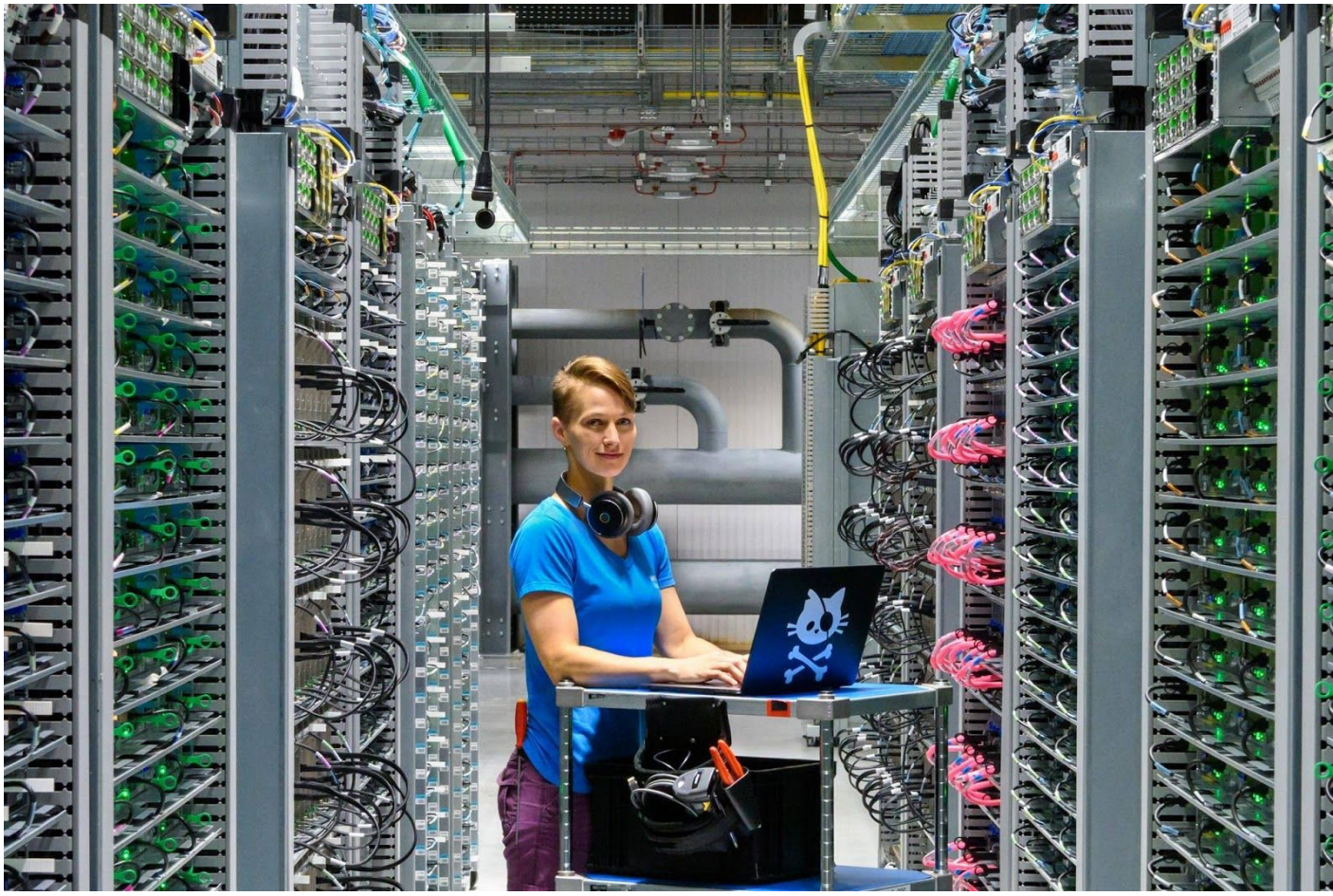
Google Workspace

Google Workspace 보안 백서



Google Cloud

목차

들어가며

클라우드 컴퓨팅은 오늘날 기업의 비즈니스 방식에 변화를 불러왔습니다. 조직에서는 주로 인프라, 업무 운영, 서비스 제공 관리 용도로 퍼블릭 클라우드를 고려하면서 제공업체가 안전하고 규정을 준수하는 인프라를 제공하기 위해 인력과 프로세스에 더 많이 투자할 수 있다는 사실을 깨닫고 있습니다.

Google은 클라우드 분야의 선도업체로서 클라우드 모델이 보안에 끼치는 영향을 충분히 이해하고 있습니다. 이에 따라 기존의 수많은 온프레미스 솔루션보다 더 강력한 보안을 제공하도록 클라우드 서비스를 설계했습니다. Google은 자체적인 업무 운영을 보호하기 위해 보안을 최우선으로 여기고 있으며 고객도 이와 동일한 Google 인프라에서 실행하므로 조직은 이러한 보호 조치의 직접적인 수혜자가 됩니다.

Google의 조직 구조, 교육 우선순위, 채용 절차에도 보안과 데이터 보호가 토대가 됩니다. 이러한 원칙은 Google 데이터 센터 운영과 기술을 결정하는 요소이자 일상적인 업무 운영과 더불어 위협 해결 방법을 비롯한 재해 방지 계획의 중심축을 이룹니다. 보안과 데이터 보호는 Google이 고객 데이터를 처리하는 방식에서 최우선으로 생각하는 요소이며 Google의 계정 관리, 규정 준수, Google에서 고객에게 제공하는 인증의 초석이라 할 수 있습니다. Google에서는 고객사와 데이터에 기울이는 노력을 Google Cloud 신뢰 원칙으로 정리하여 고객이 Google Workspace와 Google Cloud Platform을 사용하는 모든 경우에 Google에서 고객의 개인 정보를 보호하는 방식을 명시해 두었습니다.

이 백서에서는 Google의 클라우드 기반 생산성 제품군인 Google Workspace의 보안 및 규정 준수에 대한 Google의 방침을 개괄적으로 설명합니다. 수십만 명이 근무하는 대형 은행과 소매업체부터 고속 성장하는 스타트업에 이르기까지 전 세계 500만 곳이 넘는 조직에서 사용하는 Google Workspace 및 G Suite for Education에 포함된 공동작업 및 생산성 도구를 확인하려면 여기를 참조하세요. Google Workspace와 G Suite for Education은 팀원이 어디에서 어떤 기기를 사용하든 새롭고 보다 효율적인 방식으로 안전하게 협업할 수 있도록 설계되었습니다. 예를 들어 Gmail은 매주 3,000억 개가 넘는 첨부파일에서 멀웨어를 검사하며 99.9% 이상의 스팸, 피싱, 멀웨어를 사용자에게 도달하기 전에 방지합니다.[3] Google은 모든 종류의 보안 위협으로부터 보호하고자 최선을 다해 사용자와 관리자를 위한 새로운 보안 도구를 혁신하고 고객에게 안전한 클라우드 서비스를 제공하고 있습니다.

참고: Google은 앞으로 수개월 내에 교육 및 비영리단체 고객에게 Google Workspace를 제공할 예정입니다. 교육 분야 고객은 앞으로도 클래스룸, 과제 도구, Gmail, Calendar, Drive, Docs, Sheets, Slides, Meet가 포함된 G Suite for Education을 사용해 도구를 이용할 수 있습니다. 비영리단체용 G Suite는 Google 비영리단체 프로그램을 통해 자격을 갖춘 조직에 계속 제공될 예정입니다. 달리 명시되지 않은 한 이 문서의 내용은 Google Workspace 및 G Suite for Education에 적용됩니다.

[3] 2020년 4월 기준

면책조항

여기에 나와 있는 콘텐츠는 2020년 10월 기준으로 작성되었으며 이 문서가 작성된 당시의 상황을 나타냅니다. Google에서 고객 보호를 지속적으로 개선하고 있으므로 Google Cloud의 보안 정책과 시스템은 앞으로도 계속 변경될 수 있습니다.

Google의 보안 및 개인 정보 보호 중심 문화

Google에서는 모든 직원을 위해 활발하고 포괄적인 보안 및 개인 정보 보호 문화를 육성했습니다. 이 문화의 영향은 채용 과정, 직원 온보딩, 온보딩 과정에서 실시되는 교육, 보안 인식 제고를 위한 전사적 차원의 사내 행사 등에서 눈에 띄게 드러납니다.

직원의 배경 확인

Google에서는 직원을 채용하기 전에 입사 지원자의 학력과 과거 근무 이력을 확인하고 내외부 평판 조회도 거칩니다. 현지 노동법 또는 법 규정에서 허용하는 경우에는 신원, 범죄 이력, 신용도 검사도 수행하며 직책에 따라서는 비자 상태를 확인하기도 합니다.

전 직원 대상 보안 교육

모든 Google 직원은 오리엔테이션 과정에서는 물론 Google에서 근무하는 내내 지속적으로 보안 교육을 받습니다. 신입 직원은 오리엔테이션 중에 Google의 윤리 강령에 동의하는데, 이 윤리 강령에는 고객 정보를 안전하게 보호하고 보안을 유지하려는 Google의 의지가 강조되어 있습니다.

직무 역할에 따라 보안의 특정 요소에 관한 교육에 추가로 참가하게 됩니다. 예를 들어 정보 보안팀은 신입 엔지니어를 대상으로 안전한 코딩 방법, 제품 설계, 자동 취약점 테스트 도구와 같은 주제의 교육을 실시합니다. 또한 엔지니어는 보안 관련 주제에 관한 기술 프레젠테이션에 참석하고 새로운 위협, 공격 패턴, 완화 기술 등을 다루는 보안 뉴스레터를 전달받습니다.

안전한 환경

Google의 제로 트러스트 접근 방식은 기기, 기기 상태, 관련 사용자, 문맥에 관한 정보를 기반으로 중요한 액세스 제어를 적용합니다. 이 접근 방식에서는 본질적으로 내외부 네트워크를 모두 신뢰할 수 없다고 간주하므로 애플리케이션 계층에서 액세스 수준을 동적으로 어설션하고 적용하는 보더리스 규정 준수 개념을 생성합니다. 따라서 Google의 보안 및 규정 준수팀은 긴급 상황에도 평소처럼 안전과 효력을 유지할 수 있습니다.

코로나19는 작업 방식뿐 아니라 근무하는 환경까지 바꾸었기 때문에 어떤 환경에서든 업계 규정 준수 요건을 충족하는 새로운 솔루션이 필요하게 되었습니다. 제로 트러스트를 활용하면 내부 직원은 물론 외부 인력에게도 VPN 또는 위치 요구사항과 무관하게 안전하고 확장 가능한 솔루션을 제공할 수 있습니다.

내부 보안 및 개인 정보 보호 이벤트

보안 및 개인 정보 보호는 끊임없이 진화하는 영역이므로 Google에서는 전담 직원의 개입이 인식 제고의 핵심적인 수단임을 잘 알고 있습니다. 따라서 전 직원을 대상으로 정기적으로 사내 컨퍼런스를 주최해 보안과 데이터 개인 정보 보호에 대한 인식과 혁신 속도를 높이고 보안 및 개인 정보 보호 주제를 주로 조명하는 '기술 강연(Tech Talks)'을 주기적으로 진행하고 있습니다. 대표적인 예인 '프라이버시 위크(Privacy Week)' 기간에는 전 세계 사무소를 대상으로 소프트웨어 개발 및 데이터 처리부터 정책 시행에 이르기까지 모든 측면에서 개인 정보 보호에 대한 인식을 높이는 다양한 이벤트를 주최합니다.

전담 보안팀

Google은 소프트웨어 엔지니어링과 운영 사업 부문에 정규직 보안 및 개인 정보 보호 전문가로 구성된 전담팀을 가동하고 있습니다. 이 팀에는 정보, 애플리케이션, 네트워크 보안 분야에서 세계 최고로 손꼽히는 전문가들이 포진해 있습니다. 팀에서는 Google의 방어 시스템 유지보수, 보안 검토 프로세스 개발, 보안 인프라 구축, 기업의 보안 정책 구현과 같은 업무를 맡아 상용 및 커스텀 도구, 침투 테스트, 품질 보증(QA) 수단, 소프트웨어 보안 검토를 통해 보안 위협의 존재 여부를 상시 검사합니다.

Google 내부의 정보 보안팀 팀원은 다양한 핵심 서비스를 제공합니다. 모든 네트워크, 시스템, 서비스에 대한 보안 계획 검토, Google 제품 및 엔지니어링팀에 대한 프로젝트별 컨설팅 서비스 제공, Google 네트워크상의 의심스러운 활동 모니터링, 정보 보안 위협 대응, 정기적인 보안 평가 및 감사 수행, 외부 전문가를 동원한 정기 보안 평가 등이 모두 보안팀의 역할입니다. 특히 Google에서 조직한 프로젝트 제로(Project Zero)라는 전담 팀은 소프트웨어 공급업체에 버그를 알리고 외부 데이터베이스에 버그를 기록하여 표적 공격을 예방하는 것을 목표로 하고 있습니다.

보안팀은 이러한 역할에 그치지 않고 연구 및 외부 활동에도 참여하여 Google 솔루션을 선택하는 사용자뿐 아니라 폭넓은 범위의 인터넷 사용자 커뮤니티까지 보호하고 있습니다. 아울러 보안 연구 자료를 발표하여 대중에 공개하고 오픈소스 프로젝트와 학술회의를 조직하거나 참가하는 활동도 펼치고 있습니다.

Google의 개인정보보호팀

Google의 개인정보보호팀은 Google 제품 출시 과정에서 핵심적인 역할을 합니다. 자동 모니터링 도구 모음을 빌드하여 개인 정보 처리 서비스가 설계 시 의도한 대로 Google의 데이터 보호 노력에 부합하게 운영되고 있는지 확인하며 개인 정보 보호 요구사항의 준수 사실을 확인하기 위해 설계 문서와 코드 감사도 검토합니다.

여러 부서의 팀이 엄격한 개인 정보 보호 기준을 반영한 제품이 출시되도록 돕고 있습니다. 가령 사용자 데이터를 투명하게 수집하고 사용자 및 관리자에게 의미 있는 개인 정보 보호 구성 옵션을 제공하는 한편 Google 플랫폼에 저장된 정보에 대한 적절한 관리를 유지할 수 있는지 점검합니다. 제품 출시 후에는 적절한 데이터 사용 여부를 확인하기 위해 Google의 규정 준수 및 개인 정보 보호 프로그램을 통해 데이터 트래픽을 감사하는 자동 프로세스를 감독합니다. 아울러 Google은 신기술의 개인 정보 보호 권장사항에 관한 연구를 통해 선도적 사고를 제시하고 있습니다.

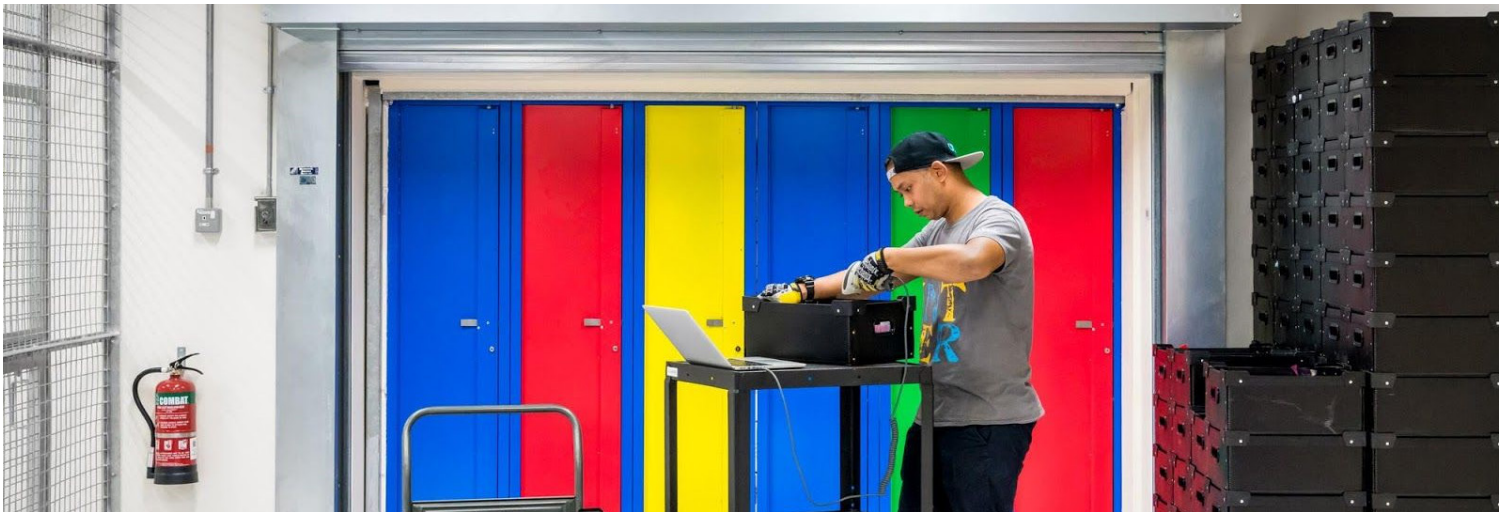
내부 감사 및 규정 준수 전문가

데이터 보호 규정은 기업에서 데이터 처리 방식, 데이터에 대한 액세스 권한을 보유한 주체, 보안 이슈를 관리하는 방식을 파악하도록 만드는 데 중점을 두고 있습니다. Google에서 갖추고 있는 엔지니어 및 규정 준수 전문가 전담 팀은 고객이 규정 준수와 위험 관리 의무를 이행할 수 있도록 지원을 제공하고 있습니다. 고객이 구체적인 규정 요구사항을 이해하고 대응하도록 돕는 것도 Google의 보안 방침에 포함됩니다. 계속 새로운 감사 기준이 마련됨에 따라 팀은 새 기준을 충족하는 데 필요한 제어 도구, 프로세스, 시스템을 파악하고 제3자 기관에 독립적인 감사 및 평가를 의뢰하고 지원합니다. 또한 상황에 따라 고객이 Google의 보안 및 규정 준수 제어 도구를 검증하는 감사를 수행하도록 허용하기도 합니다.

보안 연구 커뮤니티와의 공동작업

Google에서는 오랜 기간 보안 연구 커뮤니티와 긴밀한 관계를 맺어왔으며 Google Workspace 및 기타 Google 제품의 취약점을 파악하는 데 있어 귀중한 도움을 받고 있습니다. Google은 사용자 보호에 도움을 주는 모든 외부의 기여에 감사를 표현하기 위해 취약성 발견 보상 프로그램을 개발했습니다. 이 프로그램은 연구자가 고객 데이터의 기밀성이나 무결성에 해가 되거나 고객 데이터를 위험에 빠뜨리는 설계 및 구현 문제를 신고하도록 장려하며 수만 달러 상당의 보상금을 제공합니다.

연구 커뮤니티와 공조한 결과 2019년에는 650만 달러의 보상금을 지급했는데 이는 역대 연간 지급액의 두 배 수준입니다. Google은 공개적으로 이 모든 분들의 기여에 감사를 표현했으며 Google 제품 및 서비스의 공헌자 명단에 포함했습니다.



운영 보안

Google에서 보안은 사후 조치 또는 간헐적으로 추진되는 이니셔티브가 아니라 사업 운영의 필수적 요소입니다.

취약점 관리

Google의 취약점 관리 프로세스는 상용 도구와 목적에 맞게 제작된 사내 도구, 집중적인 자동 및 수동 침투 테스트, 품질 보증 프로세스, 소프트웨어 보안 검토, 외부 감사를 조합한 방식으로 보안 위협을 능동적으로 검사합니다. 이를 통해 해결이 필요한 취약점이 식별되면 취약점팀에서 로깅하고, 심각도에 따라 우선순위를 매기며, 담당자를 지정합니다. 팀은 각 문제를 추적하고 해결된 것을 확인할 수 있을 때까지 여러 차례에 걸쳐 후속 관리를 수행합니다.

또한 Google에서는 보안 연구 커뮤니티 회원들과 관계를 유지하고 빈번하게 교류하여 Google 서비스 및 오픈소스 도구에서 보고된 문제를 추적합니다. 보안 문제 신고에 관한 자세한 내용은 Google 애플리케이션 보안에서 확인할 수 있습니다.

멀웨어 방지

강력한 멀웨어 공격으로 인해 계정 해킹, 데이터 도용, 네트워크에 대한 추가 액세스가 발생할 수 있습니다. Google에서는 네트워크와 고객에 대한 이러한 위협을 매우 심각하게 여기며 다양한 방법을 통해 멀웨어를 예방, 방지, 근절합니다.

멀웨어 사이트나 이메일 첨부파일은 개인 정보를 훔치거나, ID를 도용하거나, 다른 컴퓨터를 공격하기 위해 사용자의 컴퓨터에 악성 소프트웨어를 설치합니다. 이러한 사이트를 방문하면 본인도 모르는 사이에 컴퓨터를 해킹하는 소프트웨어가 설치됩니다. Google의 멀웨어 전략은 멀웨어나 피싱을 옮기는 매개체가 될 수 있는 웹사이트를 Google의 검색 색인으로 걸러내기 위해 수동 및 자동 스캐너를 사용하여 감염을 예방하는 과정부터 시작됩니다. 또 다른 핵심 보호 장치 중 하나는 매주 3,000억 개가 넘는 첨부파일을 처리하여 유해한 콘텐츠를 차단하는 첨부파일 멀웨어 스캐너입니다. Google에서 차단하는 악성 문서의 63%가 나날이 달라지는 만큼 위협의 진화 속도에 한발 앞서기 위해 최근에는 딥러닝을 사용하는 차세대 문서 스캐너를 추가하여 감지 역량을 향상했습니다.

매일 40억 개 넘는 기기가 Google 세이프 브라우징 기술의 보호를 받습니다. 세이프 브라우징은 매일 수천 개의 안전하지 않은 새로운 사이트를 발견하며 대부분은 합법적인 웹사이트가 해킹된 경우입니다. Google에서 안전하지 않은 사이트를 감지하면 Google 검색 및 웹브라우저에 경고를 표시합니다.

세이프 브라우징 솔루션 외에 Google에서는 VirusTotal을 운영합니다. VirusTotal은 파일과 URL을 분석하여 바이러스 백신 엔진과 웹사이트 스캐너가 감지한 바이러스, 웜, 트로이 목마, 기타 악성 콘텐츠를 식별할 수 있는

온라인 서비스입니다. VirusTotal의 임무는 바이러스 백신 및 보안 업계의 발전에 이바지하고 무료 도구와 서비스를 개발하여 인터넷을 더 안전한 공간으로 만드는 것입니다. Google에서는 Gmail, Drive, 서버, 워크스테이션에서 여러 가지 바이러스 백신 엔진을 사용하여 바이러스 백신 서명이 놓칠 수 있는 멀웨어를 식별하는 데 도움을 줍니다.

모니터링

Google의 보안 모니터링 프로그램은 내부 네트워크 트래픽에서 수집된 정보, 시스템상의 직원 작업, 취약점에 대한 외부 지식을 주로 살펴봅니다. 오픈소스 및 상용 도구를 조합해 트래픽을 캡처 및 파싱하여 Google 글로벌 네트워크의 여러 지점에서 내부 트래픽에 의심스러운 동작(예: 봇넷 연결을 나타내는 트래픽의 발생)이 있는지 검사합니다.

Google은 Google 기술을 바탕으로 구축된 독자적인 상관 시스템을 사용하고 시스템 로그에서 고객 데이터 액세스 시도 같은 이상 동작을 식별하여 이 네트워크 분석을 더욱 보완합니다. Google 보안 엔지니어는 공개 데이터 저장소에 상비 검색 알림을 설정하여 기업의 인프라에 영향을 줄 수 있는 보안 사고를 파악\=하고 적극적으로 인바운드 보안 보고서를 검토하며 공개 메일링 리스트, 블로그 게시물, 위키를 모니터링합니다. 자동 네트워크 분석은 알 수 없는 위협이 있는지 판단하는 데 도움을 주며 문제를 Google 보안 담당자에게 전달합니다. 또한 시스템 로그에 대한 자동 분석을 통해 이 절차를 보완합니다.

Google Workspace

이슈 관리

이슈 대응은 Google의 전반적인 보안 및 개인 정보 보호 프로그램에서 핵심적인 역할을 합니다. Google은 데이터 이슈를 관리하기 위한 엄격한 프로세스를 갖추고 있습니다. 이 프로세스는 기밀성, 무결성, 고객 데이터 가용성에 영향을 줄 수 있는 모든 잠재적 이슈의 조치, 에스컬레이션, 완화, 해결, 알림을 명시합니다. Google의 이슈 대응 프로그램은 각 이슈로 인해 제기되는 문제에 맞춰 적절히 대응할 수 있도록 다수의 전문 직무 분야를 아우르는 이슈 대응 전문가 팀이 관리합니다.

이러한 팀에서는 각 분야의 전문가들이 다양한 방식으로 함께 문제를 해결합니다. 예를 들어 이슈 책임자는 이슈의 성격을 평가하고 이슈 대응 업무를 조정하는데 여기에는 이슈의 심사 평가 완료, 심각도 조정(필요한 경우), 사실 관계를 검토하고 조사가 필요한 핵심 영역을 파악하는 적절한 운영/기술 책임자가 있는 이슈 대응팀 가동이 포함됩니다. 디지털 포렌식팀은 해결 과정의 일환으로 진행 중인 공격을 감지하고 포렌식 조사를 수행합니다. 제품 엔지니어는 고객에게 미치는 영향을 제한하고 영향을 받는 제품의 문제를 해결하는 솔루션을 제공합니다. 법무팀은 담당 보안 및 개인정보보호팀 팀원과 협력하면서 증거 수집에 관한 Google의 전략을 구현하고, 사법 기관 및 정부 규제 기관과 연계해 대응하며, 법률 문제 및 요건에 관해 조언합니다. 지원 인력은 고객 대상 알림을 관리하고 추가 정보 및 지원에 대한 고객의 문의와 요청에 대응합니다.

데이터 이슈에 대해 성공적으로 조치를 취하고 해결한 후, 이슈 대응팀은 해당 이슈에서 얻은 교훈을 평가합니다. 이슈로 인해 중대한 문제가 발생할 때는 이슈 책임자가 사후 분석을 시작할 수 있습니다. 이 절차를 거치면서 이슈 대응팀은 이슈의 원인과 Google의 대응을 검토하고 개선할 주요 영역을 파악합니다. 이를 위해 경우에 따라서는 다양한 제품, 엔지니어링 및 운영 팀과 상의하고 제품 개선 작업을 해야 할 수도 있습니다. 후속 작업이 필요한 경우 이슈 대응팀은 후속 작업을 완료하기 위한 실행 계획을 세우고 장기적 개선 노력을 이끌 프로젝트 관리자를 지정합니다. 해결 조치가 마무리된 이슈는 종결 처리됩니다.

보안을 핵심 가치로 삼는 기술

하드웨어, 소프트웨어, 네트워크, 시스템 관리 기술 분야의 혁신 기업인 Google은 '심층 방어' 원칙을 이용해 기존의 기술보다 더욱 안전하고 쉽게 관리할 수 있는 IT 인프라를 만들었습니다. Google은 서버, 독점 운영체제, 지리적으로 분산된 데이터 센터를 커스텀 방식으로 설계하여 Google Workspace가 안전하게 작동하도록 구상, 설계, 구축된 기술 플랫폼을 기반으로 운영됩니다.

최첨단 데이터 센터

데이터의 보안과 보호에 대한 Google의 집중적인 노력은 Google의 주요 설계 기준에도 반영되어 있습니다. Google 데이터 센터의 물리적 보안은 커스텀 설계된 전자 액세스 카드, 경보 장치, 차량 진입 방지 장벽, 방호 울타리, 금속 탐지기, 생체 정보 인식기를 포함한 여러 레이어로 구성된 보안 모델을 갖추고 있으며 데이터 센터가 위치한 층에는 레이저 빔을 이용한 침입 감지 장치가 설비됩니다.

데이터 센터는 연중 무휴, 하루 24시간 내내 침입자를 감지하고 추적할 수 있는 고해상도 내외부 카메라로 모니터링되고 있어 사고가 발생할 경우 액세스 로그, 활동 기록, 카메라 영상을 확인할 수 있습니다. 또한 철저한 신원 조사와 훈련을 거친 전문 보안 요원이 주기적으로 데이터 센터를 순찰합니다.

데이터 센터가 위치한 층에 가까워질수록 보안 검색도 강화됩니다. 사실 Google 직원 중 데이터 센터에 출입할 수 있는 직원은 1% 미만에 불과합니다. 특정 직무를 맡아 사전 승인을 받은 직원에 한해 보안 배지와 생체 인식 기술을 활용해 다중 액세스 제어를 구현하는 보안용 복도를 통해서 데이터 센터에 출입할 수 있습니다.

데이터 센터 전력 공급

연중무휴, 하루 24시간 내내 운영하고 무중단 서비스를 보장하기 위해, Google의 데이터 센터에는 전력 시스템과 환경 제어 장치가 이중화되어 있습니다. 냉각 시스템은 서버와 다른 하드웨어를 위해 일정한 작동 온도를 유지하여 서비스 중단 위험을 줄여줍니다. 사고에 대비해 모든 핵심 구성요소에는 기본 전원과 전력이 동일한 대체 전원이 있습니다. 디젤 엔진 백업 발전기는 각 데이터 센터를 최대 용량으로 운영하기에 충분한 비상 전력을 공급할 수 있습니다. 열, 화재, 연기 감지기를 비롯한 화재 감지 및 억제 장비는 해당되는 영역, 보안 운영 콘솔, 원격 모니터링 데스크에서 시청각 경보를 트리거하여 하드웨어의 손상을 방지하는 역할을 합니다.

친환경적 영향

Google은 데이터 센터의 환경 영향을 최소화하는 데 큰 관심을 가지고 최신 '친환경' 기술을 사용해 자체 설비를 설계하고 구축합니다. 또한 스마트 온도 제어 장치를 설치하고, 냉각을 위해 외기 또는 재사용 냉각수를 사용하는 등의 '무료 냉각' 기술을 사용하고, 배전 방식을 재설계하여 불필요한 에너지 손실을 줄입니다. 종합적인 효율 측정 기능을 사용해 각 설비의 성능을 계산하여 현 상태를 지속적으로 점검합니다.

Google은 대규모 인터넷 서비스 기업으로는 최초로 전체 데이터 센터의 우수한 환경 보호, 작업장 안전, 에너지 관리 기준을 인정받아 관련 외부 인증을 취득했다는 자부심을 가지고 있습니다. 특히 '계획을 밝힌 후에는 실행에 옮기고 계속 발전시켜 나간다'는 아주 단순한 개념을 중심으로 설계된 ISO 14001, OHSAS 18001, ISO 50001 인증을 자발적으로 취득했습니다.

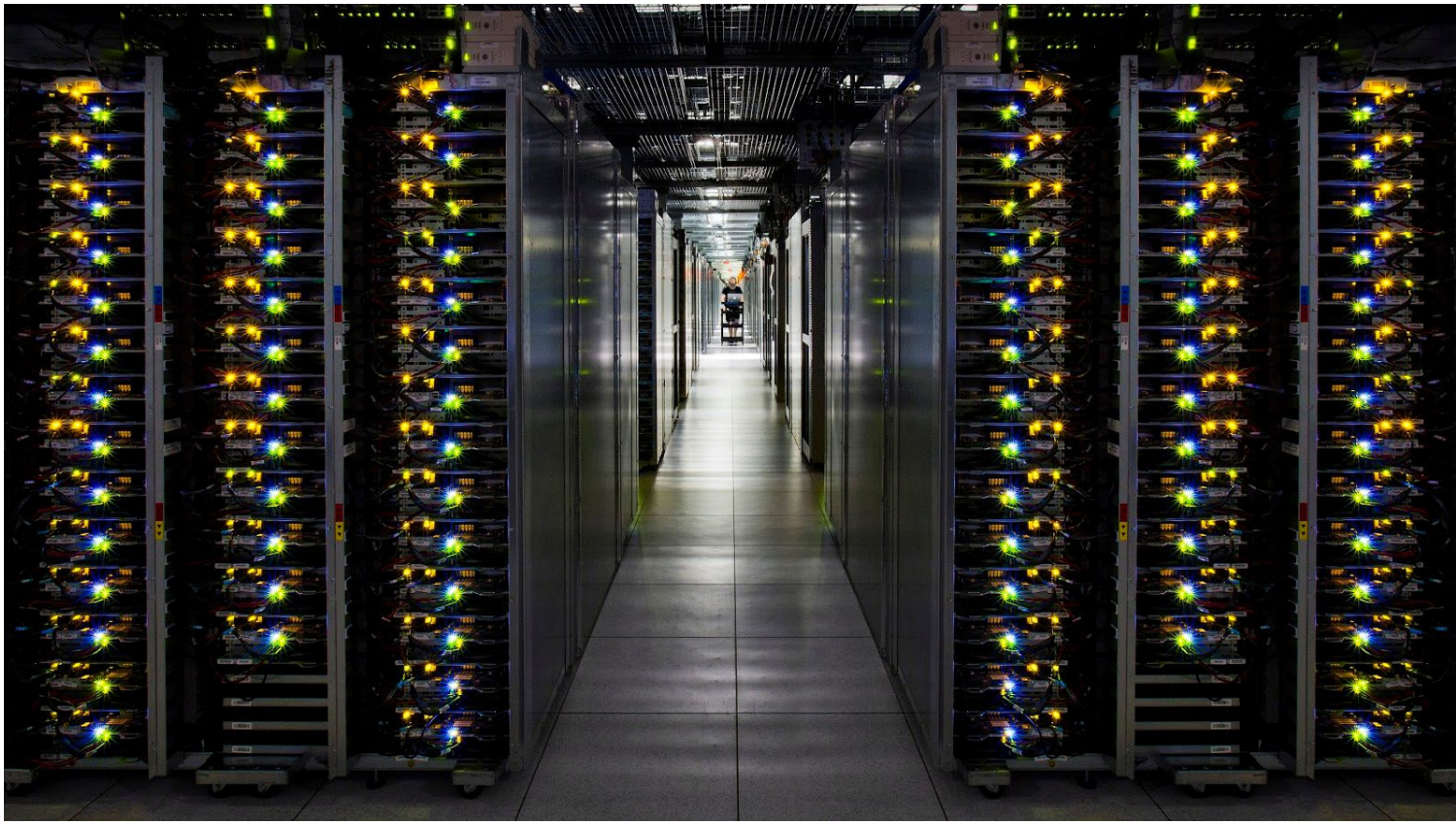
커스텀 서버 하드웨어 및 소프트웨어

Google의 데이터 센터는 에너지 효율적이고 목적에 부합하는 커스텀 서버와 네트워크 장비를 수용하며 이러한 서버와 장비는 Google에서 직접 설계 및 제조합니다. 또한 Google의 프로덕션 서버는 불필요한 요소를 제외한 Linux의 강화 버전을 기반으로 커스텀 설계된 운영체제(OS)를 실행합니다. 다시 말해 Google의 서버와 OS는 Google 서비스를 제공한다는 단 하나의 목적만 염두에 두고 설계되었습니다. 대다수 상용 하드웨어와 달리 Google 서버는 비디오 카드, 칩셋 또는 주변기기 커넥터와 같이 취약점을 유발할 수 있는 불필요한 구성요소를 포함하지 않습니다. Google 서버 리소스는 동적으로 할당되므로 고객 요구를 바탕으로 리소스를 추가하거나 다시 할당하는 성장 유연성과 신속하고 빠른 적응 기능이 가능합니다. 이 동종 환경은 시스템에서 바이너리 수정을 계속 모니터링하는 독점 소프트웨어를 통해 유지관리됩니다. 표준 Google 이미지와 달리 수정된 부분이 발견되면 시스템이 자동으로 공식 상태로 복구됩니다. 이러한 자동 복구 메커니즘을 통해 Google은 시스템 안정을 저해하는 사건을 모니터링 및 해결하고, 사고에 대한 알림을 받으며, 심각한 문제가 발생하기 전에 잠재적인 네트워크 손상을 지연할 수 있습니다.

하드웨어 추적 및 폐기

Google은 바코드와 자산 태그를 통해 획득과 설치부터 사용 중지, 폐기에 이르기까지 데이터 센터 내 모든 장비의 위치와 상태를 세심하게 추적합니다. 또한 금속 탐지기와 비디오 감시를 통해 어떤 장비도 승인 없이 데이터 센터에서 반출되지 못하도록 합니다. 데이터 센터에서 수명 주기 중 언제라도 성능 테스트를 통과하지 못한 구성요소는 인벤토리에서 삭제되어 사용 중지됩니다.

각 데이터 센터는 엄격한 폐기 정책을 준수하고 모든 불일치를 즉시 해결합니다. 하드 드라이브가 사용 중지되면 승인받은 직원이 해당 드라이브를 0으로 덮어쓰고 드라이브에 포함된 데이터가 없도록 여러 단계의 확인 프로세스를 거쳐 디스크가 삭제되었는지 확인합니다. 이유를 불문하고 드라이브의 삭제가 불가능한 경우 물리적으로 폐기될 때까지 안전하게 보관합니다. 디스크의 물리적 파기는 압축기를 사용하여 드라이브를 변형시키는 단계부터 시작해 파쇄기로 드라이브를 작은 조각으로 부순 다음 안전한 시설에서 재활용하는 다단계 절차로 진행됩니다.



고유한 보안 이점을 지닌 글로벌 네트워크

Google의 IP 데이터 네트워크는 Google 자체 광섬유 케이블, 공용 광섬유 케이블, 해저 케이블로 이루어져 있기 때문에 지구촌 곳곳으로 가용성이 높고 지연 시간이 짧은 서비스를 제공할 수 있습니다.

다른 클라우드 서비스와 온프레미스 솔루션에서는 고객 데이터가 공용 인터넷을 통해 '홉'이라는 기기 사이의 여러 이동 경로를 거쳐야 합니다. 홉의 수는 고객의 ISP와 솔루션의 데이터 센터 간 거리에 따라 다르며 홉이 추가될 때마다 데이터를 공격하거나 가로챌 새로운 기회가 생기는 셈입니다. Google 글로벌 네트워크는 전 세계 대부분의 ISP에 연결되어 있으므로 공개 인터넷에서 홉의 수가 제한될 수 있어 전송 중 데이터의 보안이 강화됩니다.

심층 방어는 Google의 네트워크를 외부 공격으로부터 보호해주는 여러 방어 계층을 설명합니다. 우선 업계 표준 방화벽과 액세스 제어 목록(ACL)을 사용하여 네트워크 분리를 시행하고 악의적 요청과 DDoS(Distributed Denial of Service) 공격을 감지하고 멈추기 위해 모든 트래픽이 커스텀 Google Front End(GFE) 서버를 통해 라우팅됩니다. 그 밖에도 GFE 서버는 내부적으로 통제되는 목록의 서버와의 통신만 가능한데 이 '기본 거부' 구성은 GFE 서버가 의도치 않은 리소스에 액세스하지 못하도록 막습니다. 마지막으로, 정기적인 로그 검사를 통해 프로그래밍 오류를 악용한 상황을 파악하며 네트워크에 연결된 기기에 대한 액세스는 승인된 직원으로 한정됩니다. 결론적으로 Google 보안 요구사항을 준수하는 승인된 서비스와 프로토콜만 Google 네트워크를 순회할 수 있으며 나머지는 모두 자동으로 삭제됩니다.

전송 및 저장 상태의 데이터 암호화

암호화는 Google Workspace 보안 전략의 중요한 요소이므로 이메일, 채팅, 화상 회의, 파일, 기타 데이터를 보호하는 데 도움이 됩니다. 첫째 Google에서는 디스크(솔리드 스테이트 드라이브 포함) 또는 백업 미디어에 '저장된 상태'의 특정 데이터를 아래의 설명과 같이 암호화합니다. 공격자나 물리적으로 접근한 사람이 데이터가 포함된 스토리지 장비를 확보하더라도 필요한 암호화 키가 없으면 읽을 수 없습니다. 둘째 인터넷을 통해 전달되거나 데이터 센터 간 Google 네트워크를 통해 이동하는 '전송 중'인 모든 고객 데이터를 암호화합니다. 공격자가 이러한 전송을 가로채는 경우 암호화된 상태의 데이터를 확보할 뿐입니다. 저장 및 전송 상태의 데이터를 암호화하는 방법은 아래에서 자세히 살펴보겠습니다.

Google은 이메일 라우팅에 전송 계층 보안(TLS)을 사용하여 업계를 선도한 업체로서 Google과 Google 이외의 서버 간 통신이 암호화 방식으로 이루어지도록 지원합니다. Google 서버에서 TLS를 지원하는 타사 서버로 이메일을 보내는 경우에도 트래픽이 암호화되어 패시브 도청을 방지합니다. Google은 TLS 보급이 업계에 중요하다고 생각하여 이메일 암호화 투명성 보고서에서 TLS 진행 상황을 보고하고 있습니다. 또한 수신 도메인에서 이메일의 전송 기밀성 및 무결성 보안을 요구하도록 만드는 MTA-STS 표준을 개발 및 지원하여 전송 중인 이메일의 보안을 강화했습니다. Google Workspace 고객은 이러한 도메인과 주소에 TLS가 적용되는 경우 특정 도메인 및 이메일 주소로만 이메일 전송을 허용하는 기능을 추가로 사용할 수 있습니다. TLS 규정 준수 설정을 통해 이 기능을 관리할 수 있습니다.

암호화에 관한 자세한 내용은 Google Workspace 암호화 백서를 참조하세요.

지연 시간이 짧고 가용성이 높은 솔루션

Google에서는 서버 설계와 데이터 저장 방식부터 네트워크 및 인터넷 연결, 소프트웨어 서비스에 이르기까지 Google 플랫폼의 모든 구성요소가 고도의 중복성을 갖도록 설계합니다. 이 '모든 요소의 중복성'에는 설계상의 오류 처리가 포함되고 단일 서버, 데이터 센터, 네트워크 연결에 종속되지 않는 솔루션이 생성됩니다.

Google의 데이터 센터는 지리적으로 분산되어 있어 자연재해 및 현지의 절전 같은 지역적 장애 요인이 미치는 영향을 최소화합니다. 하드웨어, 소프트웨어, 네트워크 장애가 발생하는 경우 해당 시설의 데이터가 자동으로 다른 시설로 옮겨가기 때문에 Google Workspace 고객은 아무런 지장 없이 작업을 지속할 수 있습니다. 인력이 전 세계에 포진되어 있는 고객은 추가 구성이나 지출 없이 문서, 화상 회의 등을 통해 공동작업을 수행하여 단일 글로벌 네트워크에서 협업하면서 성능이 높고 지연 시간이 짧은 환경을 공유할 수 있습니다.

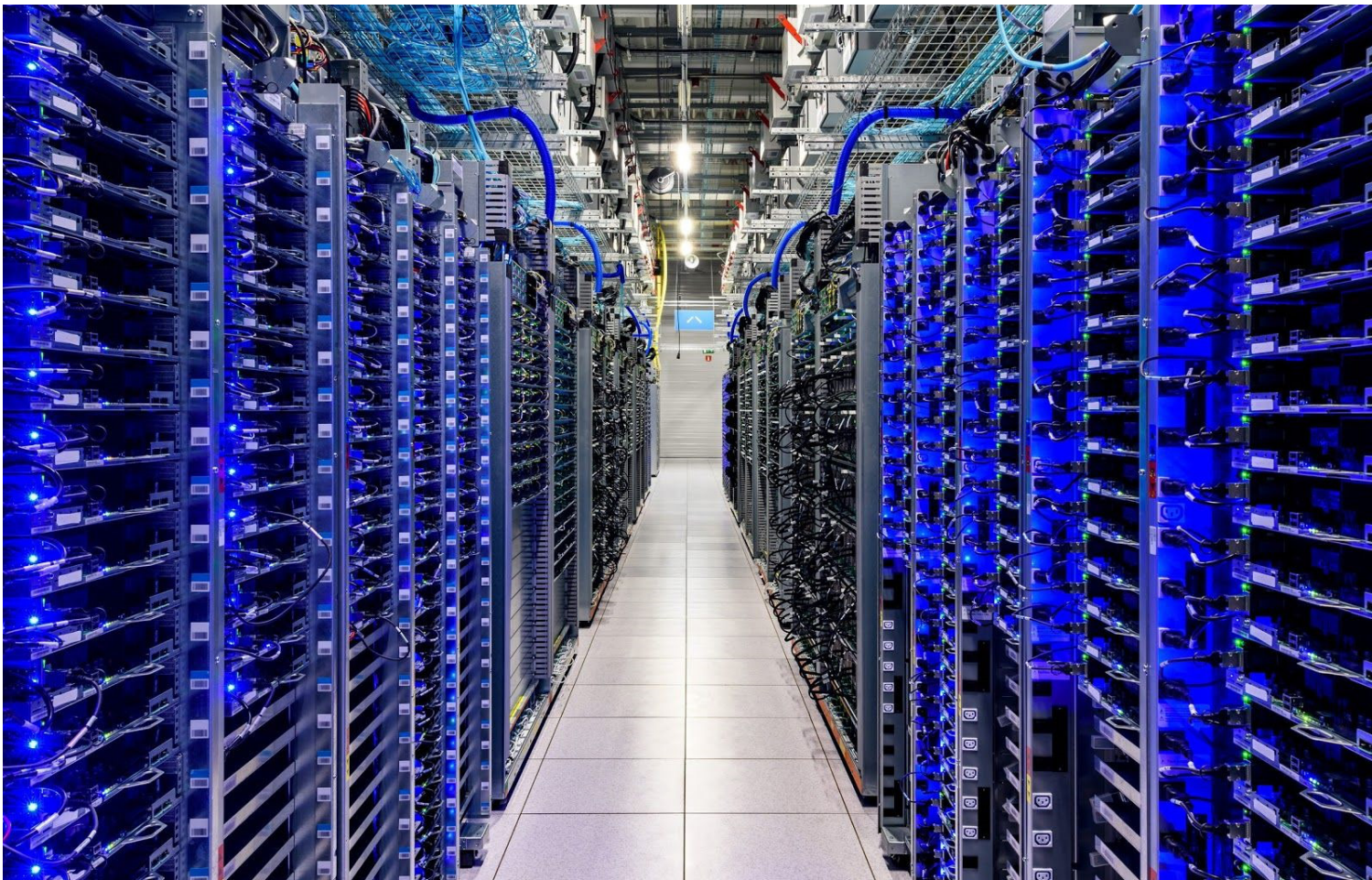
Google의 중복성이 높은 인프라 역시 데이터 손실로부터 고객을 보호해 줍니다. Google Workspace의 경우 복구 시점 목표(RPO)는 0(제로)이며 복구 시간 목표(RTO) 설계 목표 역시 0(제로)입니다. Google은 실시간 및 동기식

복제를 통해 이러한 목표를 달성하고자 합니다. 즉 Google Workspace 제품에서 수행하는 작업은 두 곳의 데이터 센터에 동시 복제되므로 데이터 센터 한 곳에 장애가 발생하더라도 작업을 반영하고 있던 다른 센터로 내 데이터가 전송됩니다.

이 작업을 효과적이고 안전하게 수행하기 위해 고객 데이터는 임의의 파일 이름이 지정된 디지털 조각으로 나누어집니다. 이러한 조각의 콘텐츠와 파일 이름 모두 사람이 읽을 수 없는 형식으로 저장되며 저장된 고객 데이터를 스토리지에서 검사하더라도 관련된 특정 고객 또는 애플리케이션을 추적할 수 없습니다. 각 조각은 단일 장애점을 피하기 위해 여러 디스크, 여러 서버, 여러 데이터 센터에 실시간에 가깝게 복제됩니다. 최악의 상황에 철저히 대비하기 위해 기업 본사를 포함해 각 데이터 센터가 30일간 작동 불능인 상태로 가정하는 재해 복구 훈련을 실시하고 있습니다.

서비스 가용성

관할권에 따라 일부 Google 서비스를 현재 또는 일시적으로 이용하지 못할 수 있습니다. Google의 투명성 보고서는 Google 제품에 대한 최근 및 지속적인 트래픽 중단을 보여줍니다. Google은 코드를 통해 시간 경과에 따른 전 세계 트래픽 패턴을 관찰하여 현저한 변경사항을 감지할 수 있습니다. 또한 기자, 사회 운동가, 현장 종사자에게 문의를 받을 때 그래프를 살펴봅니다. 이 데이터는 대중이 온라인 정보의 가용성을 분석하고 이해하는 데 도움이 되도록 제공됩니다.



Google Workspace

규정 준수 요건 지원

Google은 규정 준수 및 보고 요구사항을 충족하는 안전한 제품과 서비스를 제공하기 위해 최선을 다하고 있습니다. Google은 권장사항에 대한 광범위한 정보를 공유하며 규정 준수 문서에 대한 간편한 액세스를 제공합니다. 업계를 선도하는 Google Cloud의 보안, 제3자 감사 및 인증, 문서, 법적 계약은 규정 준수를 지원합니다. Google 제품은 보안, 개인 정보 보호, 규정 준수 관리에 대해 독립 기관으로부터 정기적인 검증을 받고 있으며, 글로벌 표준에 대한 인증, 규정 준수 증명, 감사 보고서를 취득하고 있습니다. 제3자 감사 기관은 독립적인 검증 프로세스의 일환으로 데이터 센터, 인프라, 운영을 비롯한 엔드 투 엔드 보안 관행을 정기적으로 조사합니다. 또한 공식 인증 또는 증명이 의무가 아니거나 적용될 수 없는 경우에는 프레임워크 및 법규에 따라 리소스를 문서화 및 매핑하고 있습니다. Google의 규정 준수 리소스 센터에는 규정 준수 문서 및 리소스에 관한 세부정보가 나와 있습니다.

Google은 규정 준수 범위를 확대하기 위해 지속적인 노력을 기울이고 있습니다. Google은 규정 준수 환경의 변화에 따라 앞서가는 기준과 규제 기관의 가이드를 평가해 보안 및 개인 정보 보호 프로그램을 조정합니다. 리전 및 산업별로 프로그램을 세심하게 선별하므로 고객이 규정 준수 리소스를 활용하여 비즈니스에 맞게 정보에 입각한 결정을 내릴 수 있게 됩니다.

Google Workspace를 고려하는 경우 규정 준수 서비스를 통해 제품군이 보안 및 규정 준수 니즈에 맞는지 여부를 확인해 볼 수 있습니다.

규정 준수

Google의 고객은 금융, 정부, 의료, 교육 등 규제 대상 업계에서 사업을 운영하기도 합니다. Google Cloud는 고객이 업종별 여러 요구사항을 충족하도록 지원하는 방식으로 제품과 서비스를 제공합니다. 보다 자세한 정보는 여기를 참조하세요.

독립적인 제3자 인증 및 증명

Google 고객과 규제 당국은 보안, 개인 정보 보호, 규정 준수 조치에 대한 독립 기관의 검증을 기대합니다. Google에서는 이 같은 확신을 제공하기 위해 정기적으로 여러 제3자 독립 기관의 감사를 받고 있습니다. 감사 대상인 주요 국제 기준은 다음과 같습니다.

- ISO/IEC 27001(정보 보안 관리)
- ISO/IEC 27017(클라우드 보안)
- ISO/IEC 27018(클라우드 개인 정보 보호)
- ISO/IEC 27701(개인 정보 보호)
- SOC 2 및 SOC 3 보고서

Google은 분야 및 국가별 프레임워크에도 참여하고 있으며 FedRAMP(미국 정부), BSI C5(독일), MTCS(싱가포르) 등이 그 예입니다. 또한 공식 인증 또는 증명이 의무가 아니거나 적용되지 않는 프레임워크 환경에서는 리소스를 문서화 및 매핑하고 있습니다.

규정 준수 서비스의 전체 목록은 규정 준수 리소스 센터를 참조하세요.

데이터 사용

Google의 철학

Google Workspace 고객 데이터의 소유자는 Google이 아닌 고객 본인입니다. Google Workspace 조직에서 Google 시스템에 보관하는 고객 데이터는 고객의 소유이며 Google은 광고의 목적으로 이러한 데이터를 검색하지 않습니다. Google에서는 고객 데이터 보호를 위해 기울이는 노력을 설명하는 상세한 데이터 처리 수정안을 고객에게 제공합니다. 그뿐만 아니라 고객이 데이터를 삭제하는 경우 180일 내에 시스템에서 삭제할 것을 약속합니다. 마지막으로, Google에서는 고객이 Google 서비스를 더 이상 사용하지 않기로 결정하는 경우 위약금이나 추가 비용을 내지 않고 고객 관리자가 데이터를 쉽게 가져갈 수 있는 도구를 제공합니다.

Google Workspace의 무광고 정책

Google Workspace 핵심 서비스에는 광고가 없으며 앞으로도 이 방침을 바꿀 계획이 없습니다. Google은 광고 목적으로 Google Workspace 핵심 서비스에서 데이터를 수집하거나, 검사하거나, 사용하지 않습니다. 고객 관리자는 Google Workspace 관리 콘솔에서 비핵심 서비스에 대한 액세스를 제한할 수 있습니다. Google이 고객 데이터에 색인을 생성하는 목적은 스팸 필터링, 바이러스 감지, 맞춤법 검사, 개별 계정 내 이메일 및 파일 검색 기능 같은 유용한 서비스를 제공하는 데 있습니다.

데이터 액세스 및 제한사항

관리 액세스

Google에서는 고객 데이터에 액세스할 수 있는 직원 수를 제한하고 해당 직원의 활동을 적극적으로 모니터링할 수 있도록 내부 시스템을 설계했습니다. Google 직원에게는 기업 리소스에 액세스할 수 있는 제한적인 기본 권한 집합만 부여됩니다. 내부 지원 도구 액세스는 액세스 제어 목록(ACL)을 통해 제어됩니다. Google은 정식 절차에 따라 Google 리소스에 대한 직원의 액세스를 허용하거나 취소하고 퇴사한 직원의 액세스 권한은 자동으로 삭제됩니다. 액세스 승인은 관련된 모든 시스템 계층에 적용됩니다. 승인은 워크플로 도구로 관리되고 로깅됩니다.

직원의 승인 설정은 Google Workspace 제품의 데이터 및 시스템을 비롯한 모든 리소스에 대한 액세스 권한을 제어하는 데 사용됩니다. 액세스 권한은 제어 도구의 효과에 대한 확인 차원에서 전담 보안팀에서 모니터링합니다. 이때 보안팀은 액세스 패턴을 적극적으로 모니터링하고 비정상적인 이벤트를 조사합니다.

아울러 Google은 투명성 및 사용자 신뢰성에 대한 장기적인 노력의 일환으로 액세스 투명성을 제공합니다.[3] 이 기능을 통해 고객은 Google 직원이 특정 고객 데이터에 액세스할 때 해당 직원이 수행한 작업의 로그를 검토할 수 있습니다. 액세스 투명성과 통합된 서비스의 경우 Google은 업무상 필요한 타당한 이유로 사용자의 데이터에 액세스하고 있는지 확인하는 도구를 사용하고 액세스 투명성 로그에 정당한 사유를 로깅합니다.

자세한 내용은 Google Workspace에 보관된 데이터 신뢰성 백서를 참조하세요.

고객 관리자의 경우

고객은 Google Workspace의 데이터 및 서비스에 대한 액세스 권한을 제어하여 조직에서 원하는 구성에 따라 데이터가 보호되는지 확인할 수 있습니다. 고객은 역할 기반 액세스 권한 제어를 통해 사용자를 관리자로 지정하여 Google Workspace 관리 콘솔에서 특정 작업에 액세스하고 수행하는 기능을 부여합니다. 사용자를 관리 콘솔에서 모든 작업을 수행할 수 있는 최고 관리자로 지정할 수도 있습니다. 또는 그룹 생성, 서비스 설정 관리, 사용자 비밀번호 재설정 중 하나만 허용하는 등 관리자가 수행할 수 있는 작업을 제한하는 역할을 할당할 수도 있습니다.

사법 기관의 데이터 요청

데이터 소유자로서 사법 기관의 데이터 요청에 대처할 주된 책임은 고객에게 있으며, 정부가 고객에게 데이터를 직접 요청하도록 안내하는 것이 Google의 정책입니다. 하지만 다른 기술 및 통신 회사와 마찬가지로

[2] 2단계 인증 배포에 관한 자세한 내용은 지원 페이지에서 확인할 수 있습니다.

Google에서도 전 세계 각국의 정부 및 법원으로부터 사용자가 Google 서비스를 어떻게 사용해왔는지 답해 달라는 직접적인 요청을 받을 수 있습니다. Google은 고객의 개인 정보를 보호하고 과도한 요청을 제한하는 한편 법률상 의무도 준수하기 위한 조치를 취합니다. 이러한 법률상 요청을 따르는 동시에 고객이 Google을 통해 저장하는 데이터의 개인 정보 보호와 보안을 계속 최우선순위로 삼고 있습니다.

데이터 요청 및 그러한 요청에 대한 Google의 대응에 관한 자세한 정보는 투명성 보고서를 참조하세요. 보다 자세한 내용은 Google Workspace에 보관된 데이터 신뢰성 백서에도 나와 있습니다.

제3자 공급업체

Google에서는 사실상 모든 데이터 처리 활동을 직접 수행하여 서비스를 제공합니다. 하지만 고객 지원 및 기술 지원과 같은 Google Workspace 관련 서비스를 제공하기 위해 일부 제3자 공급업체와 계약을 맺기도 합니다. 제3자 공급업체가 업무에 참여하기 전에 Google에서는 해당 공급업체의 보안 및 개인 정보 보호 관행을 평가하여 업체에 부여할 데이터 액세스 권한과 그 업체가 제공하기로 계약한 서비스의 범위에 비추어 볼 때 타당한 수준의 보안 및 개인 정보 보호를 제공하도록 보장합니다. Google에서 제3자 공급업체로 인해 발생하는 위험을 평가하고 나면 공급업체는 적절한 보안, 비밀유지, 개인 정보 보호 계약을 체결해야 합니다.

Google Workspace

사용자 및 관리자의 보안 및 규정 준수 지원

Google은 구조, 기술, 업무 운영, 고객 데이터 접근 방식에 보안 체계를 구축합니다. Google Workspace 고객이라면 누구나 Google의 강력한 보안 인프라와 시스템을 기본적으로 사용할 수 있습니다. 더 나아가 사용자가 대시보드와 계정 보안 마법사를 통해 비즈니스 니즈에 맞게 개별 보안 설정을 개선하고 맞춤설정할 수 있도록 적극적으로 지원합니다.

또한 Google Workspace는 조직의 규모에 상관없이 관리 콘솔을 통해 하나의 대시보드에 인프라, 애플리케이션, 시스템 통합을 구성할 수 있는 전체 제어 도구를 관리자에게 제공하여 관리와 구성을 간소화합니다. 온프레미스 이메일 시스템에 DKIM(피싱 방지 기능)을 배포하는 것을 고려하세요. 기존에는 관리자가 모든 서버에 대해 별도로 패칭 및 구성 작업을 수행해야 했으며 잘못 구성하면 서비스 중단이 발생했습니다. 하지만 Google의 관리 콘솔을 사용하는 경우 몇 분이면 DKIM을 수천 개, 혹은 수십만 개의 계정에 대해 안전하게 구성할 수 있으며 서비스 중단이 발생하거나 유지보수 기간이 필요하지 않습니다.

이것은 한 가지 예에 불과합니다. 관리자에게 제공되는 다양한 강력한 도구 중에는 2단계 인증 및 싱글 사인온(SSO), 보안 전송(TLS)과 같은 이메일 보안 정책 시행 등의 인증 기능이 있으며 이 모든 기능이 조직의 보안 및 시스템 통합 요구사항을 충족하도록 구성할 수 있습니다.

액세스 및 인증

2단계 인증 및 보안 키

고객은 2단계 인증 및 보안 키를 사용해 계정 보안을 강화할 수 있습니다.[3] 이 도구를 사용하면 직원의 액세스 권한 제어를 잘못 구성하거나 공격자가 계정을 해킹해 활용하는 등의 위험을 완화할 수 있습니다.[4] Google은 엔터프라이즈용 고급 보호 프로그램을 사용하여 등록된 사용자를 대상으로 선별된 강력한 계정 보안 정책을 적용할 수 있습니다. 이러한 정책에는 보안 키 요구, 신뢰하지 않는 앱에 대한 액세스 차단, 이메일 위협 검사 개선이 포함됩니다.

싱글 사인온(SAML 2.0)

Google Workspace는 사용자가 동일한 로그인 페이지와 인증 정보를 사용해 여러 서비스에 액세스할 수 있도록 지원하는 싱글 사인온(SSO) 서비스를 고객에게 제공합니다. 이 기반이 되는 SAML 2.0은 사용자 인증 및 승인 데이터를 교환하는 안전한 웹 도메인을 제공하는 XML 표준입니다. 보안을 더욱 강화하려면 SSO에서 RSA 또는 DSA 알고리즘 방식으로 생성된 공개 키 및 인증서를 사용합니다. 고객사는 SSO 서비스를 사용하여 Google Workspace의 싱글 사인온(SSO)을 LDAP 또는 기타 SSO 시스템에 통합할 수 있습니다.

OAuth 2.0 및 OpenID Connect

Google Workspace는 OAuth 2.0 및 OpenID Connect를 지원합니다. 이 기술은 고객이 여러 개의 클라우드 솔루션에 하나의 싱글 사인온(SSO) 서비스를 구성할 수 있도록 지원하는 개방형 인증 및 승인 프로토콜입니다. 사용자는 사용자 인증 정보를 다시 입력하거나 민감한 비밀번호 정보를 공유하지 않아도 Google Workspace를 통해 제3자 애플리케이션에 로그인하거나 그 반대 경로로 로그인할 수도 있습니다.

정보 권한 관리(IRM)

대부분의 조직은 **민감한 정보의 처리**를 결정하는 내부 정책을 갖추고 있습니다. Google에서는 Google Workspace 관리자가 민감한 정보에 대한 제어 기능을 유지할 수 있도록 Google Drive에서 **정보 권한 관리** 기능을 제공합니다. 관리자와 사용자는 Google Drive의 액세스 권한을 통해 파일 재공유, 다운로드, 인쇄, 복사 또는 사용 권한 변경을 방지하여 민감한 콘텐츠를 보호합니다.

이메일 전송 제한

기본적으로 도메인에서 Gmail 계정을 사용하는 사용자는 모든 이메일 주소와 메일을 주고받을 수 있습니다. 경우에 따라 관리자는 메일을 주고받을 수 있는 이메일 주소를 제한할 수 있습니다. 예를 들어 학교에서는 학생들이 교직원 및 다른 학생과 메일을 주고받도록 허용하지만 학교 외부의 사용자와는 메일을 주고받지 못하게 할 수 있습니다.

---

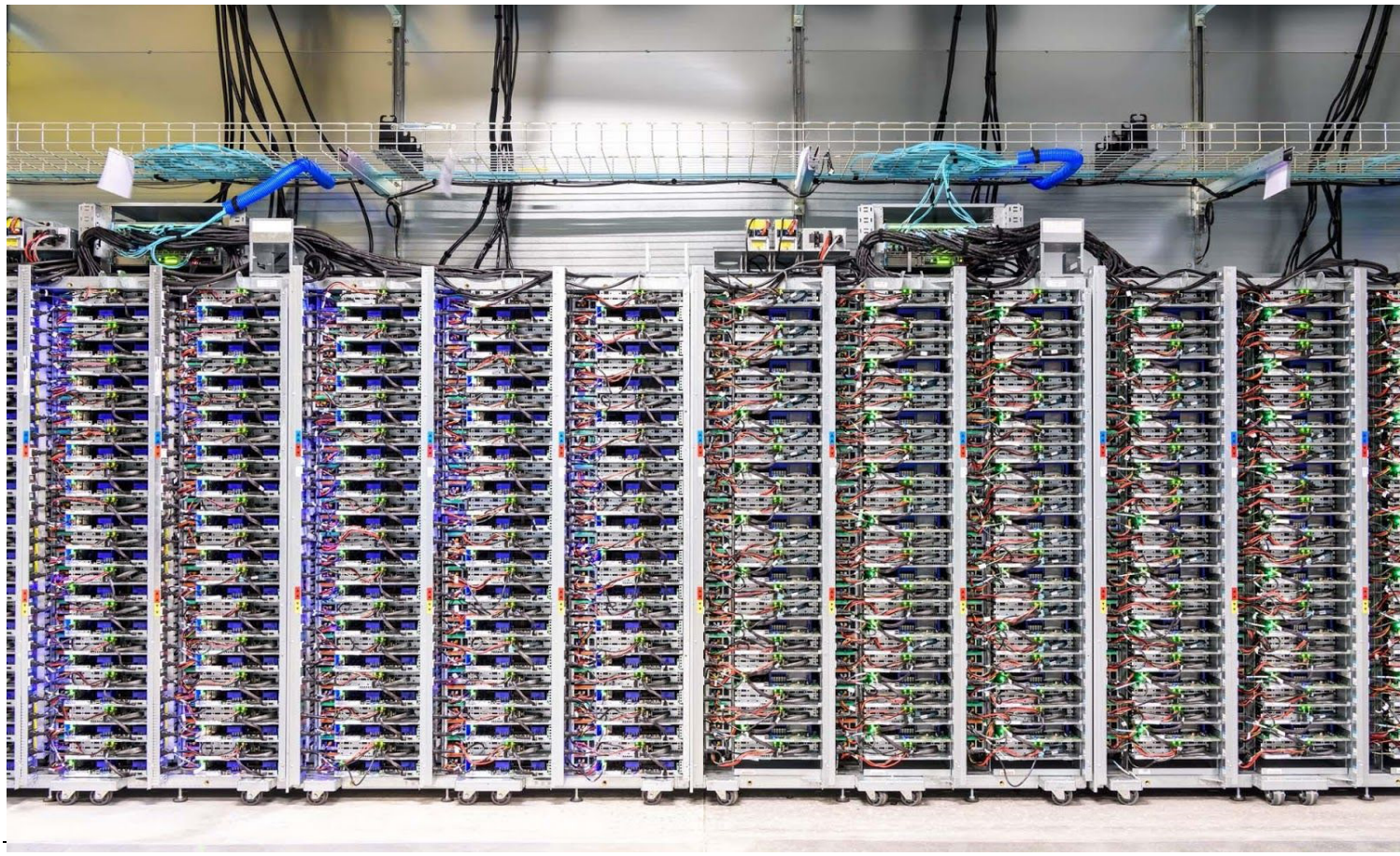
[3] 2단계 인증 배포에 관한 자세한 내용은 지원 페이지에서 확인할 수 있습니다.

[4] 보안 권장사항 가이드는 보안 체크리스트 페이지를 참조하세요.

전송 제한 설정을 사용하는 경우 관리자는 사용자가 이메일 메시지를 주고받을 수 있는 주소와 도메인을 지정할 수 있습니다. 관리자가 전송 제한 설정을 추가하면 사용자는 승인된 대상에 한해 소통할 수 있습니다. 목록에 없는 도메인으로 메일 전송을 시도하는 사용자는 해당 주소로 메일 전송을 금지한다는 정책이 명시되고 메일이 발송되지 않았음을 확인하는 메시지를 받게 됩니다. 마찬가지로, 사용자는 목록에 포함된 도메인으로부터 인증된 메시지만 수신하게 됩니다. 승인되지 않은 도메인에서 보낸 메시지 또는 승인된 도메인이더라도 DKIM이나 SPF 레코드로 확인할 수 없는 메시지는 정책 안내 메시지와 함께 발신자에게 반송됩니다.

사용자 컨텍스트 기반의 앱 액세스

사용자 액세스를 더욱 용이하게 만드는 동시에 데이터 보안을 강화하기 위해 Google에서는 컨텍스트 인식 액세스를 개발했습니다.[5] 이 기능을 통해 사용자 ID와 요청 컨텍스트(기기 보안 상태 또는 IP 주소 등)를 기반으로 Google Workspace 앱을 세밀하게 제어할 수 있습니다. Google에서 개발한 BeyondCorp 보안 모델을 기반으로 하는 경우 사용자는 원격 액세스 VPN 게이트웨이를 활용할 필요 없이 거의 모든 기기를 사용해 어디서든 웹 애플리케이션과 인프라 리소스에 액세스할 수 있으며 관리자는 기기에 대한 제어 시스템을 구축할 수 있습니다. 또한 조직 단위 또는 그룹의 모든 구성원을 위해 2단계 인증 같은 액세스 정책을 설정할 수도 있습니다.



[5] Cloud ID와 통합됨. 컨텍스트 인식 액세스 기능을 사용하여 Google Workspace 앱에 대한 액세스를 보호하려면 Cloud ID Premium 또는 Google Workspace Enterprise 라이선스가 필요합니다.

자산 보호

이메일 스팸, 피싱, 멀웨어 보호

Gmail은 스팸, 피싱 시도, 멀웨어로부터 수신 메일을 보호합니다. 이러한 기능을 수행하는 데 기존 머신러닝 모델이 매우 효과적이며 다른 보호 장치와 연계하면 Gmail 받은편지함에 도달하기 전에 99.9% 이상의 위협을 차단할 수 있습니다. 또 다른 핵심 보호 조치로 매주 3,000억 개가 넘는 첨부파일을 처리하여 유해한 콘텐츠를 차단하는 멀웨어 스캐너를 들 수 있습니다.[6] Google에서 차단하는 악성 문서의 63%가 매번 다른 종류입니다.[7] 그뿐 아니라 Gmail에서는 보안 샌드박스라고 하는 가상 환경에서 첨부파일을 검사하거나 실행할 수 있습니다. 위협으로 파악된 첨부파일은 사용자의 스팸 폴더로 보내거나 격리할 수 있습니다.

Google에서는 조기 피싱 감지를 사용해 스팸 감지 정확성을 지속적으로 개선하고 있습니다. 이 기능은 엄격한 피싱 분석을 수행하고 사용자 데이터를 해킹으로부터 보호하기 위해 메일을 선별적으로 지연(평균 메시지의 0.05% 미만)시키는 전용 머신러닝 모델입니다.

감지 모델은 수상하고 의심스러운 URL을 발견하고 표시하기 위해 Google 세이프 브라우징 머신러닝 기술과 통합됩니다. 이러한 새로운 모델은 URL의 평판 및 유사성 분석 같은 다양한 기술을 조합하기 때문에 Google은 피싱 및 멀웨어 링크에 대해 새로운 URL 클릭 시 경고를 생성할 수 있습니다. 이와 같이 새로운 패턴을 찾으면 시간이 흐를수록 모델이 개선되며 수동 시스템에 비해 훨씬 빠르게 적응합니다.

이메일 스푸핑 방지

스팸 발송자는 때때로 이메일 메시지의 '보낸사람' 주소를 평판이 좋은 조직의 도메인에서 전송된 것처럼 보이도록 위조할 수도 있습니다. 이 이메일 스푸핑을 방지하기 위해 Google은 DMARC 프로그램에 참여하고 있습니다. 이 프로그램을 통해 도메인 소유자는 자신의 도메인에서 전송된 인증되지 않은 메일의 처리 방법을 이메일 제공업체에 알릴 수 있습니다. Google Workspace 고객은 관리자 설정에서 DMARC 레코드를 만들고, 모든 발신 메일 스트림에서 SPF 레코드 및 DKIM 키를 구현하여 DMARC를 적용할 수 있습니다.

데이터 손실 방지를 위한 직원 대상 경고

직원이 데이터 보호를 위해 올바른 결정을 내릴 수 있도록 지원하면 기업의 보안 상태를 개선할 수 있습니다. 이에 도움이 되도록 Gmail은 데이터 손실 방지를 지원하는 의도하지 않은 외부 응답 경고를 사용자에게 표시합니다. 기업 도메인의 외부에 있는 사람에게 회신을 시도하면 해당 이메일을 보낼 의도가 있었는지 확인하는 경고를 즉시 받게 됩니다. 또한 Gmail의 상황별 인텔리전스가 수신자가 외부 담당자인지, 정기적으로 소통하는 사람인지 여부를 파악해 불필요하게 경고를 표시하는 것을 피할 수 있습니다.

[6] 2020년 2월 기준

[7] 2020년 2월 기준

보안 강화를 위해 호스팅된 S/MIME

Google의 호스팅된 S/MIME 솔루션을 통해 S/MIME이 포함된 암호화 이메일을 받으면 Google의 암호화를 통해 저장됩니다. 즉 모든 이메일이 정상적으로 처리될 수 있으며 여기에는 폭넓은 스팸, 피싱, 멀웨어 방지와 관리 서비스(예: Vault 보관, 감사, 이메일 라우팅 규칙), 가치 높은 최종 사용자 기능(예: 메일 분류, 고급 검색, 스마트 답장)이 포함됩니다. 이 방식은 대다수의 이메일에 가장 안전한 솔루션으로, Google 처리의 안전성과 기능이 저하되는 일 없이 전송 중에 강력한 인증 및 암호화의 이점을 제공합니다.

Gmail 비밀 모드

Gmail 사용자는 Gmail 비밀 모드를 사용해 민감한 정보를 무단 액세스로부터 보호할 수 있습니다. 비밀 모드의 메일을 받는 사람에게는 메시지(첨부파일 포함)를 전달, 복사, 인쇄 또는 다운로드할 수 있는 옵션이 제공되지 않습니다. 사용자는 메일 만료일을 설정하고, 언제든지 메일 액세스 권한을 취소할 수 있으며, 메일 액세스 시 SMS 인증 코드를 요구할 수 있습니다.

Gmail 및 Drive의 데이터 손실 방지(DLP)

데이터 손실 방지(DLP)[8]는 결제 카드 번호, 주민등록번호, 보호 건강 정보와 같은 민감하거나 개인적인 정보가 조직 외부에 유출되는 것을 방지하기 위해 설계된 보호 계층을 추가합니다. 고객은 DLP를 통해 민감한 정보가 기업에 어떻게 흘러들어가는지 감사하거나 경고 또는 차단 작업을 사용 설정하여 사용자의 **기밀 데이터 전송**을 방지할 수 있습니다. 이러한 조치를 실현하기 위해 DLP는 전역 및 리전 ID, 의료 정보, 인증 정보의 감지 기능을 포함하고 있는 사전 정의된 콘텐츠 감지기를 제공합니다. 고객은 기업 니즈를 충족하는 자체적인 커스텀 감지기를 정의할 수도 있습니다. 첨부파일 및 이미지 기반 문서의 경우 DLP는 Google의 광학 문자 인식을 사용하여 감지 범위 및 품질을 높입니다. Gmail DLP 자세히 알아보기 DLP는 사용자가 Google Drive 또는 공유 드라이브의 민감한 콘텐츠를 조직 외부의 사람들과 공유하지 못하도록 방지하는 데 사용될 수도 있습니다. 또한 고객은 IRM 제어 및 향상된 DLP 규칙의 Drive 파일 분류를 자동화할 수 있습니다.

Google Workspace 보안 설정 구성

보안 및 알림 관리

보안 및 개인 정보 보호 설정이 여럿인 조직에서는 **중앙의 한 위치에서 위협을 방지, 감지, 완화할 수 있어야** 합니다. Google Workspace 보안 센터[9]는 고급 보안 정보 및 분석을 제공할 뿐 아니라 도메인에 영향을 미치는

[8] Google Workspace Enterprise 및 G Suite Enterprise for Education 고객에 한해 사용 가능합니다.

[9] Google Workspace Enterprise 에디션 및 G Suite Enterprise for Education에 포함됨

보안 문제를 추가로 가시화하고 제어할 수 있습니다.[10] Google의 보안 분석, 활용 가능한 분석 정보, 권장사항을 모두 통합하여 조직, 데이터, 사용자를 보호하도록 지원합니다. 관리자는 보안 대시보드를 사용하여 다양한 보안 센터 보고서의 개요를 확인할 수 있습니다. 보안 상태 페이지에서는 관리 콘솔 설정을 확인할 수 있어 보안 위험을 더 잘 이해하고 관리할 수 있습니다. 또한 보안 조사 도구를 사용하면 도메인의 보안 및 개인 정보 보호 문제를 식별하고 선별하며 조치를 취할 수 있습니다. 관리자는 이러한 문제를 보다 신속하고 효율적으로 감지하여 완화하는 활동 규칙을 만들어 조사 도구에서 작업을 자동화할 수 있습니다. 예를 들어 Drive 문서가 회사 외부에서 공유되는 경우 특정 관리자에게 이메일 알림을 전송하는 규칙을 설정할 수 있습니다.

Google Workspace 알림 센터는 모든 Google Workspace 고객에게 도메인의 활동에 대해 실시간으로 실행 가능한 알림 및 보안 정보를 제공하여 피싱, 멀웨어, 의심스러운 계정, 의심스러운 기기 활동 등의 최신 보안 위협으로부터 조직을 보호합니다. 또한 Alert Center API를 사용하여 기존 티켓팅 또는 SIEM 플랫폼으로 알림을 보낼 수도 있습니다.

드라이브 공유를 위한 신뢰할 수 있는 도메인

관리자는 조직 내 사용자가 Google Drive 파일과 폴더를 공유하는 방식을 제어할 수 있습니다. 예를 들어 사용자가 조직 외부 사람들과 파일을 공유할 수 있는지 여부, 또는 공유가 신뢰할 수 있는 도메인으로만 한정되는지 여부를 결정할 수 있습니다.[11] 조직 외부에 공유되기 전에 사용자에게 파일의 기밀 여부를 확인하라는 메시지를 표시하기 위해 선택적 알림을 설정할 수 있습니다.

화상 회의 안전

Google Meet는 사용자의 정보 및 개인 정보 보호를 위해 Google에서 사용하는 보안 인프라, 기본 보호 기능, 글로벌 네트워크를 그대로 활용합니다. 웹 회의 및 전화로 참여하기의 계정 도용 방지 수단을 비롯한 각종 기본 악용 방지 조치를 통해 회의를 안전하게 보호합니다.

Chrome, Firefox, Safari, 새 Edge 사용자의 경우 별도의 플러그인이나 소프트웨어를 설치하지 않아도 Meet가 브라우저에서 원활하게 작동됩니다. 이로 인해 Meet가 공격에 노출될 가능성이 제한되고 최종 사용자의 컴퓨터에 보안 패치를 빈번하게 푸시해야 할 필요성이 줄어듭니다. 모바일에서는 Apple App Store 또는 Google Play 스토어에서 Google Meet 앱을 설치하는 것이 좋습니다.

Google은 Meet에 안전하고 편리한 여러 2단계 인증(2SV) 옵션을 지원합니다. 여기에는 하드웨어 및 스마트폰에서 작동하는 보안 키와 Google 메시지가 포함됩니다. Meet 사용자는 Google의 고급 보호 프로그램(APP)에 계정을 등록할 수 있습니다. APP는 고위험 계정을 위해 특별히 설계되었으며 Google의 가장 강력한 보호 기능을 제공하여 피싱 및 계정 도용을 차단합니다. APP에 참여하면 반복적으로 표적 공격을 당하더라도 피싱 피해를 막을 수 있습니다. 자세한 내용은 이 페이지를 참조하세요.

---

[10] 보안 센터에 액세스하려면 Google Workspace Enterprise, G Suite Enterprise for Education, 기업용 Drive 또는 Cloud ID Premium Edition 라이선스를 가지고 있는 관리자여야 합니다. 기업용 Drive 또는 Cloud ID Premium Edition 사용자는 보안 대시보드에 하위 집합의 보안 센터 보고서를 받아보게 됩니다.

[11] 허용된 도메인으로만 공유를 제한하는 등의 특정 기능은 Google Workspace Enterprise, Enterprise for Education, 기업용 Drive, Business, Education, 비영리단체 에디션에서만 사용 가능합니다.

엔드포인트 관리

모바일 및 데스크톱 기기의 정보 보호는 고객에게 중요한 우려사항일 수 있습니다. Google Workspace 고객은 엔드포인트 관리[12]를 사용하여 사용자의 개인 기기 및 조직의 기업 소유 기기에서 기업 데이터를 보호할 수 있습니다. 사용자는 관리를 위해 기기를 등록하여 Google Workspace 서비스에 안전하게 액세스할 수 있고 조직은 기기 암호화와 화면 잠금 또는 비밀번호 적용을 통해 기기와 데이터를 안전하게 보호하는 정책을 설정할 수 있습니다. 그뿐만 아니라 기기 분실 또는 도난 시 회사 계정이 휴대기기에서 원격으로 삭제되며 데스크톱 기기에서 사용자를 원격으로 로그아웃할 수 있습니다. 또한 IT 관리자는 관리 콘솔을 통해 Windows 10 기기를 관리하고 구성할 수 있습니다. 사용자는 기존 Google Workspace 계정 사용자 인증을 사용하여 Windows 10 기기에 로그인하고 싱글 사인온(SSO)을 통해 앱과 서비스에 액세스할 수 있습니다. 고객은 보고서를 통해 정책 규정 준수를 모니터링하고 사용자와 기기에 관한 정보를 얻을 수 있습니다. 여기에서 엔드포인트 관리에 관한 자세한 정보를 확인할 수 있습니다.

보고 분석

Google Workspace 감사 로그

클라우드에 데이터를 저장하는 기업은 **데이터 액세스** 및 계정 활동을 **파악**하길 원합니다. Google Workspace 감사 로그는 보안팀이 Google Workspace에서 감사 추적을 유지하고 관리자 활동, 데이터 액세스, 시스템 이벤트에 관한 상세한 정보를 볼 수 있도록 도와줍니다. Google Workspace 관리자는 관리 콘솔을 사용하여 이러한 로그에 액세스할 수 있고 필요에 따라 로그를 맞춤설정하고 내보낼 수 있습니다.

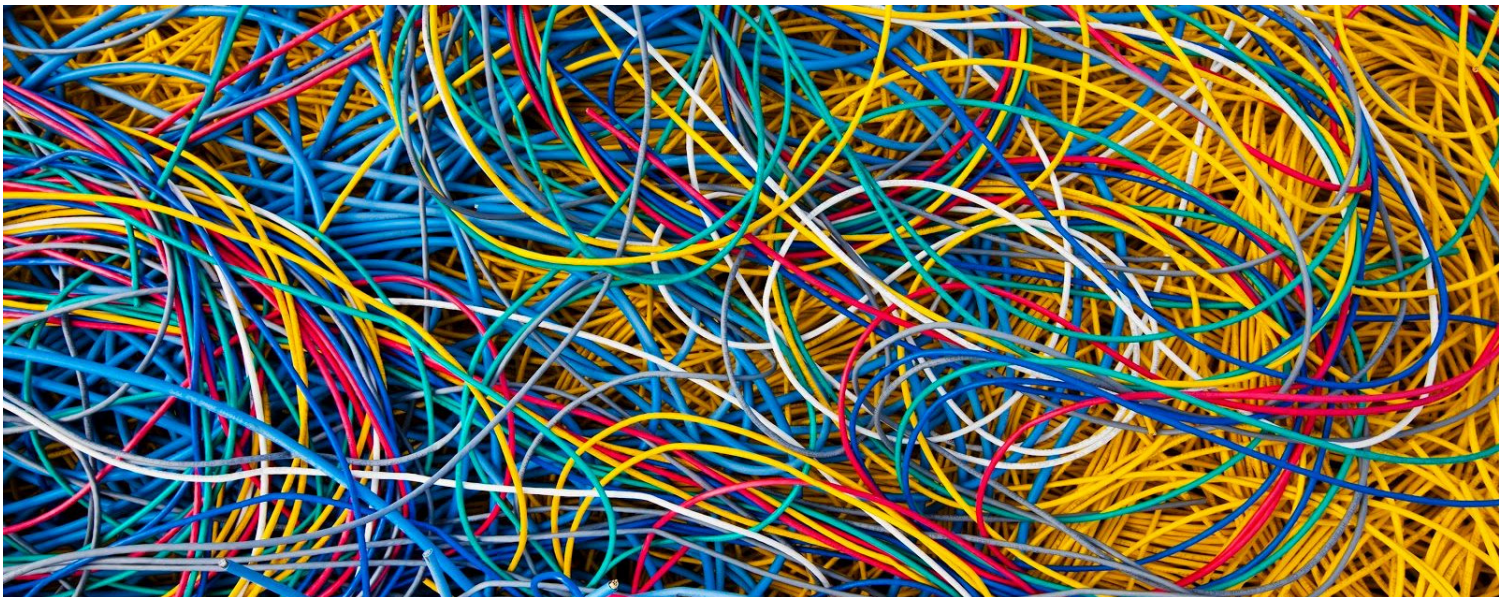
보안 보고서

Google Workspace 관리자는 조직이 데이터 해킹에 노출된 사실에 관한 필수 정보를 제공하는 보안 보고서에 액세스할 수 있습니다. 어떤 사용자가 2단계 인증을 거치지 않거나 외부 앱을 설치하거나 문서를 분별 없이 공유하여 보안을 위협하는지 신속하게 파악할 수 있습니다. 관리자는 잠재적인 보안 위협을 나타내는 의심스러운 로그인 활동이 발생할 때 알림을 받도록 선택할 수도 있습니다.

BigQuery를 사용한 유용한 정보

Google Workspace 관리자는 BigQuery로 감사 로그 및 기타 정보를 내보낼 수 있습니다. Google의 대규모 데이터 분석용 엔터프라이즈 데이터 웨어하우스인 BigQuery를 사용하는 고객은 정교한 고성능 커스텀 쿼리를 사용하여 Google Workspace 로그를 분석하고 타사 도구를 활용하여 심도 있는 분석을 할 수 있습니다.

[12] Google Workspace에서 표준으로 포함됨



데이터 복구

최근 삭제된 사용자 복구

관리자는 삭제일 후 최대 20일 동안 삭제된 사용자 계정을 복구할 수 있습니다. 20일 후에는 관리 콘솔이 사용자 계정을 영구적으로 삭제하므로 Google 기술 지원팀에 연락하더라도 복구할 수 없습니다. 참고로 계정 삭제는 고객 관리자만 수행할 수 있습니다.

사용자의 Drive 또는 Gmail 데이터 복구

사용자의 휴지통에서 데이터를 삭제한 후 최대 25일 동안 사용자의 Drive 또는 Gmail 데이터를 복구할 수 있으며 여기에는 Vault에 설정된 보관 정책이 적용됩니다. 25일 후에는 기술 지원팀에 연락해도 데이터를 복구할 수 없습니다. Google은 고객이 데이터를 삭제한 후 최대 180일 내에 합리적으로 실행이 가능할 때 즉시 시스템에서 고객이 삭제한 모든 데이터를 삭제합니다.

보관 및 디지털 증거 검색

관리자는 조직의 보관 및 디지털 증거 검색 니즈에 대한 지원을 위해 데이터를 보관, 보존, 검색하고 내보내도록 Google Vault를 사용 설정할 수 있습니다. Vault는 무엇보다도 Gmail 메시지, Google Drive 파일, Google Meet의 녹화와 같은 데이터를 지원합니다.

데이터 보존

관리자는 데이터 리전 정책을 사용하여 정책이 적용된 데이터를 특정 지리적 위치(미국 또는 유럽)에 저장할 수 있습니다. 데이터 리전 정책은 다음과 같은 Google Workspace 핵심 서비스의 기본 저장 데이터(백업 포함)에 적용됩니다. 정책이 적용되는 데이터로는 Drive 파일 콘텐츠, Google Chat 메시지 및 첨부파일, Gmail 메일 제목 및 메시지, 기타 핵심 서비스 데이터가 있습니다.

결론

데이터 보호는 Google의 모든 인프라, 제품, 직원의 업무 운영을 위한 기본적인 설계 고려사항입니다. Google은 극소수의 퍼블릭 클라우드 공급업체 또는 민간 기업 IT팀만 제공할 수 있는 보호 수준을 제공할 수 있습니다.

Google은 업계 권장사항을 기반으로 가장 엄격한 개인 정보 보호 및 보안 기준을 충족하도록 Google Workspace를 설계했습니다. Google은 데이터 소유권, 데이터 사용, 보안, 투명성, 책임과 관련한 이행 의지를 계약서에 적시해 두었습니다. 이를 통해 고객은 고객 데이터에 대한 통제권을 유지하고 광고 목적이나 Google Cloud 서비스를 제공하기 위한 목적 이외의 목적으로 데이터를 사용하지 않을 것임에 대한 보증을 포함하여 데이터의 처리 방식에 대한 통제권을 유지할 수 있습니다. 또한 Google은 규정 준수 및 보고 요구사항을 충족하기 위해 필요한 도구를 제공합니다.

아울러 데이터 보호는 Google Workspace의 핵심이므로 Google은 타사가 해낼 수 없는 규모로 보안, 리소스, 전문성에 광범위하게 투자할 수 있습니다. Google의 투자 덕분에 고객은 자체 비즈니스와 혁신에 초점을 맞출 여유가 생깁니다. 또한 Google은 보안 연구 커뮤니티와 작업 및 협업을 수행하여 신속하게 취약성을 해결하거나 완전히 방지할 수 있습니다.

이러한 이유에서 전 세계 600만 개가 넘는 조직이 가장 귀중한 자산인 정보를 Google에 믿고 맡기고 있습니다. Google은 고객에게 안전하고 투명한 방식으로 서비스 혜택을 제공하기 위해 Google Workspace에 대한 투자를 이어나갈 것입니다.