VERITAS

VERITAS ALTA™

클라우드 데이터에 대한 이상 탐지

클라우드 데이터 및 사용자 활동을 모니터링하는 효과적인 툴.

이상 탐지는 클라우드 데이터 및 사용자 활동에서 비정상적이거나 이상한 요인을 트래킹하여 알리는 강력한 조기 경고 시스템입니다. 따라서 문제가 발생하기 전에 미리 파악하여 조치하는 데 도움이 됩니다. 이상 요인은 보안 위반, 하드웨어 또는 소프트웨어 문제, 고객 요구 사항의 변화, 또는 즉시 주목해야 할 각종 문제의 지표가 될 수 있는 만큼 이를 탐지하는 것이 중요한 데이터 보안 프랙티스로 자리잡았습니다. 이를 위해 데이터 세트에서 비정상적인 요소나 패턴을 찾는 프로세스를 수행합니다. 주어진 기준선(사전에 정의된 허용 범위)에서 벗어나는 모든 것이 이상 요인으로 간주됩니다. 고객은 설정된 매개변수 및 지능형 지표 세트를 통해 즉시 주목해야 할 이상 요인에 관한 알림을 받고, 활동 모니터링을 통해 실시간으로 업데이트되는 대시보드에서 손쉽게 확인할 수 있습니다. 침입의 징후가 될 만한 비정상적인 파일 쓰기 활동(알려진 랜섬웨어 파일 확장자를 탐지할 수도 있음), 파일 액세스 패턴, 트래픽 경로, 일반적인 패턴과 대비되는 비정상적인 활동 증가 등을 이상 요인의 예로 들 수 있습니다. 비정상적인 점에 관해 즉각적인 알림을 받으면, 신속하게 조치하거나 완화할 수 있다는 점에서 매우 유익합니다. 문제가 발생할 때 제대로 파악하거나 리스크를 완화하고, 신속하게 격리하여 파괴적인 영향, 다운타임 등 보안 위반과 관련된 각종 문제를 방지할 수 있다는 것은 매우 중요합니다.

데이터 관제 센터의 역할

클라우드 데이터가 폭발적으로 의 증가하고 확산됨에 따라, 특히 사이버 위협 및 랜섬웨어에 대비하여 모든 클라우드 데이터를 통합 감시하는 이상 탐지 솔루션의 필요성이 커지고 있습니다. 지금까지 사이버 범죄자는 온갖 창의적인 방법으로 시스템과 데이터에 접근해 왔습니다. 시스템에 침투하여 암호화하기 시작하고 최대한 많이 다운로드한 다음 탐지되기 전에 빠져나갑니다. 이러한 시나리오에서 이상 탐지 기능을 구현함으로써 문제에 관한 알림을 받고 조치를 취할 수 있습니다.

클라우드는 2022년 사이버 범죄자가 가장 많이 이용한 랜섬웨어 공격 경로로[1], 사이버 범죄자는 기업 범죄 플레이북에 수록된 몇 가지 전략을 구사하면서 장기전을 펼칩니다. 이들은 완성도 높은 사이버 정찰 기술을 보여주었습니다. 잠복형 랜섬웨어, 또는 슬리퍼(Sleeper) 랜섬웨어는 방식은 이제 디지털 세상에서 흔히 볼 수 있습니다. 이는 액세스 권한을 확보한 범죄자가 전략적으로 저자세를 취하고 숨는 것입니다. 왜 그럴까요? 이들의 최우선 순위는 최적의 공격 시점을 기다리는 동안 클라우드 환경 전반을 관찰, 학습하고 돌아다니면서 취약점을 찾아 악용하는 것이기 때문입니다. 따라서 이들이 행동하기 전에 발견한다면, 문제가 발생하기 전에 사태를 파악하고 조치하여 치명적인 영향을 방지할 절호의 기회가 됩니다.

공격자는 최대한 큰 피해를 일으켜 더 많은 수익을 올리고 최고의 효과를 거두려 합니다. 여느 기업과 마찬가지로 결국 ROI가 중요합니다. 몇몇 리포트에 따르면, 랜섬웨어가 최대 18개월간 잠복할 수도 있습니다. 공격자는 피해 규모를 극대화하려면 타이밍, 범위 등과 같은 여러 요인이 작용한다는 것을 잘 알고 있습니다. 이들은 몸값을 지불하는 것 외에는 다른 선택이 없는 상황으로 피해자를 몰아넣으려 합니다. 더 이상 보안 위반과 공격이 동시에 발생하지는 않습니다. 이처럼 상황이 더욱 복잡해지면서 공격자가 피해자보다 해당 시스템을 더 잘 아는 경우도 많습니다. 따라서 일련의 작전을 통해 중요 시스템을 교란하고 무력화하여 몸값을 높일 가능성도 매우 커지고 있습니다.

클라우드 전반의 데이터 가시성

기업이 성공적인 이상 탐지 기능을 구현하려면 먼저 거시적 관점에서 모든 데이터가 있는 위치를 파악하고 혹시 미확인 데이터가 있는지 점검해야 합니다. Veritas Vulnerability Lag Research[2]에 따르면, 미확인 데이터의 비중이 여전히 35%로 우려스러운 수준입니다. 따라서 기업이 보유하는 데이터와 해당 위치를 즉시 확인하는 것이 좋습니다.

베리타스 솔루션은 모든 클라우드 제공업체, 물리적 환경, 가상 환경을 포괄하여 모든 데이터에 대한 통합 가시성을 제공합니다. 또한 스토리지, 컴퓨팅 용량, 주요 데이터 보호 솔루션, 연계 리포트까지 파악할 수 있어 모든 시스템을 빠짐없이 파악할 수 있습니다. 이는 오늘날의 위협 환경에 특히 중요합니다. 사이버 범죄자들은 피해자가 모든 애플리케이션과 데이터에 관한 정확한 인벤토리를 관리하지 않고, 데이터에 대한 보안과 관리 감독이 소홀하길 바라기 때문입니다.

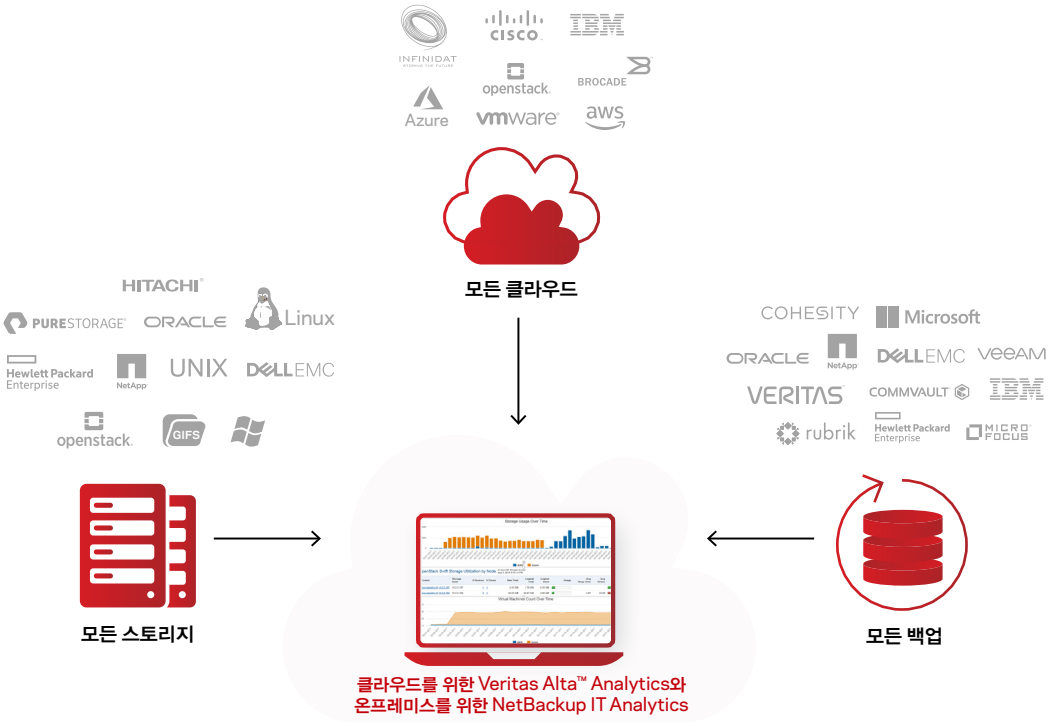

그림 1: 저장된 위치에 관계없이 모든 데이터를 포괄하는 통합 IT 인프라스트럭처

베리타스 솔루션은 고객의 환경에서 잘 드러나지 않는 영역을 조명하는 것은 물론 온프레미스, 클라우드, 데이터 보호, 스토리지를 포괄하는 통합 인사이트, 알림, 리포트 기능을 제공합니다. 백업 환경에 대한 가시성을 제공하는 리포트 옵션으로 사이버 공격을 받았을 때 정보에 근거한 의사 결정을 수행하는 데 필요한 인사이트를 확보하여 다음과 같이 활용할 수 있습니다.

- 클라우드를 위한 Veritas Alta™ Data Protection, 그리고 온프레미스를 위한 NetBackup으로 인프라스트럭처에 포함된 모든 호스트와 가상 머신(VM)을 검색 및 비교
- 백업에 누락되었거나 최근 백업이 없는 호스트가 있는 경우 잠재적 리스크 플래그 지정
- 랜섬웨어에 감염되었을 가능성이 있는 파일과 그 크기 및 해당 환경에서 저장된 위치 탐지
- 지금까지 생성된 리스크의 기록을 보여주는 대화형 그래프에 액세스

클라우드 전반의 AI 기반 이상 탐지

데이터 가시성을 확보했다면 다음 단계는 AI 기반 이상 탐지를 구현하는 것입니다. 클라우드를 위한 Veritas Alta™ Data Protection과 온프레미스를 위한 NetBackup은 전체 환경에서 비정상적인 데이터 및 사용자 활동을 탐지하고, 의심스러운 이상 요인이 있으면 거의 실시간으로 알립니다. 이 기술은 방대한 양의 데이터를 마이닝하고, 모니터링 및 리포팅을 자동화하며, 사용자 환경의 현재 상황에 관한 실행 가능한 인사이트를 제공하도록 설계되었습니다.

이상 탐지를 시각화하는 좋은 방법 중 하나는 거짓말 탐지기 검사의 원리를 적용하는 것입니다. 거짓말 탐지기 검사를 할 때 검사관은 사전 선별 검사로 시작하는데, 정상의 기준선으로 삼을 매개변수를 설정하고자 일련의 질문을 합니다. 피험자가 거짓말을 하면 예상대로 혈압, 맥박, 호흡, 피부 전도성 등의 생리적 지표가 설정된 정상 매개변수를 벗어나 변동합니다. 이와 비슷하게 클라우드를 위한 Veritas Alta™ Data Protection과 온프레미스를 위한 NetBackup은 AI 기반 탐지 엔진을 활용하여 장기간의 백업 작업 메타데이터 패턴을 토대로 정상에 해당하는 매개변수를 계산하고 맞춤형 백업 정책에 맞춰 자동으로 조정합니다.

정상의 기준을 벗어나는 이벤트를 캡처하고, 백업 팀에 거의 실시간으로 알립니다. 이상으로 관찰되면 심각도에 따라 점수가 부여됩니다. 이 점수는 관찰된 클러스터와의 거리를 기반으로 계산됩니다. 거리가 멀수록 더 심각한 점수가 부여됩니다. 그러면 관리자가 실행 가능한 인사이트를 식별하고 오탐지를 줄이는 데 도움이 됩니다.

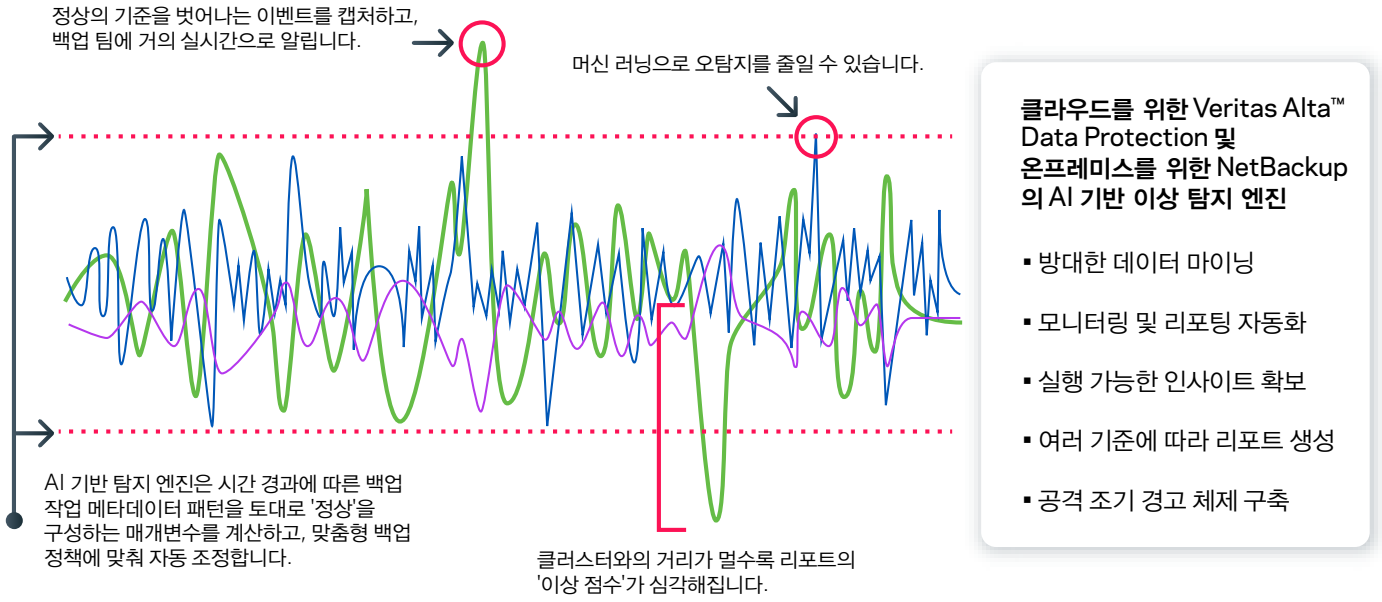

그림 2. 이상 탐지 이해

전반적으로 AI 기반 이상 탐지 엔진은 방대한 데이터를 마이닝하고, 모니터링 및 리포팅을 자동화하고, 실행 가능한 인사이트를 확보하며, 여러 기준에 따라 리포팅하고, 무엇보다도 공격에 대한 조기 경고를 설정하는 데 도움이 됩니다. 관리자는 모든 디바이스를 모니터링하고 공격에 대한 조기 경고를 설정함으로써 언제라도 데이터를 조명하고 이상 요인에 관한 권장 사항을 전달함으로써 문제가 발생하더라도 철저히 파악할 수 있습니다. 예를 들어, 베리타스의 AI 기반 이상 탐지 기능은 기본 서버와 손쉽게 통합되어 비정상적인 관찰 양상을 탐지할 수 있습니다. 즉, 클러스터에 속하지 않는 것을 이상 또는 이상치로 분류하는 것입니다. 관리자는 이러한 기능으로 이상 요인을 찾아내고 드릴다운하여 우려할 점이 있는지 확인할 수 있습니다. 이 엔진은 방대한 데이터를 마이닝하고 랜섬웨어 이벤트 해결을 위한 실행 가능한 인텔리전스를 제공하는 것은 물론 관리자가 알아야 할 해당 환경의 간단한 변경 사항도 전달합니다. 이러한 솔루션을 통해 공격이 진행 중이거나 곧 시작될 수 있다는 징후를 인식하여 즉각적인 조치를 수행하고 만일의 피해를 최소화할 수 있습니다.

게다가 이 툴은 지능적입니다. 즉, 오탐지 가능성을 파악하는데, 이를 위해 과거의 백업과 새로운 백업을 비교하여 작업 소요 시간의 큰 편차, 이미지 크기 변화, 정책 구성 변경 등의 이상 요인을 찾아냅니다. 이 AI 엔진은 파일 또는 파일 그룹을 모니터링하고, 파일 문자가 달라지는 시점을 (메타데이터 레벨까지) 알아냅니다. 파일이 블록 디스크에 있든 클라우드의 오브젝트 스토리지에 있든 상관없으며, 사후 처리 없이 수행합니다. 모든 시스템을 검사, 모니터링하고 어떤 요인에도 독립적이며 타사 백업 제품을 비롯한 모든 클라우드 플랫폼을 지원할 수 있는 기업은 베리타스가 유일합니다. 베리타스의 인공 지능/머신러닝(AI/ML) 엔진은 모든 서버에서 실행할 수 있습니다. 이처럼 차원 높은 지원으로 사각지대가 사라집니다.

악성 코드 검사

베리타스는 자동 검사 및 온디맨드 검사 기능으로 암호화 및 유출과 같은 다양한 유형의 악성 코드를 탐지하도록 지원합니다. 자동 악성 코드 검사 기능은 사람이 개입할 필요 없이 AI/ML 기술이 스스로 악성 코드를 검사할 수 있게 합니다. AI/ML 악성 코드 검사는 이상 점수가 높으면 자동으로 실행됩니다. 검사 범위에는 비정형 데이터, Windows, Linux, VMware가 포함됩니다. 이것이 중요한 이유는 대개 악성 코드가 해당 환경의 홈 디렉터리에 침투하기 때문입니다. 이 디렉터리는 일반적으로 대규모의 비정형 데이터 세트가 있는 위치입니다.

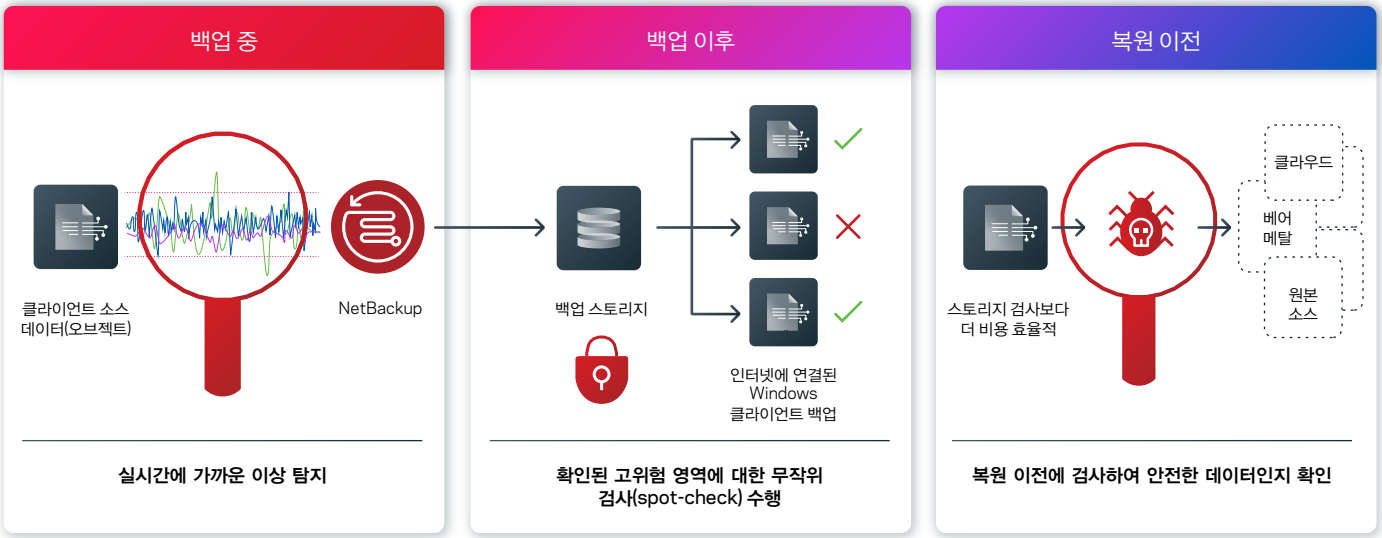

그림 3: 악성 코드 검사 개요

또한 복구가 필요한 경우 백업 데이터를 검사하여 최신 버전의 악성 코드 시그니처를 활용할 수 있습니다. 명확한 시각 요소와 경고 프롬프트를 통해 감염된 백업을 인식하여 공격의 영향을 받지 않은 안전한 데이터로만 복원할 수 있게 합니다. 이러한 방식을 흔히 정상으로 확인된 최신(last-known-good) 카피본으로 복원한다고 말합니다.

보안을 염두에 두고 설계된 베리타스

베리타스는 클라우드를 위한 Veritas Alta™ Analytics, 온프레미스를 위한 NetBackup IT Analytics로 통합 데이터 가시성, 이상 탐지, 악성 코드 검사 기능을 모두 제공합니다. 다음은 샘플 대시보드입니다.

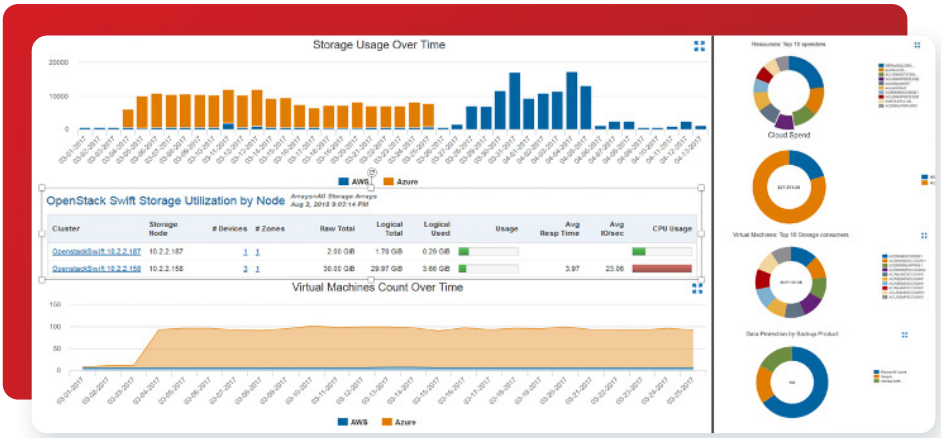

그림 4. 시간의 경과에 따른 스토리지 사용량을 보여주는 NetBackup IT Analytics 대시보드 샘플

베리타스 분석 솔루션의 특성:

- **통합적**—통합 콘솔에서 데이터 자산을 식별하는 단일 솔루션인 클라우드를 위한 Veritas Alta™ Analytics와 온프레미스를 위한 NetBackup IT Analytics는 오늘날 기업에서 사용 중인 모든 주요 서버, 스토리지, 하이퍼바이저, 데이터베이스, 애플리케이션 플랫폼을 지원합니다.
- **확장성**—중앙에서 통합 관리할 수 있도록 에이전트 없는 데이터 수집기를 제공합니다. 여기서 애플리케이션, 클라우드, 데이터 보호, 호스트, 네트워크, 스토리지, 가상화 및 비정형 데이터를 포함하여 온프레미스 및 클라우드 환경의 모든 영역으로부터 약 30,000개의 고유한 데이터 포인트를 수집합니다.
- **혁신적**—자율 설계를 위한 5가지 특허 기술과 클라우드를 통한 업데이트를 기반으로 하는 독점 알고리즘이 데이터 포인트를 분석하고 성능, 레질리언스, 사용률을 높일 방법을 추천합니다. 이 분석은 기계가 수행하지만 사람이 정한 정책을 따릅니다. 이렇게 데이터를 활용하여 실행 가능한 해법, 즉 효율 지표를 개선하고 리스크를 최소화하고 오류를 예측하고 감사 및 컴플라이언스를 간소화하는 데 도움이 될 방법을 제시합니다.
- **검증 완료**—NetBackup IT Analytics는 10년 넘게, 그리고 새롭게 추가된 클라우드를 위한 Veritas Alta™ Analytics와 함께 전사적 범위에서 데이터를 수집하고 분석하면서 업계 최고 수준의 확장성과 신뢰성을 고객으로부터 인정받고 있습니다.

베리타스 분석 솔루션의 주요 기능:

- **통합 콘솔에서 다음에 관한 인사이트 제공**
  - 로컬 및 클라우드 백업, 컴퓨팅, 스토리지
  - 클라우드 및 온프레미스 용량, 비용, 사용량
- **차지백**
  - 사용자가 정의한 그룹 기준(예: 애플리케이션, 부서, 코스트 센터)
  - 백업과 클라우드, 컴퓨팅, 스토리지를 포괄하는 사용량
- **용량 계획**
  - 클라우드 비용 및 사용률 기준 예산
  - 사용량 기준 미디어/스토리지 계획

클라우드를 위한 Veritas Alta™ Analytics와 온프레미스를 위한 NetBackup IT Analytics로 클라우드 비즈니스에서 최대 가치 실현

베리타스는 기업들이 여러 가지 이유로 클라우드로 이전한다는 것을 확인했습니다. 소기업은 데이터 센터 또는 재해 복구 사이트를 유지 관리하는 데 따르는 부담을 줄일 수 있습니다. 중견기업은 고확장성 하드웨어에 구현된 접근성이 뛰어난 오프사이트 데이터 스토리지에서 JIT(Just-In-Time) 클라우드 복구 기능을 활용할 수 있다는 점을 선호합니다. 그리고 대기업은 클라우드의 가용성 및 비용 관련 이점을 활용할 만한 워크로드를 선별하는 한편, 고가의 데이터 센터 공간은 미션 크리티컬 워크로드에 사용합니다. 특정 워크로드를 위한 임시 공간이 필요할 때도 있습니다. 그러한 경우 데이터 센터에 디스크 랙을 새로 설치하지 않고 클라우드 제공업체의 공간을 활용함으로써 데이터 센터 하드웨어 추가 구매의 비용 부담을 피할 수 있습니다. 클라우드 서브스크립션 모델은 확장 가능하고 사용하기 간편한 모델인 만큼 이러한 프로젝트에 적합합니다.

데이터를 클라우드로 이동하는 현재의 메가트렌드는 기업의 비용 절감 노력과 밀접한 관련이 있습니다. 이 클라우드 모델은 각종 요구 사항을 민첩하게 수용합니다. 따라서 하드웨어 및 그에 따른 랙과 스택을 구입하지 않고도 쉽고 빠르게 서버에 디스크를 추가할 수 있습니다. 클라우드에서는 데이터 센터와 달리 비용과 시간을 들여 하드웨어와 소프트웨어를 교체하거나 업그레이드할 필요가 없습니다. 클라우드 서비스 제공업체가 이러한 요구 사항을 해결하며, 해당 기업은 관련 내용을 알거나 관리할 필요 없습니다. 클라우드로의 전환을 결정하는 이유가 무엇이든지, 클라우드를 위한 Veritas Alta™ Analytics와 온프레미스를 위한 NetBackup IT Analytics는 온프레미스 환경과 달리 컴플라이언스 및 경제성을 모두 갖춘 경험을 보장할 수 있습니다.

베리타스는 AI 기반 관제 센터를 제공합니다. 따라서 고객은 갈수록 증가하는 클라우드 데이터를 효과적으로 통제할 수 있습니다. 베리타스를 통해 모든 데이터의 위치를 확실히 알 수 있습니다. 모든 엔터프라이즈 데이터를 저장 위치에 상관없이 단일 인터페이스에서 관리하기 때문입니다. 페타바이트 단위의 용량에도 동급 최고의 성능을 제공하면서 손쉽게 확장할 합니다. 그리고 편리한 셀프 서비스 운영 방식으로 ITaaS(IT as a Service)의 토대를 마련합니다. 베리타스는 완전한 데이터 가시성 기술, 지능형 이상 탐지, 악성 코드 검사로 불확실성을 해소합니다. 이 모든 기능이 베리타의 분석 솔루션을 통해 제공됩니다.

클라우드 네이티브 유틸리티 및 포인트 제품에 머무르지 말고 더 폭넓은 관점으로 사이버 보안 및 데이터 보호를 최우선에 두면서 통합 데이터 관리 전략을 마련하십시오.

베리타스와 함께 클라우드를 효과적으로 제어할 수 있습니다.

1. https://www.esg-global.com/ransomware
2. https://www.veritas.com/content/dam/Veritas/docs/reports/GA_ENT_AR_Veritas-Vulnerability-Gap-Report-Global_V1414.pdf

Veritas Technologies 소개

Veritas Technologies는 데이터 보호 및 가용성 분야의 글로벌 선도 기업으로, 포춘 500대 기업 중 87%를 포함한 전 세계 8만여 개 기업에서 베리타스 기술을 기반으로 IT 복잡성을 해결하고 데이터 관리를 간소화합니다. 베리타스 엔터프라이즈 데이터 서비스 플랫폼은 데이터의 위치와 관계없이 데이터 보호를 자동화하고 복구를 조정함은 물론, 비즈니스 크리티컬 애플리케이션의 가용성을 항시 보장하고 기업이 데이터 규제 변화를 준수하는 데 필요한 인사이트를 제공합니다. 더불어 높은 신뢰성과 모든 요구사항을 충족하는 배포 모델을 제공하는 베리타스 엔터프라이즈 데이터 서비스 플랫폼은 800개 이상의 데이터 소스와 100개 이상의 운영체제(OS), 1400개 이상의 스토리지 타깃, 60개 이상의 클라우드 플랫폼을 지원합니다. 보다 자세한 정보는 베리타스 홈페이지(www.veritas.com/kr) 또는 베리타스 트위터(@veritastechllc)에서 확인하실 수 있습니다.

VERITAS

서울시 송파구 올림픽로 300
롯데월드타워 35층
Tel: 02-3468-2100
www.veritas.com/kr

V1627 12/22