CLOUDFLARE

백서

다가오는 희망:

불확실한 경제 상황에서 더 나은
사이버보안 환경을 구축하는 방법

내용

핵심 요약

경제 전망이 점점 더 예측할 수 없게 되면서, 조직은 경제적인 불확실성을 겪고 있습니다. 이렇게 상황이 불확실하면 예산이 축소되는 경우가 많고, CIO와 기술 리더는 새로운 길을 찾아야 한다는 압박을 느낍니다.

다행히, 리더가 예산을 선제적으로 다시 배정하고, 효율성을 중심으로 프로세스를 재정의하며, 리소스를 크게 늘리지 않고도 계획했던 성장을 지속적으로 추구하여 고비를 넘길 전략을 세운다면 불확실성의 시대가 지나갔을 때 경쟁 우위를 확보할 수 있을 것입니다.

다음 섹션에서는 이러한 상황과 시장 여건을 유발한 여러 요소를 자세히 살펴보겠습니다. 이렇게 얻은 통찰력을 바탕으로, 리더가 보안 상태를 손상시키지 않으면서 현재 보안 환경의 효율을 높일 수 있는 기회를 찾는 데 유용한 다섯 가지 단계를 정의해 보겠습니다. 새로운 경제 환경에 맞게 IT 인프라 전략을 조정하는 리더는 미래의 성공을 준비하도록 조직을 이끌어나갈 수 있습니다.

소개

지난 몇 년 동안 위기가 거듭되면서 IT 리더는 전략을 세우고 실천해야 했습니다. 글로벌 팬데믹과 팬데믹이 후속적으로 미친 영향, 공급망 부족, 동유럽의 고조되는 갈등과 같이, IT 리더는 경제 위축을 유발하는 요인에 대처해야 했습니다. 스탠포드 경제학자 Paul Romer는 "위기를 낭비하는 것만큼 끔찍한 일은 없다"(출처) 라고 말했습니다. CIO는 원격 근무를 지원하기 위해 선택을 내렸고, 의도치는 않았지만 기업에서 원격 근무를 지원하는 데 매력을 느끼게 되었다는 장기적인 이점으로 이어지고 있습니다. 경제 전망이 어두운 지금도 이와 같이 보안, 네트워킹, 원격 액세스, 스토리지, 개발, 인프라에 대한 리더의 선택은 결국 미래의 큰 성장을 안정적으로 달성하기에 더 유리하고 강력한 위치를 점하는 데 도움이 될 것입니다.

매출에 미치는 영향, 규모 및 정교함에 대한 새로운 벤치마크가 구축될 정도의 랜섬웨어와 정교한 사이버 위협이 대유행하면서 원격 근무도 떠올랐습니다(출처). 네트워크 경계로 남았던 부분이 사라지고 직원 이직률도 역사적으로 증가하면서 보안 격차가 생기고 전략적 IT 프로젝트가 지연되었습니다. 이로 인해 조직은 채용 및 직원 유지에 관한 방식뿐만 아니라 시스템 및 컴퓨터 액세스 제어 방식까지 고민해야 했습니다. 팬데믹이 어머어마한 사이버 범죄를 초래했다곤 하지만(출처), 조직 및 이사회에서 효율적인 사이버 보안의 긴급한 필요성을 인식할 계기가 되기도 했습니다. 이제, 조직에서는 안전하고 생산적이면서 가용성도 뛰어난 하이브리드 업무 인프라를 구축한다는 장기적인 계획에 더 전략적으로 접근해야 합니다.

예산에 맞게 비즈니스 위험을 완화하고 곧 닥쳐올 위협에 조직이 효과적으로 맞설 수 있도록 행동할 수 있는 다섯 가지 조치를 소개합니다.

1. 기존 보안 도구를 감사하여 중첩되는 기능을 파악하세요

조직이 보안 벤더를 통합하여 얻을 수 있는 이익은 많습니다. 단 하나의 도구로 CISO의 마음에 들 '묘책' 솔루션을 구축할 수는 없지만, 보안 솔루션을 사용 중인 여러 기업에서는 현재 최적의 방어 능력을 구축하지도 못한 채로 너무 많은 도구를 사용하며 돈을 낭비한다고 생각합니다. 다양한 벤더의 여러 가지 도구를 지원하려면, 직원의 소중한 업무 시간을 단절되어 있는 여러 시스템과 관련한 조달, 구현, 관리, 문제 해결, 지원 업무에 낭비하게 되고, 인프라 및 데이터 보안 업무에는 시간을 들일 수 없게 됩니다. 실제로 2022년 6월, 연례 RSA Conference에서 진행한 설문에 따르면 "응답 기업 중 절반 이상(53%)이 사이버 보안 예산의 50% 이상이 낭비되고 있고 여전히 위협을 완화하지 못하고 있다고 답했습니다. 또한, 43%의 응답자가 위협 감지 및 완화와 관련한 가장 큰 문제로 도구의 과잉을 꼽았고, 10%의 조직이 사이버 보안 위협을 완화하는 데 효과적인 도구가 부족하다고 답했습니다"(출처). 도구를 일부분만 처분하더라도 직원의 소중한 시간을 아끼면서 보안까지 개선할 수 있습니다.

자본 지출에서 운영 비용으로 투자를 전환하면 단기 현금 흐름이 즉각 개선될 뿐 아니라 다년간의 자본 투자에 발이 묶여 비즈니스 민첩성이 저하되는 사태도 피할 수 있습니다. 간소화 방법 중 하나는 기존 하드웨어에 대한 의존성을 줄이는 것입니다. 레거시 장비에서 서비스형 솔루션으로 전환하면 예산이 줄더라도 최우선 이니셔티브에 자금을 계속 투입할 수 있습니다. 서비스형 모델에 투자하면 근본적으로 더 빠른 소프트웨어 혁신 주기라는 이점을 누릴 수 있고, 레거시 하드웨어의 피할 수 없는 약점인 잦은 패치도 필요하지 않습니다. 패치를 없애고 혁신을 추진하면 팀이 진정한 비즈니스 차별 우위를 높일 활동에 집중할 수 있습니다. 불확실한 상황에서 전략적으로 간소화하고 통합하면 장기적인 성공을 달성하는 데 크게 도움이 됩니다.

2. 단순한 도구가 아닌 데이터에 집중하세요

리더십 팀이 패턴과 이상 상황을 더 효율적으로 파악하려면, 단순한 도구 통합이 아니라 보안 도구 세트 전반에서 데이터를 통합하는 데 집중해야 합니다. 여태까지 보안 팀에서는 너무 많은 위치에 너무 많은 데이터세트를 보유할 때 어떠한 장기적인 영향이 있을지 고려하지 못한 채로, 갈수록 더 많은 도구들을 추가해 왔습니다. 이렇게 상호 운용성 및 데이터 투명성이 부족한 채로 여러 제품을 짜깁기하게 되면서, 사람의 실수가 발생할 확률이 높아져 정확도가 낮아지고 통찰력까지 약해지는 부작용을 낳는 경우가 많습니다. 여러 데이터세트를 불러와 합치고 쿼리를 실행하는 데 걸리는 시간은 그 자체로 팀에게 낭비지만, 당연히 리소스 측면에서도 낭비입니다. 리소스를 낭비하지 않았다면 더욱 전략적인 비즈니스 이니셔티브에 투입할 수도 있었을 것입니다.

수동으로 데이터세트를 합치는 문제나 CSV 가져오기 및 내보내기 같은 상호 운용성 문제를 창의적으로 해결할 방법을 팀에서 찾아낼 수도 있겠지만, (효율성은 그렇다 치더라도) 보안 도구의 가치는 데이터를 수집하고 생성해 방어 기능에서 이용할 수 있도록 만드는 데 있다는 점을 고려해야 합니다. 데이터가 분류되지 않고, 보호되지 않으며, 제대로 관리되지 않은 채로 모든 곳에 분산되어 있다면 그 데이터에서 유의미하게 뽑아낼 수 있는 인사이트가 왜곡될 수 있습니다. 전적으로 배제되었을 수 있는 섀도우 IT 인스턴스에 데이터가 있다면 더욱 그렇습니다. 도구 세트를 통합하고 보안 스택의 상호 운용성을 신중하게 고려하면 사람에 의한 오류를 줄이고 데이터 보안을 강화할 수 있습니다. 지금 제공되는 최고의 도구에 투자하더라도, 데이터 세트와 섀도우 데이터 세트가 사일로화되면 인사이트가 힘을 잃게 되기 때문입니다.

효율성의 측면에서 생각하면, Zero Trust(“절대 믿지 말고 항상 인증하라”) 시대에는 도구가 많을수록 팀이 업무를 시작하기도 전에 로그인, 인증, 시스템 액세스 획득에 더 많은 시간을 들여야 합니다. 직원이 다루어야 할 시스템이 줄어들면 시간을 절약하고 더 빨리 업무를 처리할 수 있습니다. 시스템 내의 데이터뿐 아니라 업무를 처리하기 위해 액세스해야 하는 시스템의 수에 따라, 팀이 위협에 사후 반응하게 될지, 시기 적절하게 위협에 대응할 능력을 갖추게 될지 결정된다는 점을 반드시 알아야 합니다.

3. 서비스형 클라우드 모델을 추구하여 혁신을 극대화하고 복잡성을 최소화하세요

경쟁력을 유지하려는 모든 기업은 혁신해야 하지만, 사이버 보안 업계에 속해 있지 않은 회사라면 전체 인프라를 안전하게 보호하는 데 필요한 최신 CVE, 공격 동향, 중요 패치를 바로 바로 적용하기에는 시간, 예산, 리소스가 부족합니다. 가능한 만큼 서비스형 모델을 도입하는 리더는 타협점을 찾거나 기술 부채와 관련한 결정을 어렵게 내릴 필요 없이 지속적인 혁신의 이점을 누릴 수 있습니다.

트래픽 제한을 초과하면 초과 비용을 부과하는 보안 서비스도 있고, 대역폭 수수료를 부과하는 보안 서비스도 있다는 것을 알고 있어야 합니다. 조직에서 월 또는 연 단위로 지불하는 비용을 철저히 검토하여 생각보다 지출 비용이 많은지 파악해보세요. 비용이 생각보다 많다면, 비용을 절감하면서도 장기적으로 더 쉽게 예측할 수 있도록 초과 비용이 없는 다른 솔루션을 찾아보세요. 팀이 더 건설적인 미래를 계획할 수 있게 됩니다. 조직에서 이러한 종류의 클라우드 기반 서비스를 이용한다면 필요한 만큼 여유 있게 늘리고 줄일 수 있습니다. 값비싼 하드웨어와 하드웨어에 수반되는 수명 주기 관리에 얽매일 필요가 없습니다. 불확실성의 시대에 기업에서는 변화하는 시장 환경에 민첩하게 바로 대응할 수 있어야 합니다. 현금 흐름이 우려될 때 비용을 최소화하거나 덜어내는 능력이 있다면 시장의 상황이 어떻든, 힘들게 생존하는 조직과 번성하는 조직 간의 차이를 만들어낼 전략적 이점이 됩니다.

4. 직원 경험을 개선하세요

포브스지에서는 “설문 결과에 따르면 복잡한 다단계 로그인 프로세스는 직원을 짜증나게 하고, 업무 시간을 낭비하며, 생산성을 떨어뜨리고, 중요한 업무 관련 작업들을 포기하게 만듭니다. 정말 아이러니한 점은 응답한 직원 중 40%가 부담스러운 로그인 프로세스 때문에 새로운 업무 보안 앱을 설정하는 일을 미루거나 다른 사람에게 맡겼거나 아예 생략했다고 답한 겁니다. 돈을 주고 살 수 있는 가장 강하고 크고 안전한 대문(레이저 불을 뿜는 용이 지키는 문 같은 것)으로 집을 보호하면서 정작 밤에는 문을 잠그지 않고 내버려두는 것과 같은 일입니다.”라고 밝혔습니다. 어떤 도구가 어떤 기능을 갖고 있는지 일일이 확인하는 일은 방어 담당자에게 비효율적이고 어려운 일이기도 하지만, 대시보드가 너무 많고 데이터도 너무 많은 곳에 위치한다면 어떤 조직이든 중요한 보안 위험과 가시성 부족 문제를 겪을 수밖에 없습니다. 사이버 보안 위협에 앞서고 싶은 기업이라면 클릭 한 번, 키 입력 한 번조차도 중요한 이벤트에 대응하는 데 필요하여 소중한 시간, 에너지, 집중력을 소모할 수 있다는 점을 이해해야 합니다. 더 효율적이고 간소화된 직원 경험을 구현하려면 방어 전문가가 작업을 효율적으로 처리하기 위해 사용해야 하는 도구가 몇 개나 되는지, 중요한 보안 이벤트가 발생했을 때 사후에 대처하지 않고 시기 적절하게 대응하는 데 필요한 시간을 줄이려면 무엇을 없애고 무엇을 통합해야 하는지 리더십 팀에서 철저하게 검토해야 합니다.

기술 외 업무를 맡은 직원이나 방어 전문가가 아닌 직원이 원격 근무를 하면서 개인 생산성을 높이려고 섀도우 IT나 우회 방법에 의존하게 될 수도 있다는 점도 인식해야 합니다. 특히 원격 근무 환경에서 Zero Trust 제어는 조직을 더 안전하게 만들 확실한 방법을 제공해 주지만, 분명 모든 Zero Trust 접근법이 똑같이 만들어진 건 아닙니다. 필요한 시스템에 액세스하는 방식이 복잡할수록 직원이 보안 수단을 고수하기보다 우회 방법을 찾을 가능성도 높아집니다. 리더는 보안 제품의 효과뿐 아니라 사용 편의성까지 고려해야 합니다. 직원 경험을 무시하면 결국 조직의 전반적인 위험이 증가할 수밖에 없기 때문입니다.

5. 네트워크 성능을 희생시키지 않는 보안 서비스를 찾아보세요

도구만의 문제가 아닙니다. 차이를 만들어내도록 도구를 구성하고 관리하는 방법이 중요합니다. 팀의 현재 구성과 맞춤 설정을 감사하여, 성능 개선에 도움이 될 만한 기회를 파악해보세요. 성능을 개선할 수 없다면 처음부터 성능에 중점을 둔 솔루션을 찾아보세요. 성능이 뒷전인 솔루션으로는 리더가 이루려는 목표를 쉽게 달성할 수 없습니다. 네트워크 성능에 관한 한, 질낮은 아키텍처로는 코드 이상의 성능을 보일 수는 없다는 점을 염두에 두세요. 건물의 기초가 이미 완성된 후에는 청사진을 다시 설계하기 어려운 것과 마찬가지로 네트워크도 궁극의 성능을 구현하려면 처음부터 다시 설계해야 합니다. 소스와 가장 가까운 곳에서 데이터를 처리하는 글로벌 에지 네트워크의 성능을 이용할 수 있는 조직은 현재는 물론 미래에도 전략적 이점을 확보할 수 있습니다. MIT Technology Review에 따르면 “대량의 데이터를 처리하면 성능 문제가 발생할 수 있습니다. 이러한 문제에 대응해 많은 조직은 소스와 가까운 곳에서 데이터를 처리하는 에지 컴퓨팅으로 전환하여, 신속하게 실시간으로 분석하고 대응하면서 개인 정보 보호 및 보안 요건까지 충족하고 있습니다”(출처). 미래를 생각한 아키텍처 위에 이미 구축되어 있는 솔루션을 전략적으로 선택한다면, 개인 정보 보호 및 보안의 핵심 요소를 희생하지 않으면서 팀에게 더 나은 네트워크 성능이라는 전략적 이점을 안겨줄 수 있습니다.

요약해보면, 불확실성의 시기에 다음의 단계를 밟아 더 나은 사이버보안 환경을 구축할 수 있습니다.

1. 기존 보안 도구를 감사하여 중첩되는 기능을 파악하세요

- 중첩되는 도구를 통합하세요
- 자본 지출에서 운영 비용으로 투자를 전환하세요

2. 단순한 도구가 아닌 데이터에 집중하세요

- 도구의 상호 운용성은 더 효율적이고 더 정확한 데이터세트로 이어집니다
- 데이터세트 및 보고 기능이 더 정확해지면 더 나은 인사이트를 확보할 수 있고, 이는 비즈니스 목표를 달성하는 데 핵심입니다

3. 서비스형 클라우드 모델을 추구하여 혁신을 극대화하고 복잡성을 최소화하세요

- 사이버보안 업계에 있는 기업이 아니라면 패치를 없애고, 서비스형 솔루션으로 업그레이드해 관리한다면 많은 이점을 누릴 수 있습니다
- 클라우드 및 서비스형 모델은 급변하는 경제 상황 속에서 민첩성을 갖추는 데 필요한 유연성을 제공합니다

4. 직원 경험을 개선하세요

- 너무 많은 도구가 너무 많은 위치에 분산되어 있으면 보안 사각지대와 직원의 불만이 생겨날 수 있기 때문에 이를 통합하여 간소화하면 직원 경험을 최적화할 수 있습니다
- 직원 편의성을 최적화하면 직원 유지율 향상에 도움이 되고, 업무를 위해 섀도우 IT에 의존하는 일을 방지할 수 있습니다

5. 현재의 사이버 보안 스택에 감춰져 있는 비용과 성능 개선 기회를 파악하세요

- 기존 도구를 감사하여 성능을 최적화할 기회를 찾아보세요. 하지만 질낮은 아키텍처를 최적화할 수는 없다는 점을 기억하세요
- 예상 고객 위치와 가장 가까운 곳에 구축된 도구를 도입하면 조직에서 더 뛰어나고 안전한 고객 경험을 제공할 수 있습니다

Cloudflare가 도움을 드리는 방법

Cloudflare는 2008년 경제 위기의 여파가 아직 남아 있던 2010년부터 온프레미스 인프라에서 클라우드로의 전환을 주도하고 있습니다. 더 나은 인터넷 환경을 구축하는 데 일조한다는 대담한 목표로 Cloudflare 플랫폼을 구축했습니다. Cloudflare의 제품군은 하드웨어 추가, 소프트웨어 설치, 코드 변경 없이 인터넷에 연결된 모든 것을 보호하고 성능을 가속화합니다.

Cloudflare가 구동하는 인터넷 자산은 Cloudflare의 지능형 전역 네트워크를 통해 라우팅된 모든 웹 트래픽을 보유하고 있으므로 요청이 있을 때마다 더 스마트해집니다. Cloudflare는 고객이 더 스마트하게 일하고, 더 나은 환경을 구축하고, 더 빨리 실행하며, 안전하게 성장할 수 있도록 돕습니다. 현재 Cloudflare는 수백만 인터넷 자산을 보호하고 가속화합니다.

제어

정책 제어 권한은 그대로 남겨두면서도 포괄적인 연결성, 보안, 컴퓨팅 성능을 제공하는 통합 전역 네트워크의 힘을 누려보세요.

유연성

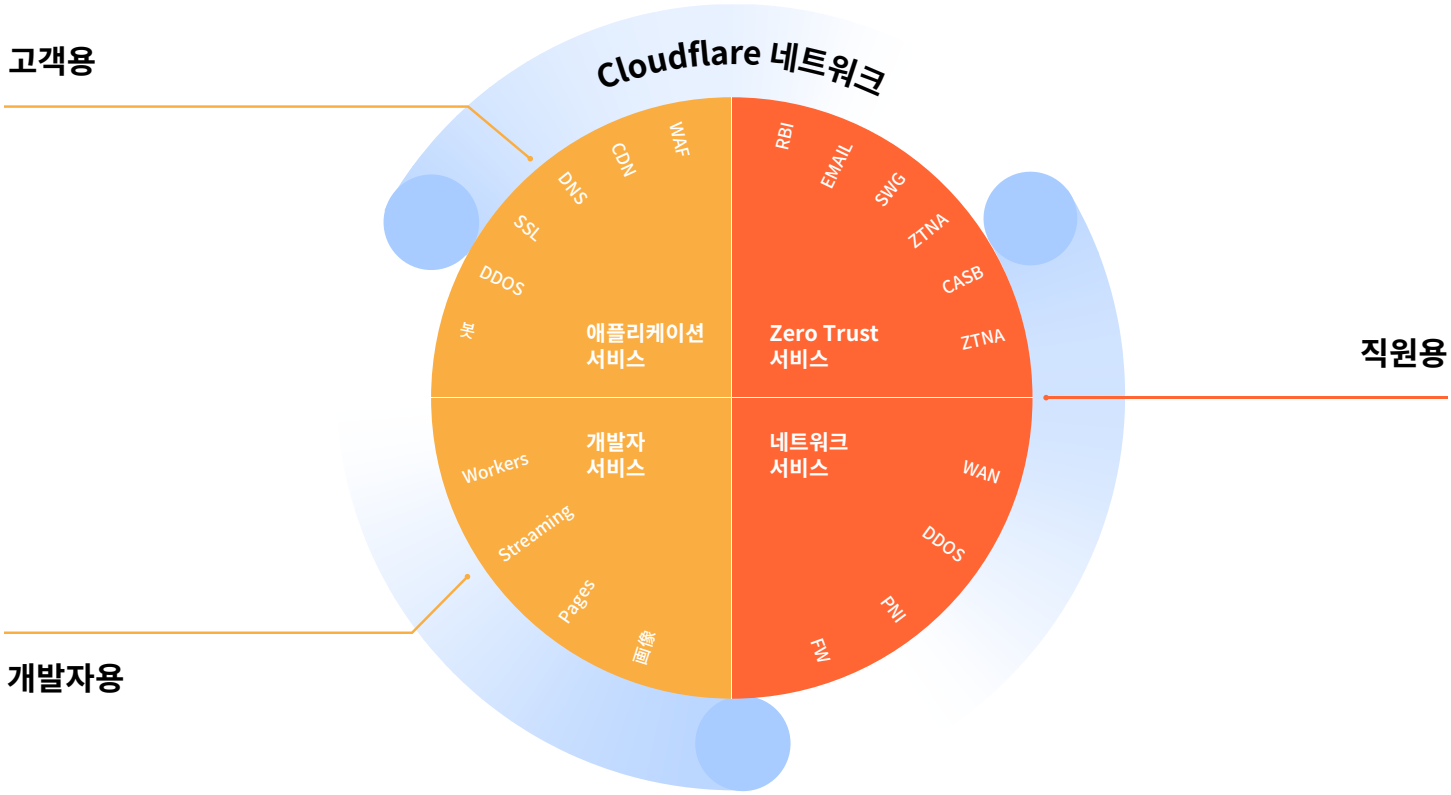
클라우드 네이티브 서비스를 이용하면 자본 지출 투자가 사전에 필요하지 않습니다. 변화하는 비즈니스 상황에 맞춰 사용량을 쉽게 늘리거나 줄여보세요.

예측 가능성

무한히 늘어나는 송신료 등 뜻밖의 비용 없이 청구액을 예측할 수 있습니다. 내년에 제공되는 하드웨어를 위해 자본 지출이 필요하지 않습니다.

Cloudflare 전역 네트워크는 인터넷에 연결하는 모든 것을 보호하고, 비밀을 유지하면서, 신속하고 안정적으로 만들어줍니다.

- 보안 - 웹 사이트, API, 인터넷 애플리케이션의 보안을 유지합니다
- 보호 - 기업 네트워크, 직원, 장치를 보호합니다
- 작성 및 배포 - 네트워크 에지에서 실행되는 코드를 작성하고 배포합니다



Cloudflare 정보

Cloudflare는 2010년부터 온프레미스 인프라에서 클라우드로의 전환을 주도하고 있습니다. 더 나은 인터넷 환경을 구축하는 데 일조한다는 대담한 계획을 바탕으로 Cloudflare 플랫폼을 기초부터 구축했습니다. Cloudflare의 플랫폼은 하드웨어 추가, 소프트웨어 설치, 코드 변경 없이 모든 인터넷 애플리케이션이 온라인 상태를 유지할 수 있도록 보호하고 가속화합니다.

Cloudflare에서 구동하는 인터넷 자산은 Cloudflare의 지능형 전역 네트워크를 통해 라우팅된 모든 웹 트래픽을 보유하고 있으므로 요청이 있을 때마다 더 스마트해집니다. Cloudflare는 고객이 더 스마트하게 일하고, 더 나은 환경을 구축하며, 더 빨리 실행하고, 안전하게 성장할 수 있도록 지원합니다. 현재 Cloudflare에서는 수백만 인터넷 자산을 보호하고 가속화합니다.

자세한 정보는 www.cloudflare.com을 참조하세요.

007-9814-2030-192 | enterprise@cloudflare.com | cloudflare.com/ko-kr

REV:BDES-4771.2023OCT4