Google Workspace

더 안전한 대안

Microsoft에서 심각한 사이버 보안 사고가 발생함에 따라, Google Workspace는 더 안전한 대안을 제공하고자 합니다.

목차

핵심 요약

Microsoft의 지속적인 보안 문제는 최근 고객을 위험에 빠뜨리며 세간의 많은 이목을 끈 일련의 사고로 더 이상 간과할 수 없는 단계에 이르게 되었습니다. 2023년 여름, Storm-0558로 알려진 그룹에 의해 22개의 조직, 500명 이상의 개인, 수만 개의 이메일을 포함하여 미국 및 영국의 고위 공무원 계정이 침해되는 사고가 발생했습니다. 이로 인해 미국 국토안보부의 사이버 안전 검토위원회(CSRB)는 데이터 침해를 초래한 Microsoft의 "연쇄적인 보안 실패"[1]에 대한 세부정보 보고서를 발표했습니다. 이 보고서에서는 장기적인 시스템 문제와 "기업 보안 투자와 엄격한 위험 관리 모두를 우선시하지 않는 기업 문화"에 대한 세부적인 내용을 설명합니다.[2]

사이버 보안 및 인프라 보안국(CISA)는 Storm-0558 침해 사고가 발생한 지 불과 몇 달 후인 2023년 11월에 발생한 별도의 Microsoft 정보 유출 사고에 대응하기 위해 긴급 지침 ED 24-04를 발표하면서 다음과 같은 내용을 전했습니다. "국가 차원의 후원을 받는 Midnight Blizzard라고 알려진 사이버 공격자가 Microsoft 기업 이메일 계정을 도용하는 데 성공하여, 연방 민간 행정부(FCEB) 기관과 Microsoft 간의 이메일 서신이 유출되었습니다."[3]

Microsoft의 보안 문제가 반복적으로 발생함에 따라, 기업과 공공부문 조직 모두에게 더 나은 대안이 필요해졌습니다. Google은 입증된 엔지니어링 우수성, 최첨단 방어 기능에 대한 집중적인 투자, 고객에게 보안을 제공하는 것을 중대한 책임으로 여기는 투명한 문화를 갖춘 Google Workspace가 더 안전한 대안이라고 생각합니다.

이러한 믿음은 현장에서 검증된 경험을 바탕으로 합니다. 어떤 조직도 고도로 정교한 공격으로부터 자유로울 수 없습니다. 실제로 2009년에도 동일한 국가 차원의 공격자들이 Google을 공격했으며, 이러한 공격으로 인해 Google은 광범위한 보안 개선 조치를 취했으며, 이는 CSRB 보고서에서도 인정받았습니다. 보고서에서는 "또한 Google은 인프라 보안에 대한 포괄적인 점검을 실시했습니다."라고 밝히고 있습니다.[4]

이 백서에서는 Google의 보안 전략이 어떻게 발전해 왔는지 그 역사를 살펴보고 Gmail, Google Drive, Slides, Docs, Meet, Chat 등의 앱을 포함한 Google Workspace 사용의 제어 및 보안 관련 이점에 대해 자세히 설명합니다.

참고: 이 백서는 workspace.google.com에서 설명하는 Google Workspace 제품에 적용됩니다. 이 백서에 포함된 내용은 2024년 5월 기준으로 작성되었으며, 작성 당시의 상황을 반영합니다. 향후 출시 예정 기능에 대한 언급은 주석으로 표시되어 있으며, 이는 특정 출시 일정에 대한 약속을 의미하지는 않습니다. Google에서는 고객 보호 조치를 지속적으로 개선하고 있으므로 Google의 보안 정책과 시스템은 앞으로도 계속 변경될 수 있습니다. 이 자료에서 설명된 제품 기능의 사용 가능 여부는 다양한 Google Workspace 버전 제품의 라이선스 제공 여부에 따라 달라질 수 있습니다.

Microsoft에서 발생하는 보안 문제의 패턴

Microsoft의 보안 침해 사고는 어떻게 발생했을까요?

2023년 여름, Storm-0558로 알려진 중국(People's Republic of China) 정부의 후원을 받는 공격자가 Microsoft의 환경을 침해하고 서명 키를 탈취하여 "Storm-0558이 기본적으로 전 세계 모든 Exchange Online 계정에 대한 전체 액세스 권한을 얻을 수 있도록 허용"했습니다.[5] 이러한 사고로 인해 미국 국무부, 상무부, 하원, 주중 미국 대사 등 미국 국가 안보와 관련된 업무를 담당하는 미국 정부 고위 관계자 및 전 세계 22개의 기관과 500명의 개인의 이메일 계정에 대한 무단 액세스가 발생하게 되었습니다.

Storm-0558이 탈취한 서명 키는 "...원격 시스템에 대한 보안 인증에 사용되며, [그리고] 모든 클라우드 서비스 제공업체의 암호화에 있어 핵심 요소입니다."[6] 이 키는 호텔의 모든 방을 여는 마스터키와 같습니다. 일단 획득하면 광범위한 액세스 권한을 얻을 수 있기 때문입니다. Microsoft는 여러 계정 유형에서 동일한 키를 신뢰할 수 있도록 허용했기 때문에, 한 번의 침해로 인해 소비자, 기업, 정부 계정 모두가 동일하게 영향을 받았습니다. CSRB는 "이 보고서 작성일 기준 현재, Microsoft는 Storm-0558이 언제 어떻게 서명 키를 획득했는지에 대해 파악하지 못했습니다."라고 밝혔습니다.[7]

CSRB는 또한 "서명 키 분실 그 자체도 심각한 문제지만, 서명 키의 분실 경위를 파악하지 못한 것은 훨씬 더 심각한 문제라고 할 수 있습니다. 이는 피해 기업이 공격자의 시스템 침투 경로와 관련 취약점의 차단 여부를 확인할 수 없다는 것을 의미하기 때문입니다."라고 언급했습니다.[8] 이는 지금까지 발생한 주요 클라우드 서비스 제공업체의 정보 유출 사건 가운데서도 가장 심각한 사고 중 하나입니다. CSRB는 이 사건을 "매우 성공적인 첩보활동(espionage equivalent of gold)"이라고 표현했습니다.[9]

불과 몇 달 후인 2023년 11월, 러시아에서 국가 차원의 후원을 받는 또 다른 해킹 그룹인 Midnight Blizzard는 비밀번호 스프레이 공격을 통해 Microsoft 고위 경영진, 보안, 법무팀을 비롯한 여러 팀의 기업 이메일 계정을 침해했습니다.[10] 이 그룹은 미국 정부 관료와의 이메일 서신에 액세스했습니다. 2024년 3월 Microsoft는 2023년 11월에 시작된 Midnight Blizzad의 공격이 5개월이 지난 해당 시점에서도 진행 중이라고 밝히며 "최근 몇 주간 Midnight Blizzard가 Microsoft 이메일 시스템에서 유출된 정보를 사용하여 무단 액세스 권한을 얻거나 얻으려고 시도하고 있다는 증거를 발견했으며, 여기에는 회사의 소스 코드 저장소 및 내부 시스템 일부에 대한 액세스 권한도 포함됩니다."라고 전했으나, 문제 해결 타임라인에 대해서는 언급하지 않았습니다.[11]

단순한 사고에 불과할까요?

이러한 공격의 심각성을 과소평가해서는 안 됩니다. 정부의 통신 및 시스템에 접근할 수 있는 외국의 공격자들은 지정학적 분쟁이 발생할 경우 스파이 활동을 하거나 주요 인프라를 공격할 수 있으며, 이는 정부와 민간인에게 심각한 영향을 미칠 수 있습니다.

보안 및 위험 관리에 우선순위를 두지 않음

Storm-0558 침해 사고에 대해 CSRB는 "이 침입은 예방할 수 있었으며 결코 일어나서는 안 되는 일이었다"[12]라고 결론내리며, "특히 기술 생태계에서 Microsoft가 차지하는 비중과 고객이 데이터 및 운영 보호를 위해 이 회사에 기대하는 신뢰 수준을 고려할 때, Microsoft의 보안 문화는 미흡했으며 재정비가 필요합니다."[13]라고 덧붙였습니다.

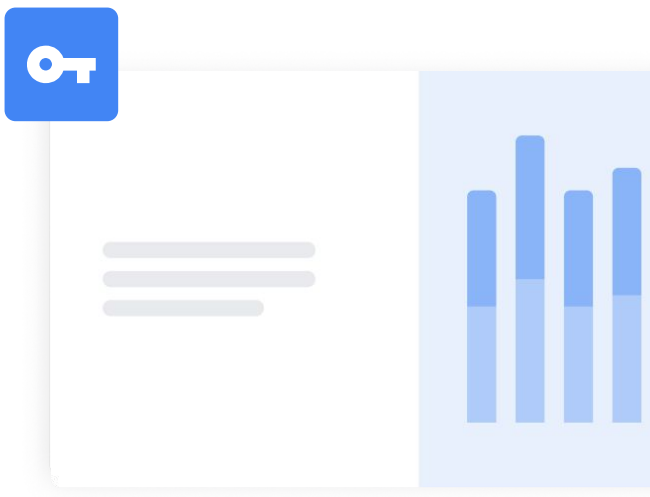
부정확한 공개 성명을 수정하지 않음

CSRB는 또한 "이 사고에 대한 부정확한 공개 성명을 적시에 수정하지 않고"[14] "위원회가 검토를 마치고 Microsoft의 수정된 성명 발표 계획에 대해 거듭 질문한 후에야 수정하기로 결정"[15]하는 등 Microsoft의 보안 사고 처리 방식에 대해 심각한 우려를 표했습니다. 또한 이 때문에 "Microsoft의 고객들은 이번 침입 사고가 일어난 후 Microsoft 클라우드 환경의 보안에 대한 자체 위험 평가를 수행하는 데 필요한 필수 정보를 얻을 수 없었습니다."라고 전했습니다.[16]

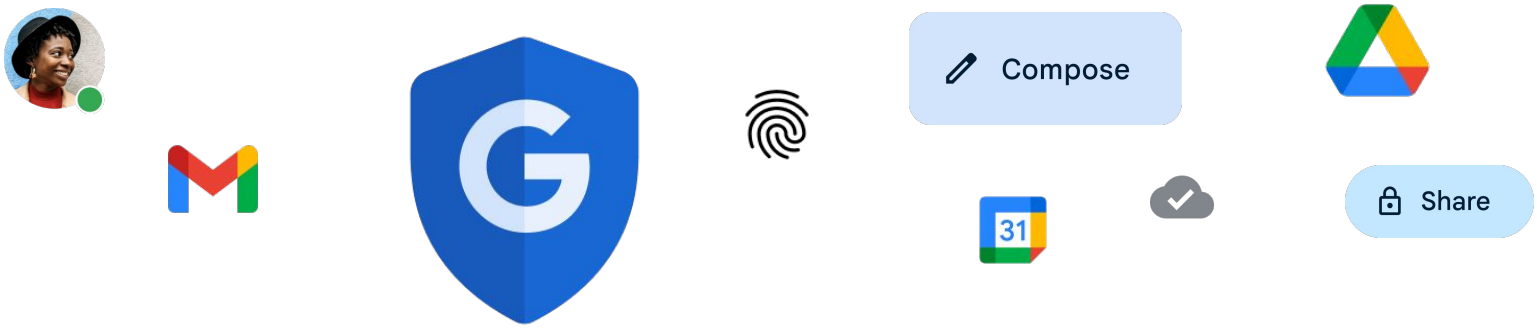
키 분실 경위를 확인하지 못함

근본적인 사고 원인이 확인되지 않았기 때문에, Microsoft가 이러한 유형의 사고의 재발을 방지할 수 있을지 여부는 사실상 불확실합니다. CSRB는 "위원회가 검토를 마무리하는 시점에서 Microsoft가 3월 12일에 사고 관련 정보를 업데이트했으나, 여기에서도 Microsoft가 2016 MSA 키가 포함된 크래시 덤프 또는 해당 키의 부적절한 이동에 대한 어떤 증거도 식별하지 못한 것으로 드러났습니다."라고 밝혔으며,[17] 또한 "위원회는 Microsoft가 Storm-0558이 2016 MSA 키를 어떻게 획득했는지 모른다고 평가합니다."라고 언급했습니다.

고도로 정교한 공격자의 표적이 되는 일을 피할 수 있는 조직은 없겠지만, 이러한 분명한 증거 패턴은 Microsoft가 시스템과 고객의 데이터를 안전하게 보호할 수 없음을 시사합니다.



Google Workspace에서 제공하는 더 차별화되고 **안전한 방식**



근본적으로 다른,
더 안전한 접근 방식

Google Workspace는 업계 권장사항을 기반으로 엄격한 개인 정보 보호 및 보안 표준을 지원하도록 설계되었습니다.

- 클라우드 중심, 브라우저 기반 방식을 사용하여 지속적으로 업데이트되어 로컬 기기, 네이티브 앱 또는 이메일 첨부파일이 필요하지 않습니다.
- 제로 트러스트 접근 방식에 기반하여 제어, 암호화, 인증 기능이 기본 제공되어 직원이 어디에서나 작업할 수 있고 VPN이 필요하지 않습니다.
- 조직의 정보를 피싱, 멀웨어, 랜섬웨어, 공급망 공격으로부터 보호하기 위해 글로벌 규모로 작동하며, 부가기능이 필요하지 않습니다. Gmail은 스팸, 피싱 시도, 멀웨어가 받은편지함에 도달하는 것을 99.9% 이상 차단합니다. 또한 Gmail은 서드 파티 표준 바이러스 백신 제품보다 평균적으로 2배 더 많은 멀웨어를 탐지합니다.
- 패치나 강력한 계정 탈취 보호가 필요 없는 보안 엔드포인트(회사 제공 또는 BYOD(Bring Your Own Device))로 모두가 더욱 안전해집니다. — 보안 내재화 설계로, 기본적으로 기본적으로 안전합니다.

보안에 대한 Google의 차별화된 접근 방식을 보여주는 사례로, CSRB는 Google이 이러한 유형의 공격에 대해 탄력적으로 대응할 수 있는 시스템과 제품을 만들기 위해 오랜 시간 동안 기울여온 상당한 노력을 인정하며 다음과 같이 언급했습니다. 'Google은 모든 사용자 인증 정보를 발급할 때 고유 식별자를 할당하고 데이터베이스에 기록하여 Google이 받은 사용자 인증 정보가 Google이 발급한 사용자 인증 정보임을 되돌릴 수 없는 증거로 사용하는 스테이트풀(Stateful) 토큰에 최대한 의존하도록 ID 시스템을 재작업했습니다. 또한 Google은 가능한 경우 완전 자동 키 순환을 구현하고 스테이트리스(Stateless) 토큰의 유효성 검사 기간을 강화하였고, 이로 인해 위협 행위자가 활성 키를 찾고 획득하는데 쓸 수 있는 시간을 줄였습니다. 또한 Google은 이러한 ID 시스템을 보호하기 위해 제로 트러스트 네트워크와 하드웨어 지원, Fast Identity Online(FIDO) 호환 2단계 인증(2FA)을 구현하는 등 인프라 보안에 대한 포괄적인 점검을 실시했습니다.'[19]

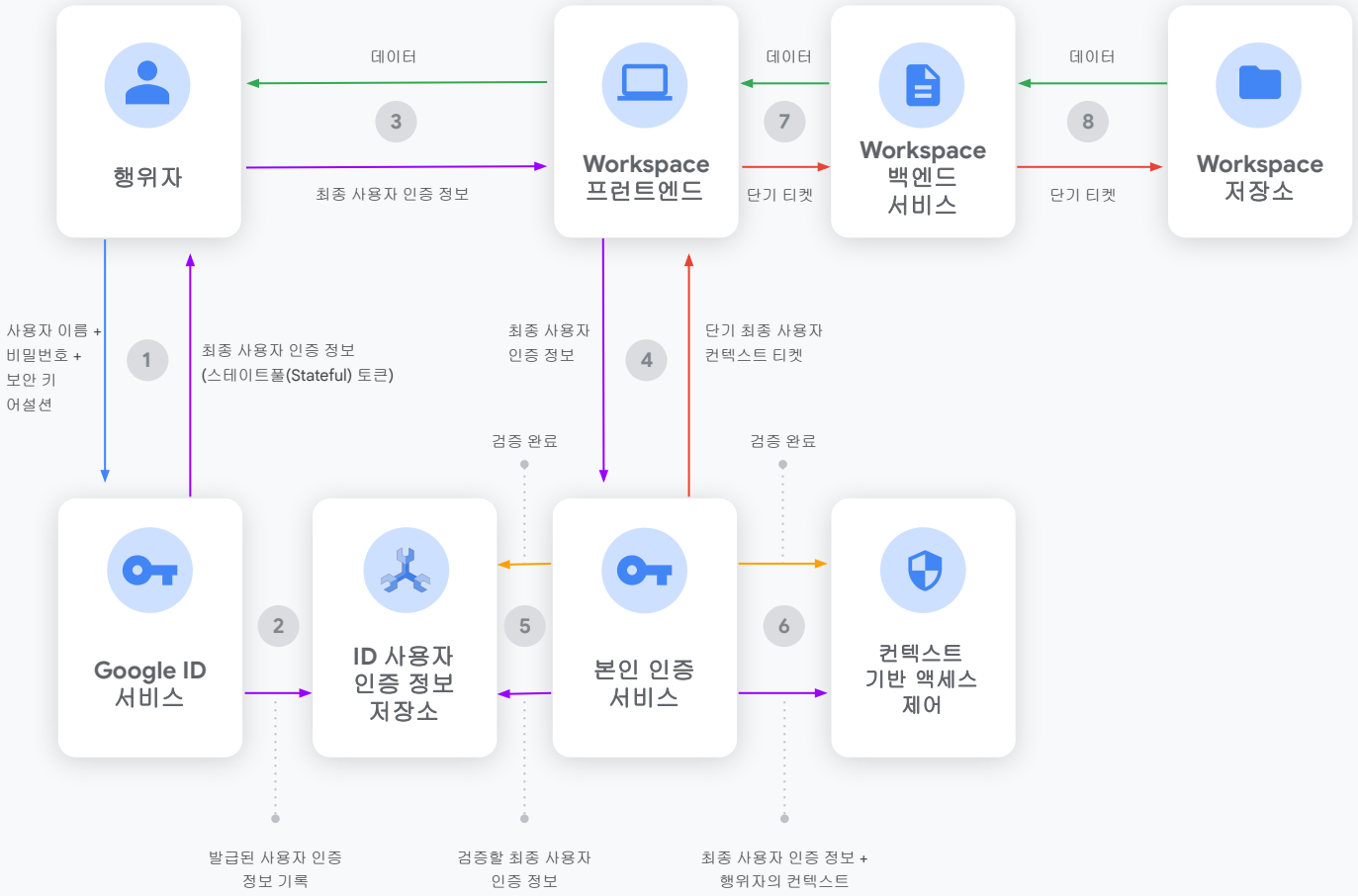
CSRB에서 언급했듯이 Google은 스테이트풀(Stateful) 토큰을 가능한 많이 활용합니다. 이 개념을 조금 더 자세히 살펴보겠습니다.

- Google ID 서비스는 사용자 로그인을 확인한 다음 쿠키나 OAuth 토큰과 같은 사용자 인증 정보를 사용자 기기에 발급합니다. 이 인증 정보는 Google ID 사용자 인증 정보 저장소에 기록되며 스테이트풀(Stateful)로 간주됩니다. 이후 기기에서 Google 인프라로 전송되는 모든 요청에는 해당 사용자 인증 정보가 요구됩니다.

- 서비스에서 사용자 인증 정보를 받으면, 서비스는 발급된 유효한 인증 정보 목록과 비교하여 확인할 수 있도록 해당 인증 정보를 ID 서비스에 전달합니다. 사용자 인증 정보가 확인되면, ID 서비스에서 사용자의 요청과 관련된 원격 프로시저 호출(RPC)에 사용할 수 있는 단기 사용자 컨텍스트 티켓을 반환합니다. 이 시점부터 모든 연속 호출에서 호출 서비스는 RPC의 일부로 피호출자에 사용자 컨텍스트 티켓을 보낼 수 있습니다. 해당 티켓은 Google 프로덕션 환경에서 내부적으로만 사용할 수 있습니다.

Google의 보안이 내재화된 스테이트풀(Stateful) ID 토큰은 사용자 인증 정보 위조를 방지하여 사용자 계정을 보호합니다. 암호화 키가 침해되더라도 외부 공격자가 이를 직접 사용하여 사용자 데이터에 액세스할 수 없습니다. 해당 토큰은 대신 Google에서 발행한 토큰인지를 확인하는 별도의 프로세스를 통해 검증을 받은 후에 사용자 정보에 대한 액세스 권한을 부여받습니다.

스테이트풀 (Stateful) 토큰의 개념적 아키텍처의 흐름



스테이트풀(Stateful) 토큰의 도입이 Google이 고객의 데이터를 안전하게 보호하는 유일한 방법인 것은 아닙니다. Google의 Google 인프라 보안 설계 백서에서는 물리적 보안 및 직원 제어를 비롯하여 하드웨어부터 클라이언트까지 스택의 각 계층에서의 보안 관련 고려사항이 자세히 설명되어 있습니다. 여기에는 제로 트러스트 원칙을 인프라에 구현하는 Google의 접근 방식인 BeyondProd가 포함됩니다. BeyondProd에서는 IP 주소나 호스트 이름과 같은 프로덕션 네트워크의 위치가 아니라 코드 출처, 신뢰할 수 있는 하드웨어, 서비스 ID와 같은 특성에 따라 신뢰가 결정됩니다. BeyondProd를 사용하면 서비스 간 상호 신뢰가 내재되지 않고, 네트워크 에지 보호 조치가 네트워크 공격으로부터 워크로드를 격리하며, 서비스 전반에 걸쳐 일관된 정책이 적용됩니다. 이 인프라 모델의 발전에 대한 자세한 내용은 Google의 BeyondProd 백서에서 확인할 수 있습니다.

강력한, 보안 중심의 문화

2009년, Google은 중국의 지원을 받은 일련의 사이버 공격(2023년 여름 Microsoft의 보안을 침해한 Storm-0558 그룹과 동일한 그룹으로 추정)인 오로라 작전의 표적 중 하나였습니다. CSRB의 보고서는 "업계에서는 Storm-0558이 2009년 Google을 포함한 20여 개 기업을 표적으로 했던 오로라 작전과 관련이 있다고 판단하고 있습니다."라고 전합니다.[20]

최근 Microsoft와 그 고객들에게 영향을 미치고 있는 사건과 10여년 전 Google에 영향을 주었던 침해 사건의 차이는, Google은 수십억 명의 사람들을 안전하게 지켜야 한다는 책임감을 바탕으로 사이버 보안에 대한 생각을 근본적으로 바꾸었다는 점입니다.

> "오로라 작전은 2010년 미국 민간 기업을 표적으로 한 중국으로부터의 일련의 사이버 공격이었습니다. 위협 행위자들은 Yahoo, Adobe, Dow Chemical, Morgan Stanley, Google 및 기타 20여 개 기업의 네트워크를 침해하여 영업 비밀을 탈취하는 피싱 캠페인을 벌였습니다. Google은 피해를 인정하고 특정 중국 인권 운동가들의 Gmail 계정이 침해되었음을 대중에게 공개한 유일한 기업이었습니다. 또한 Google은 이 사건의 주모자가 중국임을 공개적으로 밝혔는데, 이는 기업들이 중국 시장에 대한 접근이 위태로워질까 봐 주저하는 일이었습니다. 이 보안 사고는 산업 스파이 활동의 도구인 사이버 작전을 대중에게 알렸다는 점에서 근래 사이버 작전 역사의 이정표로 여겨지고 있습니다. 이로 인해 Google은 중국에서의 운영을 중단했지만, 홍콩에서는 현지화된 버전의 검색 엔진을 계속 운영하고 있습니다. Gmail 침해 사고 이후부터, Google은 계정이 침해되었거나 국가가 후원하는 공격자의 표적이 된 것으로 의심되는 경우 사용자에게 이를 알리기 시작했습니다. 이러한 관행은 이후 다른 이메일 제공업체로 확산되었습니다." [21]
>
> **오로라 작전 - 미국 외교협회 (Council on Foreign Relations)**

Google은 자사 블로그 게시물 사이버 공격의 어두운 세계에서의 투명성(Transparency in the shadowy world of cyber attack)에서 "오로라 작전은 우리에게 투명성을 수용해야 할 필요성을 알려줬을 뿐만 아니라, 두 번째이자 더 중요한 교훈인 보안 아키텍처와 관련하여 효과가 있는 것과 그렇지 않은 것이 무엇인지에 대해 가르쳐 주었습니다."[22]라고 공유한 바 있습니다.

CSRB 권고안보다도 앞서 나간 Google의 접근 방식은 고객, 조직, 정부가 신속하게 대응하여 위협 행위자가 악용할 기회를 줄일 수 있도록 지원합니다. 이러한 문화는 Google이 고객과 소통하고, 엔지니어링 결정의 우선순위를 정하며, 제품 투자를 결정하는 방식에 영향을 미칩니다.

특히 주목할만한 점은 제로 트러스트 및 심층 방어 개념을 선도적으로 도입하고 모든 직원이 VPN을 사용하지 않고도 신뢰할 수 없는 네트워크에서 작업할 수 있도록 하는 BeyondCorp라는 내부 이니셔티브를 출범한 것입니다. 오늘날 전 세계의 조직은 이와 동일한 접근 방식을 취하여, 액세스 제어를 네트워크 경계로부터 개인과 데이터로 전환하고 있습니다.

고객을 위한 심층 제로 트러스트 제어 기능 내장

BeyondCorp의 개념을 한 단계 더 발전시킨 Google Workspace를 통해 고객은 Google에서 구현한 심층적인 제어 기능 외에 추가적인 데이터 보호 계층을 구성할 수 있습니다. 이러한 보호 기능은 CISA의 제로 트러스트 성숙도 모델과 긴밀히 연계되도록 설계되었으며, 다음의 기능도 제공합니다.

패스키 및 보안 키:

사용자 인증 정보 침해를 방지하는 패스키는 웹사이트와 앱에서 편리하고 안전한 인증 환경을 제공할 수 있는 비밀번호 없는 로그인 방법으로, 사용자는 휴대전화, 노트북 또는 데스크톱에서 지문, 얼굴 인식 또는 기타 화면 잠금 메커니즘으로 로그인할 수 있습니다. 보안 키는 하드웨어 기반의 피싱 방지 2단계 인증(2FA)을 제공하여 중요한 사용자를 보호하도록 지원합니다.

컨텍스트 인식 액세스(CAA) 및 BeyondCorp Enterprise (Chrome Enterprise):

사용자 ID, 위치, 기기 보안 상태, IP 주소 등의 속성을 기반으로 앱에 대한 상세 액세스 제어 보안 정책을 제공합니다. CAA를 사용하면 기기의 조직 내 IT 정책 준수 여부와 같은 컨텍스트를 기반으로 사용자 액세스를 제어할 수 있습니다.

강력한 데이터 컨트롤:

고객은 DLP 및 데이터 분류와 같은 도구를 활용하여 조직의 기밀 정보를 고유하게 식별할 수 있습니다. 데이터의 위험 프로필이 설정되면 고객은 자사 직원에게 요구하고자 하는 적절한 제어(공유, 다운로드 방지)를 적용할 수 있습니다.

Google은 기본 구성 가이드를 제공하는 보안 클라우드 비즈니스 애플리케이션(SCuBA) 프로젝트에서 CISA와 긴밀히 협력하고 있습니다. Google Workspace 제로 트러스트 제어 기능에 대한 자세한 내용은 미국 공공 부문 기관을 위한 제로 트러스트 권장사항 가이드와 Google Workspace 보안 및 신뢰 웹페이지에서 확인하실 수 있습니다.

기술 못지않게 중요한 **연구** 및 **투자에 대한 사고방식**

보안은 Google의 운영 구조에 깊숙이 뿌리내리고 있습니다. Google의 전담 보안 팀에는 정보 및 애플리케이션 보안, 암호화, 네트워크 보안, 위협 모델링 분야에서 세계에서 가장 많은 연구 성과를 내는 연구원들이 소속되어 있습니다. Google은 주요 표준을 준수하며 규제 기관 및 과학계와 협력함으로써 업무 방식의 모든 측면을 관리하는 내부 프로세스를 개발합니다.

Google은 전사적인 접근 방식을 통해 시스템을 방어하고 고객의 데이터를 안전하게 보호하고 있습니다. 예를 들어, Google은 Chrome Enterprise 제어 기능을 활용하고 모든 직원이 시스템 액세스에 보안 키를 사용하도록 요구합니다. Google은 사이버 보안 강화, 제로 트러스트 프로그램 확대, 소프트웨어 공급망 보호, 오픈소스 보안 강화를 위해 향후 5년간 미화 100억 달러를 투자하기로 약속하는 등 보안 기능 향상에 상당한 금액을 지원하고 있습니다.

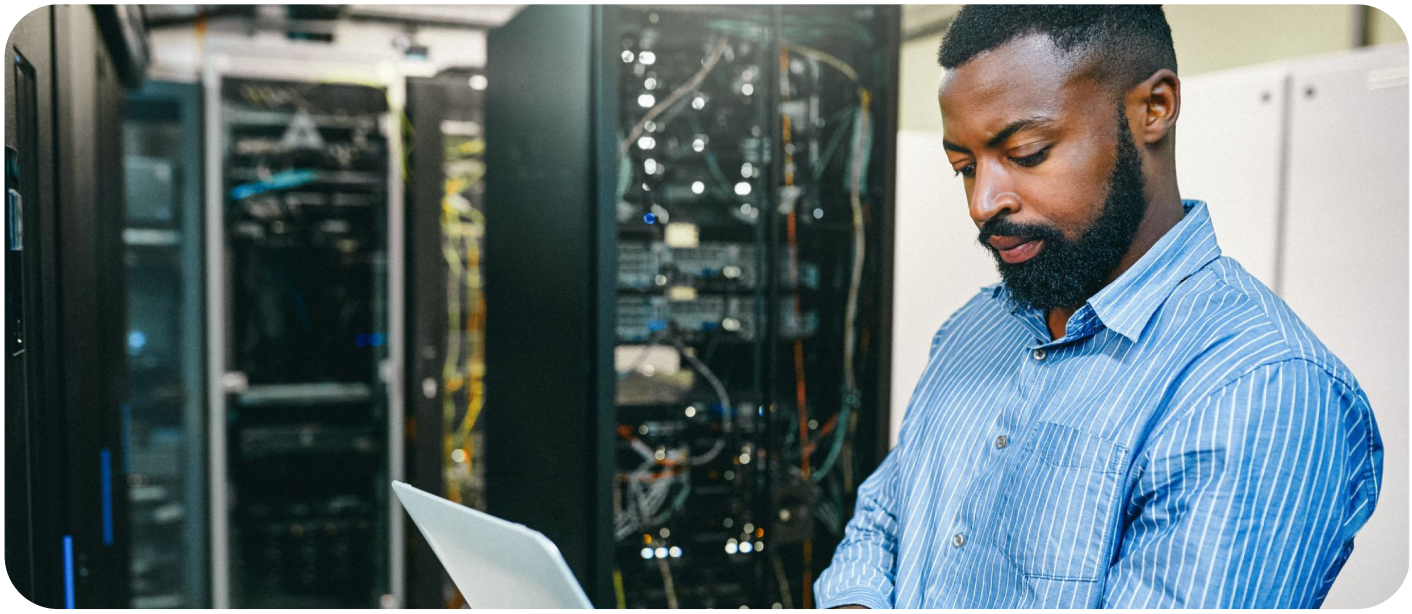
Google의 연구:

Google 연구팀은 보안, 개인 정보 보호, 악용 방지에 관한 다양한 프로젝트를 지원하고 있습니다. 연구팀의 활동에는 안전하고 신뢰할 수 있는 시스템 구축,[23] 보안 내재화 설계,[24] 소프트웨어 안전을 위한 생태계 개발[25]과 같은 간행물이 포함됩니다. Google의 보안 연구원들은 하드웨어 및 소프트웨어 시스템의 제로데이 취약점을 연구하는 프로그램인 Project Zero도 운영하고 있습니다. Google Cloud의 CIOS실, Google의 위협 분석 그룹(TAG), Mandiant, 다양한 Google Cloud 제품팀을 포함한 Google의 인텔리전스 및 보안팀은 정기적으로 Google Threat Horizons 보고서에 인사이트를 제공합니다.

커뮤니티 참여:

Google 보안 엔지니어링팀은 커뮤니티의 공동 이익을 위해 연구 결과를 공개하는 것 외에도, Google 시스템의 취약점 테스트에 외부 커뮤니티를 참여시키는 Bug Hunter 프로그램을 운영합니다. 이 프로그램에는 커뮤니티의 참여를 장려하기 위한 금전적인 보상이 포함되어 있습니다. Bug Hunter 프로그램 Tsunami는 범용 오픈소스 네트워크 보안 스캐너입니다. 높은 신뢰도로 심각도가 높은 취약점을 탐지할수 있는 확장 가능한 플러그인 시스템을 갖추고 있으며, Google의 다양한 오픈소스 보안 프로젝트 중 하나입니다.

앞서 언급했듯이, 어떤 조직이든 고도로 정교하고 집요한 공격자의 표적이 될 수 있습니다. 오로라 작전 후 14년이 넘는 기간 동안 Google은 이러한 침해 사고로부터 내부 시스템과 고객을 보호하기 위해 플랫폼의 기본 아키텍처, 심층 방어 접근 방식, 핵심 보안 원칙을 중심으로 한 문화를 전면적으로 점검해 왔습니다.



미래를 향한 혁신

앞서 언급한 바와 같이 CSRB의 권고안 중 일부는 이미 Google의 보안 접근 방식에서 핵심적인 부분을 차지하고 있습니다. 또한 Google은 업계 전반에서 직면하고 있는 문제를 선제적으로 해결하고 끊임없이 진화하는 보안 문제에 대한 업계 최초의 솔루션을 제공하기 위해 노력하고 있습니다. 다음은 이에 대한 몇 가지 예시입니다.

Device Bound Session Credentials(DBSC):

쿠키 도용이 미치는 영향을 크게 줄이기 위해 Google은 웹 세션을 기기 하드웨어에 암호화 방식으로 바인딩하는 새로운 개방형 표준을 발표했습니다. DBSC는 인증 세션을 기기에 바인딩하기 때문에 쿠키를 유출해도 쓸모가 없게 되므로 공격자들을 혼란에 빠트릴 수 있습니다.

AI의 혁신:

현재 Gmail의 고급 AI 보호 기능은 스팸, 피싱 시도, 멀웨어가 받은편지함에 도달하는 것을 이미 99.9% 이상 차단하고 있습니다. 대규모 언어 모델을 사용하여 Gmail에서 스팸을 20% 더 줄였으며, 매일 사용자가 신고하는 스팸을 1,000배나 더 많이 평가할 수 있게 되었습니다. 최근에는 AI 분류를 통해 문서를 분류하는 대규모 언어 모델의 강력한 기능을 도입하였습니다. 이를 통해 고객은 맞춤형 개인 정보 보호 모델을 사용하여 민감한 정보를 식별하고 보호할 수 있습니다. Google은 앞으로도 고객을 더 안전하게 보호할 수 있는 최첨단 기술을 통해 제품에 새로운 AI 방어 계층을 도입할 계획입니다.

Google Workspace가 지원하는 방법

Google은 고객의 안전을 지키고 더 안전한 업무 방식을 위한 대안을 제공하는 데 계속 집중하고 있습니다. 귀사에 보다 안전한 업무 방식을 제공하는 방법을 알아보고 싶으시다면 고객 담당자와 상담하거나 여기에서 시작해 보세요.

부록: 각주

각주 번호	출처
1	CSRB, 2023년 여름 Microsoft Exchange Online 침입에 대한 검토(Review of the Summer 2023 Microsoft Exchange Online Intrusion), ii, (CSRB, 2024).
2	Ibid., iv
3	CISA, ED 24-02: Microsoft 기업 전자 메일 시스템에 대한 국가 지원 공격이 초래한 중대한 위험 완화(Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System), (CISA, 2024).
4	CSRB, 2023년 여름 Microsoft Exchange Online 침입에 대한 검토(Review of the Summer 2023 Microsoft Exchange Online Intrusion), 20페이지, (CSRB, 2024)
5	Ibid., iii
6	Ibid., iii
7	Ibid., iii
8	Ibid., 18
9	Ibid., ii
10	CISA, ED 24-02
11	Microsoft 보안 대응 센터(Microsoft Security Response Center), 국가의 후원을 받는 행위자 Midnight Blizzard의 공격에 따른 Microsoft 조치에 대한 업데이트(Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard), (Microsoft, 2024년).
12	CSRB, 2023년 여름 Microsoft Exchange Online 침입에 대한 검토(Review of the Summer 2023 Microsoft Exchange Online Intrusion), iii페이지, (CSRB, 2024년)
13	Ibid., iii
14	Ibid., iii
15	Ibid., iii
17	Ibid., 16
18	Ibid., 5
19	Ibid., 20
20	Ibid., iii
21	미국 외교협회, 오로라 작전, (미국 외교협회, 2010년)
22	켄트 워커, 사이버 공격이라는 어두운 세계에서의 투명성 확보(Transparency in the shadowy world of cyberattacks),(Google, 2022년)
23	헤더 앳킨스, 벳시 베이어, 폴 블랭킨십, 애나 오프레아, 피오트르 레반도프스키, 애덤 스터블필드, SRE를 위한 시스템 설계와 구축(Building Secure and Reliable Systems) (O'Reilly Media, 2020년)
24	크리스토프 컨, Google의 보안 내재화 설계(Secure by Design at Google)(Google, 2024년)
25	크리스토프 컨, 소프트웨어 안전을 위한 개발자 생태계(Developer Ecosystems for Software Safety)(Google, 2024년 2월)