와 함께 제공된 보증문에 명시된 내용만이 적용됩니다. 본 문서에는 어떠한 추가 보증 내용도 들어 있지 않습니다. Hewlett Packard Enterprise는 본 안내서의 기술상 또는 편집상의 오류나 누락에 대해 책임지지 않습니다.

Windows는 미국 및/또는 다른 국가에서 Microsoft Corporation의 등록 상표 또는 상표입니다. Linux는 미국 및 기타 국가에서 Linus Torvalds의 등록 상표입니다. ITIL®은 AXELOS Limited의 등록 상표입니다. VMware는 미국 및 기타 국가에서 VMware, Inc.의 등록 상표 또는 상표입니다. 기타 모든 타사 상표는 해당 소유주의 자산입니다.

a00006637KOP, 2017년 10월, Rev. 1