Quorum onQ®

Ransomware 119 - 완벽하게 막을 수 없다면 완벽하게 복구하십시오.

Quorum® onQ™ 는 랜섬웨어의 위협에서 기업의 정보서비스와 자산을 보호하기 위해 발표된 최신 제품입니다. 정보서비스의 다운타임을 줄이는 수호신으로 각광받고 있는 온큐의 원클릭 리커버리 기술을 이용해서 랜섬웨어에 감염된 서버를 정상 시점으로 되돌리는 제품입니다.

어떻게 동작하는가?

Quorum® onQ™ 를 네트워크에 연결하고 운영 중인 서버들을 백업합니다. 서버별로 지정된 백업주기에 맞추어서 운영서버들의 백업 스냅샷이 만들어지면 암호화해서 저장합니다. 이후 랜섬웨어 감염사고가 발생하면 백업했던 스냅샷으로 가상머신(virtual machine)을 가동합니다. 5분 이내에 랜섬웨어 감염 서버의 서비스를 정상화합니다. 혹시 랜섬웨어 감염사고상황이 되었을 때 가상머신이 제대로 동작하지 않을 수 있다는 걱정은 온큐에서 필요 없습니다. 백업한 후 자동으로 가상머신의 동작을 자동으로 테스트합니다.

랜섬웨어 감염상황이 발생하면 어떻게 해야하는가?

감염된 서버를 즉시 네트워크에서 분리시켜야합니다. 그래야 다른 서버자원으로 랜섬웨어가 전파되는 것을 막을 수 있습니다. 온큐에서 감염되기 전의 정상상태 백업 스냅샷을 선택하고 해당 가상머신을 가동합니다. 수 분 안에 감염된 서버를 대신하여 온큐가 정보서비스를 정상으로 운영합니다.

> “2년 동안 랜섬웨어 공격이 3번이나 있었습니다. 전부 직원들이 깨끗하다고 생각했던 메일의 첨부문서를 열어서 생긴 일이었습니다. 일이 터질 때 마다 즉시 서버를 네트워크에서 분리시키고 온큐를 이용해서 몇 분 안에 정보서비스를 복구했습니다. 솔직하게 말해서 온큐가 없었다면 우리 회사는 망했을지도 모르겠습니다.”
>
> Confidential Oil and Gas

정보서비스를 즉시 복구

서버가 다운되면 관리자 PC의 웹브라우저에서 클릭 한 번으로 백업했던 어느 시점으로도 돌아가서 즉시 서비스를 켤 수 있습니다.

서비스복구 자동 테스트

실제 장애상황에서 가동할 복제서버가 제대로 잘 동작할지 자동으로 테스트하므로 실제상황에서 가용성을 안심할 수 있습니다.

서버 안심 테스트

소프트웨어 패치나 OS 업그레이드, 서버 운영환경 변경설정 같은 작업을 온큐에서 시험삼아 해본 후 실제 서버에 적용하면 서버를 더욱 안정적으로 운영할 수 있습니다.

서버 이전(마이그레이션;Migration)

빈 서버에 백업한 서버를 OS를 포함하여 전부 복구할 수 있습니다. 또한 서버가 다운된 후 온큐를 대신 운영한 시간 만큼의 분량만 복구할 수 있습니다. 이기종서버로 복구할 수 있으면 가상서버와 전통적 물리서버 모두 지원합니다.

서버 보관(아카이브;Archive)

거의 무한대의 분량으로 얼마 동안의 기간으로도 서버를 아카이브(Archive)할 수 있습니다.

백업(Backup)과 암호화

설치 후 최초 백업에서 응용프로그램과 데이터, OS까지 서버를 통째로 백업한 후 증분백업합니다. 설정가능한 최소 백업주기는 15분이며 백업된 서버는 암호화되어 저장됩니다.

중복제거(Deduplication)와 압축(Compression)

백업하는 서버(Source)와 온큐(Target)에서 모두 중복제거를 합니다.

복제(Replication)

서버실에 있는 온큐에서 원격지의 온큐나 DRaaS로 압축과 암호화 처리 후 복제 전송합니다. 안심전송을 위해 PCI, HIPAA, SOX 등 세계적 권위의 3대 보안인증을 받은 유일한 안심제품입니다

Quorum® onQ™ 는 랜섬웨어에서 안전한가요?

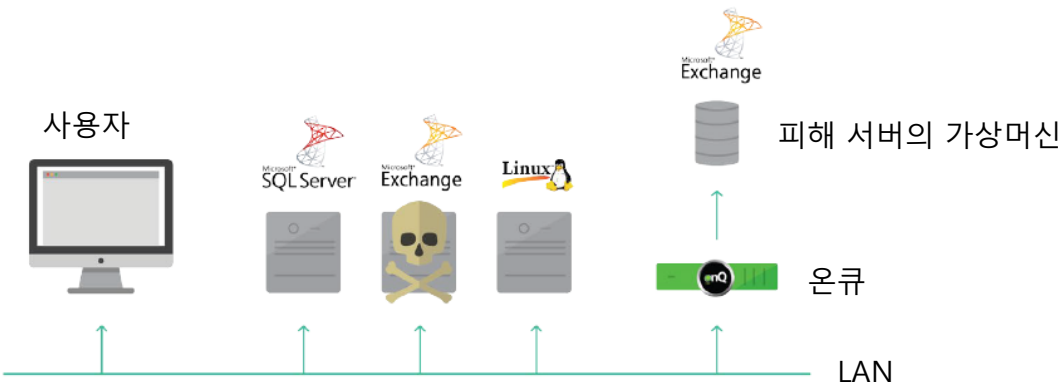
Quorum® onQ™ 는 백업한 스냅샷을 보호하기 위해 몇 가지 안전장치를 가지고 있습니다. 우선, 액티브디렉토리(AD:Active Directory)와 관계없이 별도로 동작하므로 랜섬웨어의 표적이 될 가능성이 떨어집니다. 그리고 온큐는 보안취약성을 대폭 개선하여 안정성이 더욱 강화된 리눅스(Linux) 기반의 장비제품입니다.

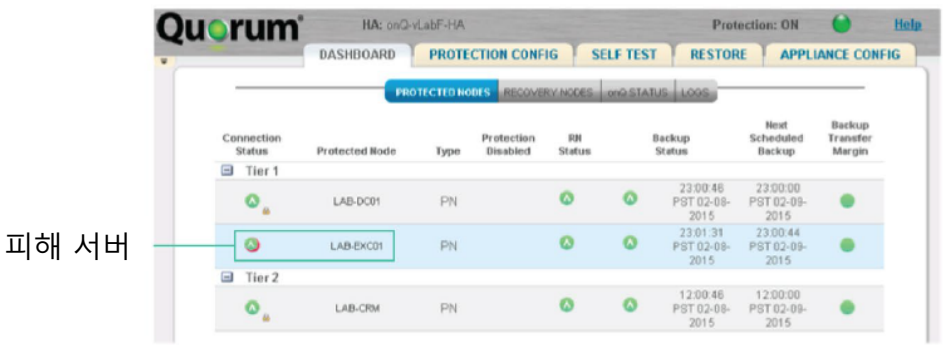
만약 온큐가 랜섬웨어에 감염된 서버를 백업하고 그걸 기반으로 가상머신 자동테스트를 한다고 하더라도 온큐의 자동테스트 기능은 내부 네트워크에서만 동작하므로 실제 운영환경에는 아무런 영향을 주지 않습니다.

온큐는 백업한 모든 데이터를 전송하고 전장할 때 고유의 방식으로 암호화합니다. 따라서 랜섬웨어가 백업한 데이터를 침범할 수 없습니다.

주요 특징

- 다수의 서버를 보호할 수 있는 장비(appliance) 제품
- 4 ~ 24 CPU 코어, 64GB ~ 256GB 메모리, 2U
- 2.5TB ~ 25TB 스토리지
- 데이터 전송과 저장에 모두 암호화
- 내부 테스트 네트워크 운영
- 보안성을 강화한 리눅스 운영체계
- 백업에서 가상머신 가동 자동 테스트
- 서버별 백업 주기 임의 설정





Quorum®