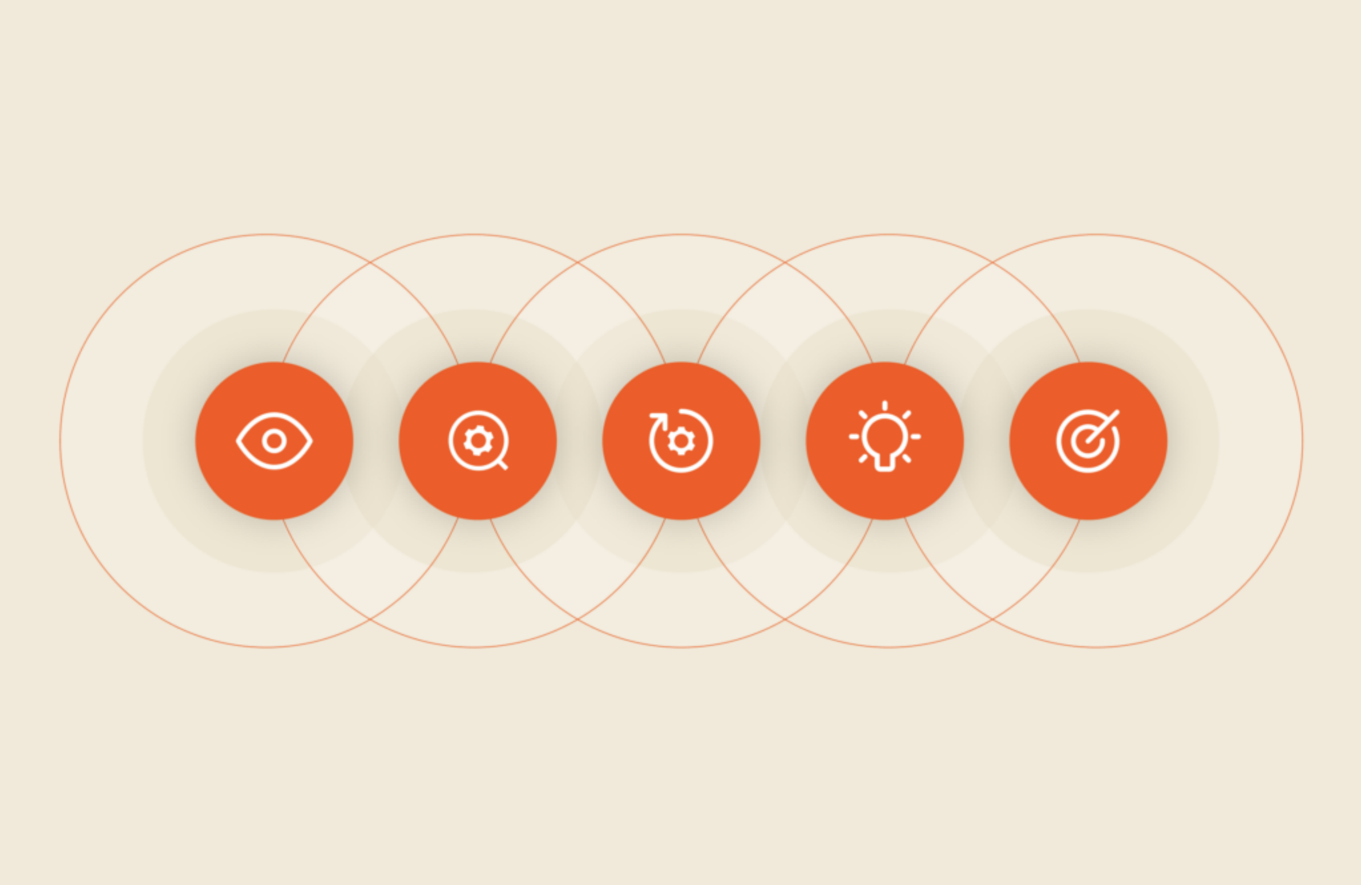
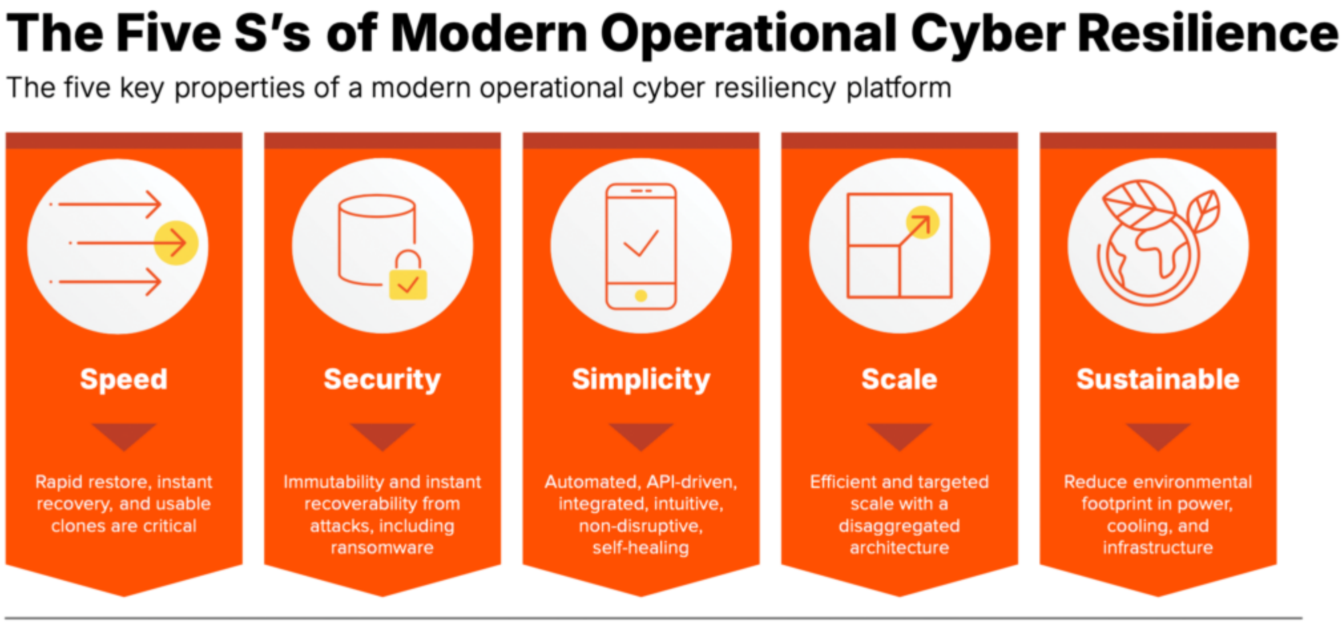


퓨어스토리지의 **5//S** 원칙을 활용한 운영 사이버 복원력 구축

지난 5~10년 동안 사이버 복원력(일명, 비즈니스 연속성 또는 재해 복구)이 크게 변화했습니다. 이전에는 허리케인, 토네이도 또는 고속도로에서의 위험한 유해 물질 유출과 같은 자연 재해 및 운영 재해에 중점을 두었습니다.

오늘날 랜섬웨어, 피싱, 증가하는 에너지 비용, AI를 통한 자동화 및 많은 복합적인 요인들은 공격의 실행 가능성과 빈도를 높이는 동시에, 공격의 복잡성과 실행 시간을 감소시켰습니다. 이러한 악의적인 공격은 사이버 복구로 정의되는 복구 프로세스의 추가 단계를 필요로 합니다. 침해 사고 대응 프로토콜은 공격이 어떻게 발생했는지 이해하고, 데이터가 위협 및/또는 악용된 취약점으로부터 안전한 상태임을 보장합니다.

이처럼 끊임없이 진화하는 위협에 대응하기 위해 조직은 속도, 보안, 단순성, 확장성, 지속 가능성이라는 다섯 가지 핵심 요소를 기반으로 빠른 플래시 기술에 활용한 차세대 데이터 플랫폼이 필요합니다.



이러한 원칙은 중요한 애플리케이션 데이터의 가용성을 보장하여 조직이 자연적 또는 악의적인 사고로부터 신속하게 운영을 재개할 수 있도록 합니다. 안전하고 탄력적인 데이터 기반을 제공하여 신뢰할 수 있는 애플리케이션 및 서비스, 사이버 보안, 그리고 규정 준수 달성과 같은 성과를 가능하게 합니다.

각 항목이 어떻게 적용되는지 살펴보겠습니다.

원칙 1: 속도

> "전쟁에서 핵심은 속도입니다. 적이 준비되지 않은 틈을 활용하세요."
>
> – *Sun Tzu, "전쟁의 예술", 제11장*

공격자들은 여러분이 얼마나 빠르고 완전하게 대응할 수 있는지에 대비하고 있을까요? 속도 원칙은 애플리케이션 스택을 복구하고 사용자에 대한 서비스를 복구하는 데 필요한 시간입니다.

애플리케이션과 환경을 알려진 시점부터 몇 분 또는 몇 시간 내 신속하게 온라인 상태로 복구할 수 있다면, 왜 돈을 지불해야 할까요? 이러한 요구는 재무적 요구일 뿐만 아니라, 규제적 요구 사항이기도 합니다. DORA와 같은 요구 사항이 이러한 타임라인을 주도합니다. 운영 결제 시스템의 경우 2시간은 도전적인 목표이지만, 적절한 기술과 오케스트레이션을 통해 충분히 실현 가능합니다.

퓨어스토리지 고객의 애플리케이션과 데이터는 랜섬웨어에 의해 암호화되었고, 백업에서 복구하는 것만이 유일한 옵션이었습니다. 당시 이들은 퓨어스토리지의 복원력 기능을 아직 구현하지 않은 상태였습니다. 이들은 널리 배포된 디스크 기반 목적 지향 백업 어플라이언스(PBBA)에서 데이터를 복구하기 시작했으며, 기계적 구성 요소가 고장 나거나 손상되지 않기를 바랐습니다. 10일 후, 환경의 약 10%가 복구되었고, 중요한

애플리케이션은 복구되지 않았습니다. 처음부터 재구축하는 것이 실제로 복구를 계속하는 것보다 더 빨랐습니다.

고객은 5S 원칙에 기반한 아키텍처를 구현했으며, 퓨어스토리지가 지원하는 두 가지 핵심 혁신, 즉 SafeMode™ 스냅샷을 사용한 애플리케이션 복구의 계층화된 접근 방식과, 데이터 보호 파트너와 함께 수행한 신속한 복구 기능을 적용했습니다. 이를 통해 약 3시간 내에 분기마다 완전한 데이터센터 복구를 테스트하고 검증할 수 있습니다. 두 번째 공격을 받았을 때는, 퓨어스토리지가 제공한 '정상 데이터 복사본'으로 티어-0 애플리케이션을 약 15분 만에 복구해 온라인 상태로 전환할 수 있었습니다.

원칙 2: 보안

> "...공격적인 작전은 종종 방어의 가장 확실한 수단이며, 어쩌면 유일한 방법일 수도 있습니다."
>
> – 조지_워싱턴

방어력이 우수하면 공격에 성공적으로 대응할 수 있는 최적의 위치에 놓이게 됩니다. 공격자가 공격 비용을 증가시켜 금전적, 정치적 또는 사회적 이익을 기하급수적으로 줄임으로써 공격에 대한 인센티브를 잃기를 원합니다. 공격 초기에 포기하고 물러나기를 바라야 합니다.

퓨어스토리지는 보안 애플리케이션 및 XDR/EDR 시스템과 협력하여 신속하게 조치를 취할 수 있습니다. 퓨어스토리지의 핵심 목표 중 하나는 데이터와 해당 데이터를 목적에 맞게 활용할 수 있도록 하는 애플리케이션의 보안성과 복구 가능성을 확보하는 것입니다. 방어적인 보안 풋프린트는 세 가지 핵심 영역에 관여해야 합니다.

1. 주변 감지: 네트워크 에지에서 발생하는 최초의 방어 장벽입니다. 방화벽, 침입 탐지, VPN 및 다단계 인증과 같은 액세스 제어는 모두 모범 사례입니다. 이를 통해 네트워크와 프로토콜 수준의 애플리케이션을 격리하여 공격으로 인한 피해 확산 범위를 줄일 수 있습니다.
2. 처리 탐지: 이러한 두 번째 방어 계층을 통해 애플리케이션 소비자의 행동을 실시간으로 평가할 수 있습니다. "이 프로세스가 올바르게 작동하고 있는가?" "이 사용자의 행동 또는 상호작용 프로필에 변화가 있었는가?" 이러한 질문은 공격이 진행 중인지 판단하기 위해 SIEM 시스템에서 수행됩니다.
3. 지속성 감지: 이를 통해 스토리지 시스템의 데이터에 활성 또는 잠재 위협이 있는지 평가하고, 데이터의 알려진 복사본을 거의 즉각적으로 복구할 수 있습니다.

지속성 계층에서 인프라 시스템은 두 가지 기능적인 정의, 즉 삭제 불가능성과 불변성을 충족해야 합니다. 이러한 속성은 권한이 있는 공격자가 사전 정의된 보존 기간이 완료되기 전이나 대역 외 수동 승인 프로세스 없이 시스템의 보안 태세를 변경하거나 시스템의 데이터를 제거할 수 없도록 합니다. 퓨어스토리지에서는 이러한 영구성 강화 계층을 'SafeMode'라고 부르는데, 이는 불변성 계층과 볼륨 스냅샷을 기반으로 하여 데이터의 특정 시점을 변경 불가능한 형태로 보존합니다.

원칙 3: 간소화

"우리는 훨씬 더 포괄적이고 단순한 무언가를
만들기 위해 노력했습니다. 처음 문제 해결을 시작할 때, 가장 먼저 찾아낸 해결책은 매우 복잡하며, 대부분의 사람들이 거기서 그만두고 있습니다. 하지만 계속 진행하면, 매우 우아하고 간단한 솔루션을 얻을 수 있습니다. 대부분의 사람들은 그 목표를 달성하기 위해 시간이나 에너지를 투자하지 않습니다."

– 스티브 잡스, *"Newsweek"* 인터뷰, *2006*년 *10*월 *14*일

이 만트라는 Apple의 "iDevices"를 성공적으로 만들었습니다. 유감스럽게도, 단순성은 매우 어렵습니다. 퓨어스토리지의 핵심은 간소함으로, 팀은 비즈니스에 혁신적이고 중요한 것에 집중할 수 있습니다. 팀은 경보와 오탐에 압도되어 서로 다른 시스템을 보호하고 현대적인 보안 툴, 레거시 아키텍처의 기술적 부채 또는 제대로 구축되지 않은 시스템의 일상적이고 반복적인 작업을 적용하기 위해 애쓰고 있습니다.

시스템을 간단하게 구축할 수 있다면 어떨까요? 간단한 작동? 자가 치유? 낮은 수준의 LUN 관리가 필요하지 않았나요? 알려진 데이터 복사본을 식별할 수 있을까요? 아니면 어떤 데이터가 침해되었습니까? 공격이 탐지되면 애플리케이션과 서비스를 보호하기 위해 자동화 워크플로우를 트리거할 수 있을까요?

물론, 이를 통해 더 많은 애플리케이션을 사용할 수 있고, 중대한 사고는 줄어들 것입니다. 이러한 사고방식과 기술의 변화로 무엇을 구축할 수 있는지 상상해 보세요.

원칙 4: 유연한 확장

"엔지니어링은 세상에 존재하는 마법과 가장 가까운 것입니다."

– 일론 머스크

가장 까다로운 엔지니어링 과제 중 하나는 규모입니다. 환경이 고정된 양의 리소스로 제한될 때, 이를 최적화하는 것은 비교적 간단합니다. 워크로드, 소비 및 활용은 제한될 수 있으므로 서비스 수준을 보장할 수 있습니다. 오늘날의 인터넷스케일 시스템은 새로운 패러다임을 만들었습니다. 우리는 새로운 기법을 배우고, 기존 해답을 넘어 성장하며, 이전에는 고려하지 않았던 방식으로 혁신해야 합니다.

애플리케이션과 데이터의 확장은 프로토콜 계층, 네트워크 계층, 메타데이터 계층 및 스토리지 지속성 계층에서의 혁신의 조합입니다. 기존 "파일 시스템"이라는 용어와 개념이 이제 확장 가능하고 고성능 시스템을 구축하는 방식과 맞지 않기 때문에, 저는 "스토리지 지속성 레이어"라는 표현을 사용합니다. 이 분야의 새로운 혁신은 프로토콜 계층에서 그러한 개념을 추출하고 키-값 저장소와 같은 새로운 기법을 사용하여 확장성과 내구성을 보장합니다.

네트워크 규모는 데이터센터에 상당한 문제입니다. 프로비저닝된 각 포트는 전력, 냉각 및 랙 공간 등 필요한 자본, 운영 원시 데이터센터 비용을 수반합니다. 이를 개선하는 한 가지 방법은 데이터 스토리지와 네트워크 포트가 독립적으로 확장되도록 하는 것입니다. 이러한 구성 요소를 분리함

으로써 스토리지 확장은 인프라 비용 증가가 아닌, 용량, 트랜잭션 및 처리량 증가에 집중할 수 있도록 합니다.

미국의 한 대형 은행은 백업 복구를 위한 SLA를 충족하지 못했습니다. 현재 시스템은 700개 이상의 10Gb 네트워크 포트를 사용했으며 시기 적절한 복구 처리량을 제공할 수 없었습니다. 퓨어스토리지는 사이버 복구 파트너 중 한 곳과 함께 네트워크 포트 수를 100개 미만의 10Gb 네트워크 포트로 줄이고 복구 SLA를 크게 초과하는 솔루션을 제공했습니다. 이 은행은 공간, 인프라 비용 및 데이터센터 비용을 절감했으며, 이후 시스템을 여러 번 확장했습니다.

오늘날의 네트워크 대역폭은 이를 처리할 수 있는 플랫폼에 새로운 기능을 제공할 수 있습니다. 스토리지, 컴퓨팅 및 네트워크 리소스 등 시스템의 임의 규모를 고려한 아키텍처 모델이 필요합니다.

프로토콜과 API는 이러한 분산 아키텍처에서도 중요합니다. 복원성 애플리케이션은 엔드포인트(예: S3 프로토콜 클라우드 스토리지 소비자를 위한 URL)에 연결하기만 하면, 서비스는 모든 컴퓨팅, 네트워크 및 가용 스토리지 리소스 전반에서 자동으로 연결의 균형을 유지합니다. 특별한 구성이나 기법이 필요 없습니다. Evergreen이 작동하기 때문에 데이터를 마이그레이션하거나 다시 가동 중단을 겪을 필요가 없으므로 확장성과 서비스 가용성의 한계를 높일 수 있습니다.

원칙 5: 지속가능성

> "미래를 이해하기 위한 핵심은 지속가능성입니다."
>
> – 패트릭 딕슨, "미래형"

지속 가능성은 전력 및 냉각 비용, 운영 노력 또는 특정 작업에 필요한 구성 요소 등 시스템을 실행하고 유지하는 데 필요한 리소스의 합계를 의미합니다. 리소스를 줄이면 시스템과 솔루션의 지속가능성이 직접적으로 향상됩니다. 에너지 비용이 증가함에 따라, 복원력은 차세대 효율성으로 자원의 한계를 뛰어넘는 것을 의미합니다.

"모던 스토리지가 데이터센터의 전력 활용을 상쇄하는 방법"에 대한 이 기사에서는 특별히 제작된 DirectFlash® 모듈이 어떻게 엄청난 에너지, 바닥 공간 및 관련 냉각 비용을 절감하는지 알아봅니다. 영향을 받는 것은 스토리지 비용과 성능에만 그치지 않고, 인프라와 관련된 모든 운영 비용에까지 확장됩니다.

저는 고객들이 이를 통해 새로운 핵심 프로젝트의 데이터센터 경제성을 실현하는 것을 목격했습니다. 34개의 랙을 4개의 랙으로 통합하여 랙, 인프라 및 모든 관련 유틸리티를 88% 절감했습니다! 멀티엑사바이트 규모의 동영상 제공업체 한 곳은 모든 데이터센터에서 메가와트에 달하는 전력을 절감하고, 네트워크 포트 요건과 인프라는 크게 감소할 수 있습니다. 비용 및 리소스를 절감하여 더 나은 고객 경험을 제공하는 동시에 중요한 차세대 혁신을 위한 리소스를 확보합니다.

퓨어스토리지 플랫폼은 직원의 지속가능성에도 영향을 미칩니다. 5S 원칙에 기반한 사이버 복원력 아키텍처를 구축한 후, 원칙 1에서 앞서 언급한 회사의 직원들은 이 정도 수준의 애플리케이션 복구 능력이 없다면 다른 곳에서는 일하지 않겠다고 말했습니다. Evergreen과 함께하면, 전면 교체 업그레이드 및 데이터 마이그레이션으로 인한 위험은 과거의 과제이며, 변경 관리 회의, 마이그레이션 계획, 예정된 애플리케이션 중단, 부품 교체 및 기타 운영 노력도 마찬가지입니다.

결론

> “다른 사람들이 사용할 수 있는 좋은 도구를 구축하는 데 큰 만족이 있습니다.”
>
> – 프리만 다이슨, “유니버스를 방해하다”

5S는 사이버 복원 아키텍처에 적용될 때 고객에게 더 나은 서비스와 경험을 제공할 수 있는 핵심 속성입니다. SLA를 대폭 개선하고, 비용과 복잡성을 줄이며, 리소스를 확보하여 다음 번 대규모 프로젝트를 처리할 수 있습니다.

퓨어스토리지 팀에 문의하여 사이버 복원력 전문가와 상담하고 5S 원칙이 어떻게 도움이 되는지 알아보세요.