퓨어1(PURE1®)의 보안성

퓨어1(PURE1) 개요

퓨어1은 고객이 퓨어스토리지 제품을 모니터링, 관리 및 지원하는 데 사용하는 웹 기반 서비스입니다. 이 서비스는 유효한 서비스 계약을 보유한 모든 고객에게 제공되며, 제품이 인터넷에 연결되어 있기만 하면 사용이 가능합니다. 퓨어1은 퍼블릭 클라우드 제공업체가 호스팅하는 안전한 *가상 프라이빗 클라우드*(VPC)에서 실행됩니다. (현재 기준 VPC: Amazon Web Services) 고객은 퓨어스토리지가 제공하는 브라우저와 모바일 디바이스 애플리케이션을 통해 퓨어1에 액세스할 수 있습니다. 퓨어1의 주요 기능은 다음과 같습니다.

- 고객이 보유한 모든 퓨어스토리지 제품의 성능, 사용률 및 경고 정보를 단일 화면에서 확인
- VMware 환경의 엔드-투-엔드 I/O 성능을 보여주는 '풀스택' 분석
- 다양한 시나리오를 평가하는 AI 기반 워크로드 시뮬레이션

퓨어1은 퓨어스토리지가 개발, 관리 및 운영합니다. 고객은 서비스 및 라이선스 구매, 설치, 업데이트 또는 관리를 할 필요 없이, 사용만 하면 됩니다. 서비스는 전 세계적으로 제공됩니다. 그림 1처럼 고객이 보유한 모든 퓨어스토리지 제품들에 대한 최신 정보를 요약해 보여주는 *대시 보드*를 통해, 전 세계에 배포되어 있는 제품을 확인하고 각 시스템의 세부 정보를 살펴볼 수 있습니다.

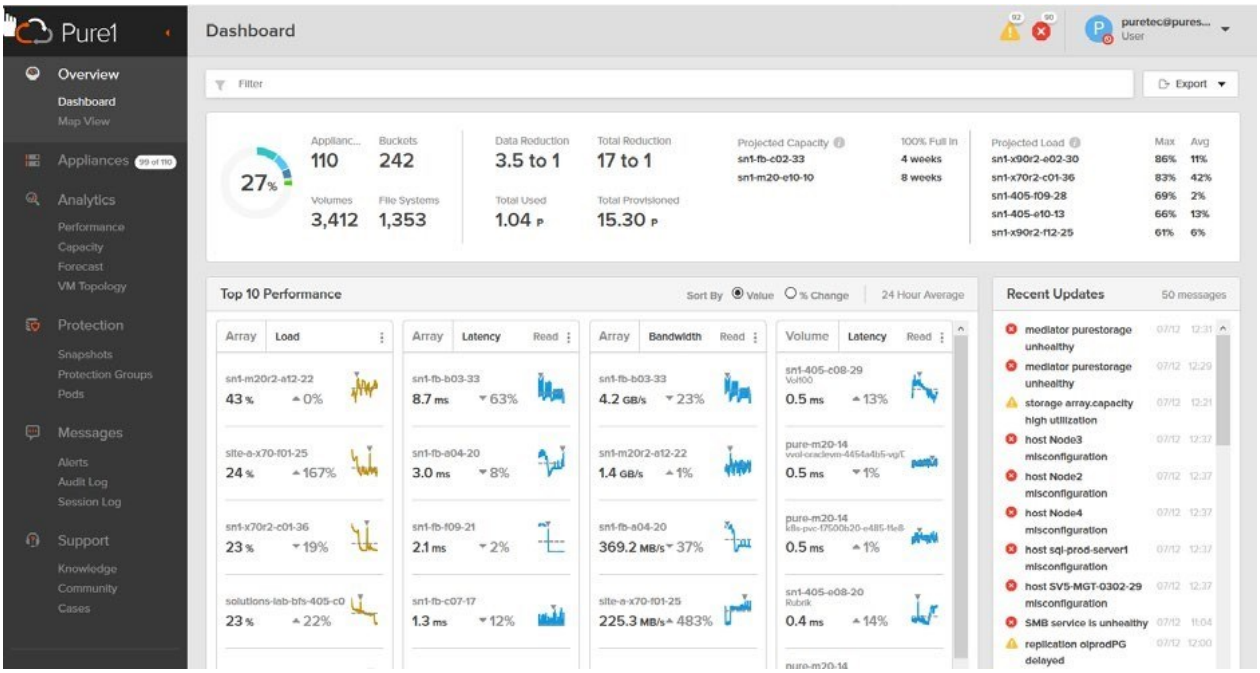

그림 1. 퓨어1 대시보드 예시

퓨어1 기능

퓨어1 VPC는 고객 시스템에서 업로드된 사용률, 성능 및 경고 상태에 대한 정보를 수신, 필터링, 분석 및 저장합니다. 이벤트로 보증이 되는 경우, 퓨어1 서버가 서포트 티켓을 생성합니다.

이 서비스는 두 가지 주요 요소로 구성됩니다.

퓨어1 매니지(Pure1 Manage, 일반적으로 'Pure1'으로 지칭)

퓨어1 데이터베이스의 정보를 사용해 조직이 보유한 모든 퓨어스토리지 제품의 성능, 사용률 및 경고 내역을 표시해주는 웹 애플리케이션입니다. 고객은 앱을 통해 서포트 티켓을 생성하고 관리할 수 있으며 분석과 향후 계획을 위한 툴에 액세스할 수 있습니다. 향후 계획에는 시스템에 워크로드 추가, 시스템 간 워크로드 이동 등 다양한 시나리오가 포함됩니다.

지원 인프라

퓨어스토리지는 다음과 같이 조직의 주요 툴을 지원합니다.

- 업로드된 시스템 로그를 분석해 잠재적인 문제를 식별하고 해결 작업에 착수합니다. 일반적으로 전체 서포트 티켓의 절반 이상을 퓨어1이 생성합니다.
- 잠재적인 문제를 식별하고 방지하기 위해, 고객 시스템의 설정과 상태를 알려진 제품의 *핑거프린트* 및 환경적 문제와 지속적으로 비교합니다.
- 소프트웨어 업그레이드나 기타 실무적인 지원이 필요한 경우, 고객 시스템과 서포트 엔지니어가 직접 상호작용할 수 있도록 *RemoteAssist* 채널을 제공합니다.

이 두 가지 주요 서비스 외에도, 퓨어1은 포털을 통해 고객과 퓨어스토리지 직원들이 지식과 우수 사례를 공유하는 지식센터와 협업 포럼을 제공합니다.

퓨어1의 가치

퓨어1은 퓨어스토리지 고객에게 다음과 같은 혜택을 제공합니다.

- 하나의 화면에서 조직의 시스템을 어디서나 모니터링하고, 향후 스토리지 및 I/O 요구 사항을 예측하며, 다양한 시나리오에 대한 분석을 수행하고, 공개된 서포트 사례들을 모니터링할 수 있습니다.
- 스토리지 관리 서버 구매, 통합, 교육 및 유지·보수 작업에서 벗어나되, 최신 스토리지 관리 서비스에 항상 액세스할 수 있습니다.
- 퓨어스토리지 지원 팀이 고객 문제 진단, 핑거프린트 추출, 분석과 향후 계획을 지원하는 알고리즘을 훈련시키는 데 기여할 수 있습니다.
- 고객 시스템과 퓨어스토리지 지원팀 간의 소통 창구를 제공합니다. Phonehome을 활성화하면 별도의 RemoteAssist 연결이 필요하지 않습니다.

퓨어1은 설치 기반에 대한 현재 및 과거 정보의 집약으로, 문제 해결 속도를 높여주며 선제적 지원을 가능하게 해줍니다. 운영 중인 시스템들이 지속적인 피드백을 제공해 기존 기능들을 검증해주며, 새로운 기능에 대한 요구 사항과 잠재적 가치에 대한 인사이트를 제공하고, 운영 환경에서 잠재적인 문제를 파악할 수 있도록 합니다.

퓨어1 VPC 컴포넌트

그림 2는 퓨어1 VPC의 주요 컴포넌트를 보여줍니다. '서버'는 클라이언트 로드에 기반해 인스턴스를 시작 및 중지하는 오토 스케일링 클러스터입니다. 로드 밸런서는 클라이언트 액세스를 제어하고 다른 서버들 전반에서 로드의 균형을 맞춰 줍니다.

Phonehome

연결된 시스템에서 수신된 정보를 **Worker** 서버에서 처리될 수 있도록 대기열로 보냅니다. Phonehome 서버는 이밖에도 *RemoteAssist*(RA) 세션 중에 서포트 엔지니어가 시스템과의 상호작용에 사용하는 채널입니다.

Worker

유입되는 정보를 필터링하고 처리합니다. 다양한 Worker가 원시 정보와 추출 결과를 저장하고, 서포트 엔지니어가 사용할 수 있도록 로그 포맷을 지정하며, 경고를 분석하고, 문제를 식별하며, 필요에 따라 서포트 티켓을 생성합니다.

퓨어1 매니지 및 REST

클라이언트에게 모니터링, 분석 및 지원 사례 관리를 제공합니다. REST 서버는 클라이언트 요청을 **퓨어1 매니지** 데이터베이스로의 호출로 전환합니다.

서버는 업로드된 성능, 사용률, 경고 및 로그 정보의 데이터베이스(**System History** 및 **Quick Access**), 관리자 작업 및 내부 시스템 이벤트(**Support**), 그리고 클라이언트에게 신속하게 그래픽으로 제공할 수 있도록 포맷 및 업로드된 정보의 추출 결과(**Pure1 Manage**)를 관리합니다.

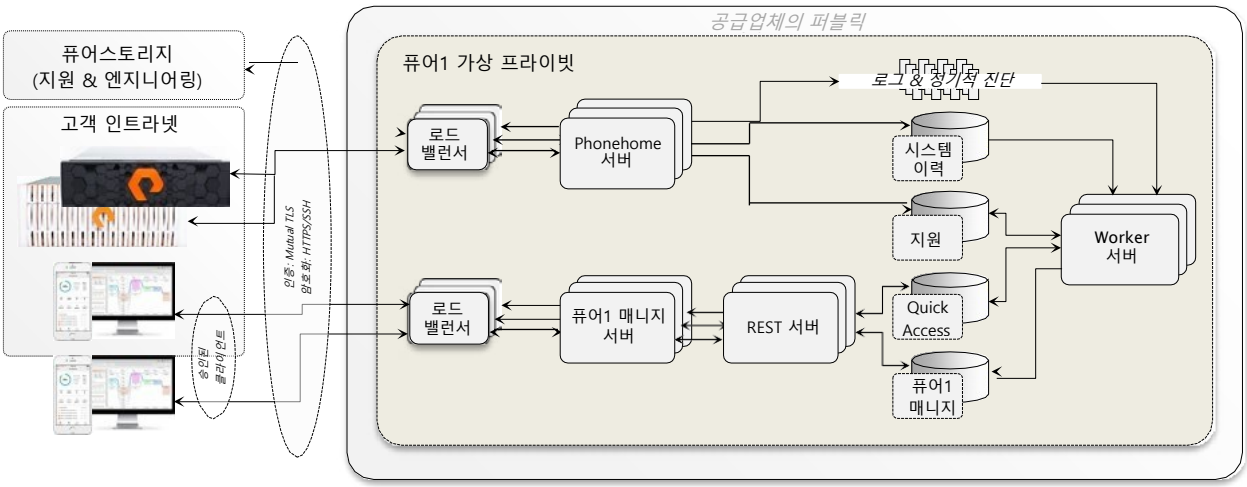

그림 2. 퓨어1의 주요 컴포넌트

퓨어1 정보의 흐름

설치된 시스템은 다음의 두 가지 방식으로 퓨어1 VPC와 상호작용합니다.

Phonehome

Phonehome이 활성화된 시스템은 30초마다 퓨어1 클라우드(Pure1 Cloud)에 상태 및 설정 정보를 업로드하고, 1시간마다 보다 포괄적인 로그를 업로드합니다. 네트워크 액세스나 조직의 정책으로 외부 연결이 금지된 경우를 제외하고, 대부분의 고객은 시스템에서 Phonehome을 활성화합니다. 시스템 관리자는 언제든지 Phonehome을 활성화 및 비활성화 할 수 있습니다.

RemoteAssist

서포트 엔지니어는 Phonehome 채널을 사용해 고객이 제어하는 *RemoteAssist* 세션 범위 내에서 시스템과 직접 상호작용합니다. RemoteAssist를 통해 엔지니어는 내부 시스템 정보를 조회하고 관리자가 할 수 없는 소프트웨어 유지·보수 및 기타 기능을 수행할 수 있습니다.

그림 3은 시스템, 클라이언트, 퓨어스토리지 지원 및 퓨어1 VPC 간의 정보 흐름을 개괄적으로 보여줍니다. 시스템은 보안 Phonehome 채널을 통해 정기적으로 정보(*텔레메트리*)를 전송합니다. VPC의 서버는 수신된 정보를 저장하고 필터링하여 고객이 표시, 분석 및 계획하고 퓨어스토리지 지원이 사용할 수 있도록 대체 형식으로 저장합니다.

퓨어1 클라이언트는 데이터베이스의 정보를 포맷하는 서버를 통해 시스템의 성능, 사용률 및 경고 상태에 대한 정보를 확보하여 편리하게 그래픽으로 표시할 수 있습니다. (클라이언트는 자신의 조직 시스템에 대한 정보에만 액세스 가능) 전체 설치 기반의 입력으로 훈련된 알고리즘을 통해 다양한 시나리오에 대한 분석을 요청할 수 있습니다.

RemoteAssist 세션은 통신에 Phonehome 채널을 사용합니다. 서포트 엔지니어는 고객 시스템에 로그인하여 소프트웨어를 업그레이드하고 문제를 진단하며 고객의 관리 작업을 지원합니다.

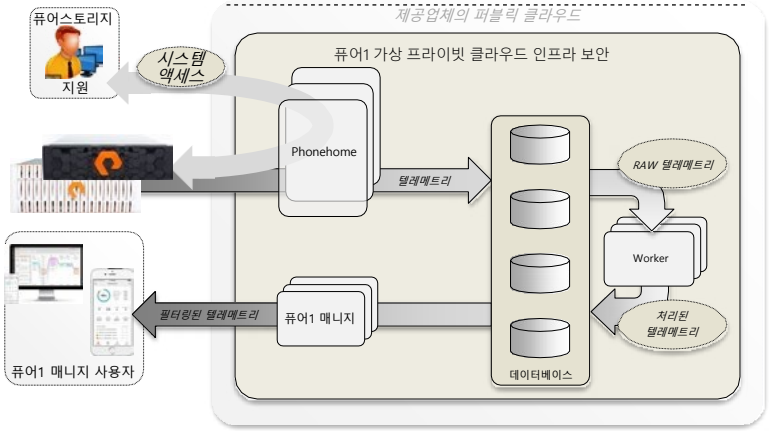

그림 3. 퓨어1 정보의 흐름

개요의 나머지 부분은 퓨어1이 이러한 정보 흐름을 어떻게 보호하는지 설명합니다.

퓨어1 액세스 보안

그림 3과 같이, 퓨어1 서비스에 액세스하는 두 가지 경로는 Phonehome 채널과 퓨어1 클라이언트 애플리케이션입니다. 두 경로 모두 인증이 필요하고, 통신을 암호화하며 의심스러운 상황을 감지하기 위해 지속적으로 모니터링됩니다.

Phonehome 채널 보안

시스템은 Phonehome 채널을 사용해, 환경(예: 연결된 호스트의 이름 및 네트워크 주소), 성능, 사용률 및 퓨어스토리지 제품에 대한 경고 정보를 퓨어1으로 전송합니다. 퓨어1 애플리케이션은 *사용자 데이터*(호스트가 작성하고 제품에 저장된 데이터)에 대한 액세스 권한이 없습니다. 제품은 다음과 같은 형태로 정보를 전송합니다.

정기적 진단(30초마다)
시스템 설정, 하드웨어 및 소프트웨어 상태, 성능, 사용률 및 경고 정보

로그(시간별)
관리자 작업 및 중요한 이벤트에 대한 세부적인 기록(예: 여유 공간이 20% 이하로 내려가는 경우)[1]

정보를 업로드할 때마다 시스템은 퓨어1 VPC **로드 밸런서**를 통해 연결되며, 상호 인증을 위해 HTTPS로 TLS(버전 1.1 및 1.2)를 사용합니다.[2] 시스템은 설치 중에 퓨어스토리지에서 발행한 고유 인증서로 인증하고, 연 1회 이상 갱신됩니다. 데이터센터 정책으로 아웃바운드 연결을 금지하고 있는 고객의 경우, 방화벽에서 퓨어1 DNS 이름 또는 IP 주소를 화이트리스트에 추가하여 Phonehome 통신을 활성화할 수 있습니다.

퓨어1 액세스 보안

퓨어1은 VM Analytics에 의해 사용되는 성능, 스토리지 사용률 및 기타 정보를 일정 기간 동안 클라이언트가 사용할 수 있도록 합니다.[3] 퓨어스토리지는 문제 해결, 핑거프린트 추출, 잠재적인 제품 개선 및 향상 기회를 모색하기 위해 일부 정보를 무기한 보관합니다. 클라이언트에게 표시되는 정보는 시스템에서 직접 가져오는 것이 아니라 Phonehome 업로드에서 파생됩니다.

퓨어 1 클라이언트 인증

퓨어 1 **지원** 데이터베이스에는 각 퓨어스토리지 고객별로 두 개의 오브젝트가 존재합니다.

- 고객을 구분하는 **조직** 오브젝트
- 고객을 위한 *Pure1 어드민 클라이언트*(**Pure1admin**) 오브젝트(계정)

Pure1admin 클라이언트는 조직에 추가 계정을 생성하고, 수정 및 삭제할 수 있습니다.

시스템 설치 중에, 퓨어1은 **지원** 데이터베이스에 **시스템** 오브젝트를 생성해 이를 담당 조직에 연결합니다. 퓨어1은 이러한 오브젝트를 사용해 정보에 대한 클라이언트의 액세스 범위를 결정합니다.

퓨어1은 최초 설치 중에 설정된 고객의 아이덴티티 프로바이더(IDP)를 사용해 클라이언트를 인증합니다. IDP를 사용하지 않는 조직의 경우, 퓨어스토리지의 공인 IDP(현재 기준 Salseforce.com)를 사용해 클라이언트 액세스를 제어합니다. 퓨어1과의 모든 클라이언트 통신은 HTTPS로 암호화됩니다.

파트너 액세스

공인 서비스 제공업체(Authorized Service Providers; ASP)도 퓨어1에 액세스할 수 있습니다. ASP는 자사 고객의 시스템과 관련된 퓨어1 정보에만 액세스할 수 있습니다. ASP가 아닌 파트너를 통해 제품을 구매하는 조직은 시스템 정보에 대한 파트너 액세스를 가능하게 해주는 계정을 생성할 수 있습니다.

---

1 FlashArray 텔레메트리 콘텐츠는 비밀 유지 협약을 체결한 고객에게 제공됩니다. 목록은 아래에서 확인하실 수 있습니다.
https://support.purestorage.com/FlashArray/FlashArray_Security/FlashArray_Security_Reference/Phone_Home_Contents

2 Purity//FA의 5.2 이전 버전과 Purity//FB의 2.5 이전 버전은 암호화된 SSH 터널을 통해 통신을 했습니다.

3 이 문서가 간행된 시점에, 퓨어1은 35일간의 성능 이력, 13개월 동안의 스토리지 사용 이력, 7일간의 VM Analytics 데이터를 클라이언트에 제공합니다. 프리미엄 **VM Analytics Pro** 옵션은 최대 3년 동안 VM Analytics 데이터를 보존합니다.

퓨어스토리지 파트너와 법무 조직은 액세스 권한을 부여하기 전에 잠재적인 파트너의 자격을 심사합니다.

> *비밀번호로 보호되는 모든 시설과 마찬가지로, 보안의 강도는 비밀번호의 강도와 관련이 있습니다. 고객은 퓨어1에 비밀번호 정책을 지정하고 시행할 책임이 있습니다.*

퓨어스토리지 직원 액세스

퓨어스토리지의 전사적 IDP(현재 기준 Okta)는 퓨어1에 대한 직원 액세스를 관리합니다. 업무상 액세스가 필요한 직원은 Phonehome이 활성화된 모든 고객 시스템에 업로드된 정보를 조회할 수 있습니다. AE 및 SE는 퓨어1을 사용해 자사 고객의 시스템을 모니터링하고 향후 계획을 지원합니다.

RemoteAssist 액세스 보안

RemoteAssist 세션은 인증 및 승인된 지원과 개발 엔지니어의 문제 진단, 해결, 소프트웨어 설치 및 기타 고객 지원을 위해 시스템 콘솔에 액세스할 수 있게 해줍니다. 엔지니어가 고객의 시스템에 액세스하려면, **어레이** 권한을 보유한 관리자가 RemoteAssist를 활성화해야 합니다. (관리자는 RemoteAssist를 비활성화하여 언제든지 세션을 종료할 수 있습니다.) 관리자가 갱신하지 않는 한, 세션은 48시간 후에 자동으로 종료됩니다.

고유한 시스템 식별

모든 퓨어스토리지 제품에는 **puresupport** 계정과 퓨어스토리지의 SSH 인증기관(CA) 간의 신뢰를 구축해주는 일반 인증서가 사전 설치되어 있습니다. 제품 설치 시 자동으로 CA에 *등록*이 이루어지고, 고유한 식별을 가능하게 하는 *어플라이언스 ID*가 포함된 새로운 인증이 확보됩니다. 이후, 등록된 제품의 어플라이언스 ID가 SSH 인증서의 주체로 표시되면, 지원 인프라가 제품 **puresupport** 계정 SSH 액세스를 부여합니다. 이를 통해 한 시스템에 대해 발급된 인증서를 실수로 사용해 다른 시스템에 액세스하는 것을 방지할 수 있습니다.

퓨어1 서포트(Pure1 Support) 인프라에 대한 퓨어스토리지 및 ASP 직원 액세스

모든 RemoteAssist 활동은 퓨어1 클라우드를 통해 수행됩니다. 퓨어스토리지 엔지니어는 사내에서 또는 회사 VPN을 통해 클라우드에 액세스합니다. ASP 엔지니어는 퓨어스토리지가 관리하는 IDP(현재 기준 Salesforce.com)를 사용해 인증합니다. 인증된 엔지니어는 제한된 시간(현재 기준 10시간) 동안 필요한 클라우드 기능에 대한 액세스 권한을 부여하는 SSH 인증서를 받습니다.

퓨어1 클라우드에 연결되면, 엔지니어는 SSH CA를 통해 *퓨어1 서포트 인프라*(RemoteAssist 액세스 보안의 첫 번째 관문)에 액세스합니다. (퓨어스토리지 직원의 경우 LDAP 또는 Okta를 통해, ASP 엔지니어의 경우 Salesforce.com을 통해) 엔지니어가 인증되면, CA는 엔지니어를 지원 인프라에 액세스할 수 있는 보안 주체로 하여 최대 10시간 동안 지속되는 임시 SSH 인증서를 발급합니다. ASP 엔지니어는 자신의 조직이 담당하는 시스템에만 액세스할 수 있습니다.

엔지니어는 SSH 인증서로 지원 인프라에 액세스할 수 있지만, RemoteAssist 세션에는 액세스할 수 없습니다. 세션에 참여하려면, 엔지니어는 CA에 타깃 시스템의 고유한 *어플라이언스 ID*를 SSH 인증서의 주체에 추가해줄 것을 요청해야 합니다. 보강된 인증서는 엔지니어가 지정된 시스템의 **puresupport** 계정에 짧은 시간(현재 기준 2분) 동안 로그인할 수 있는 권한을 부여합니다. 한 번 로그인하면 엔지니어는 최대 10시간 동안 세션을 수행할 수 있습니다.

지원 인프라는 모든 RemoteAssist 세션 활동을 기록합니다. 고객 요청 시 퓨어스토리지는 시스템의 RemoteAssist 세션 로그를 제공합니다.

퓨어1 클라우드 인프라 관리

퓨어1 클라우드 리소스 액세스 보안

퓨어1 클라우드 서버 및 데이터베이스는 클라우드 제공업체가 호스팅하는 *퓨어1 서포트 대시보드*를 통해 중앙에서 관리됩니다. 승인된 사용자만 대시보드에 액세스할 수 있으며, 퓨어스토리지 내부 네트워크를 통해서만 액세스가 가능합니다. 퓨어스토리지의 Okta 아이덴티티 관리 시스템을 통해 권한이 인증된 직원만 대시보드에 액세스할 수 있습니다. 아이덴티티 관리 시스템은 인사 시스템과 연결되어, 직원의 재직 상태에 따라 대시보드에 대한 액세스를 자동으로 부여 또는 취소합니다.

지원 및 개발 엔지니어만이 퓨어1 서포트 데이터베이스에 있는 세부적인 이벤트 내역을 조회할 수 있습니다. 서포트 엔지니어는 퓨어스토리지에서 개발한 *플레이백 GUI*를 사용하며, 이 GUI는 관리 작업 및 시스템 응답을 순서대로 표시하여 진단 작업을 지원합니다. 개발자는 자동화된 시스템을 사용해 클라우드 소프트웨어 업데이트를 설치하고 클라우드 데이터베이스를 관리합니다.

침입으로부터 퓨어1 클라우드 보호

퓨어1은 클라우드 제공업체가 권장하는 보안 지침과 우수 사례를 구현합니다. *Lacework* 등의 클라우드 보안 모니터링 툴을 사용해 의심스러운 활동과 자원 오용을 파악하고 보고합니다. 이 툴은 보안(예: 액세스 규칙 위반), 성능(예: 서비스 한도 도달) 및 가용성(예: 가상 서버 충돌)의 측면에서 잠재적 문제를 표시하여 클라이언트 측 서비스에 영향을 미치기 전에 해결 우선순위를 정합니다.

퓨어스토리지의 보안 팀은 미국 컴퓨터 긴급 대응팀(US-CERT) 등의 인증된 컴퓨터 보안 경고 소스를 모니터링해 잠재적인 위협, 악용 및 취약성을 파악하고 심각도에 따라 선제적으로 해결 우선순위를 지정합니다. 모든 퓨어1 클라우드 보안 강화 작업은 퓨어스토리지의 지원 티켓팅 시스템으로 추적되기 때문에, 보안 문제 상태를 중앙에서 관리할 수 있습니다.

개발 및 유지·보수 보안

설계 검토 및 침투 테스트

퓨어스토리지는 신뢰할 수 있는 외부 기업과 정기적으로 협력해, 퓨어1 클라우드에 대한 독립적인 설계 검토 및 침투 테스트를 수행합니다. 중요하거나 위험도가 높은 취약점이 발견되면, 발생할 확률과 잠재적인 기술 및 재정적 영향을 기반으로 해결 우선순위가 지정됩니다. 중요한 문제(운영 중단 또는 보안 사고)가 발생하는 경우, 보안 및 사이트 안정성 엔지니어링(SRE) 팀이 사후 분석을 수행하여 근본 원인을 파악하고 향후 유사한 문제의 발생을 예방하거나 그 영향을 완화하기 위한 계획을 수립합니다.

퓨어1의 개선 및 변경 관리 절차

보안 팀은 퓨어스토리지의 지원 티켓팅 시스템을 사용해 퓨어1 클라우드 코드의 모든 변경 사항과 기능 향상 내역을 추적합니다. 변경 사항을 적용하는 절차는 다음과 같습니다.

1. 보안 팀은 설계 결함, 잠재적 보안 문제 및 불필요한 복잡성의 측면에서 개발자의 제안을 검토합니다.
2. 개발자는 제안서를 코딩하고(필요한 경우 수정), 동료 검토를 위해 코드를 제출합니다. 검토자는 설계가 제안서를 충족하는지 확인합니다.
3. 개발자는 코드를 구현 및 테스트하고, 결과를 내부 클라우드 서비스에 스테이징합니다.
4. SRE 팀은 스테이징된 구현을 확인하고 통신, 배포 및 유지 관리 계획에 대해 개발자와 합의합니다.
5. 다른 개발자나 SRE 대리인의 감사를 받은 후, 개발자는 새로운 코드를 운영 환경에 적용합니다.