

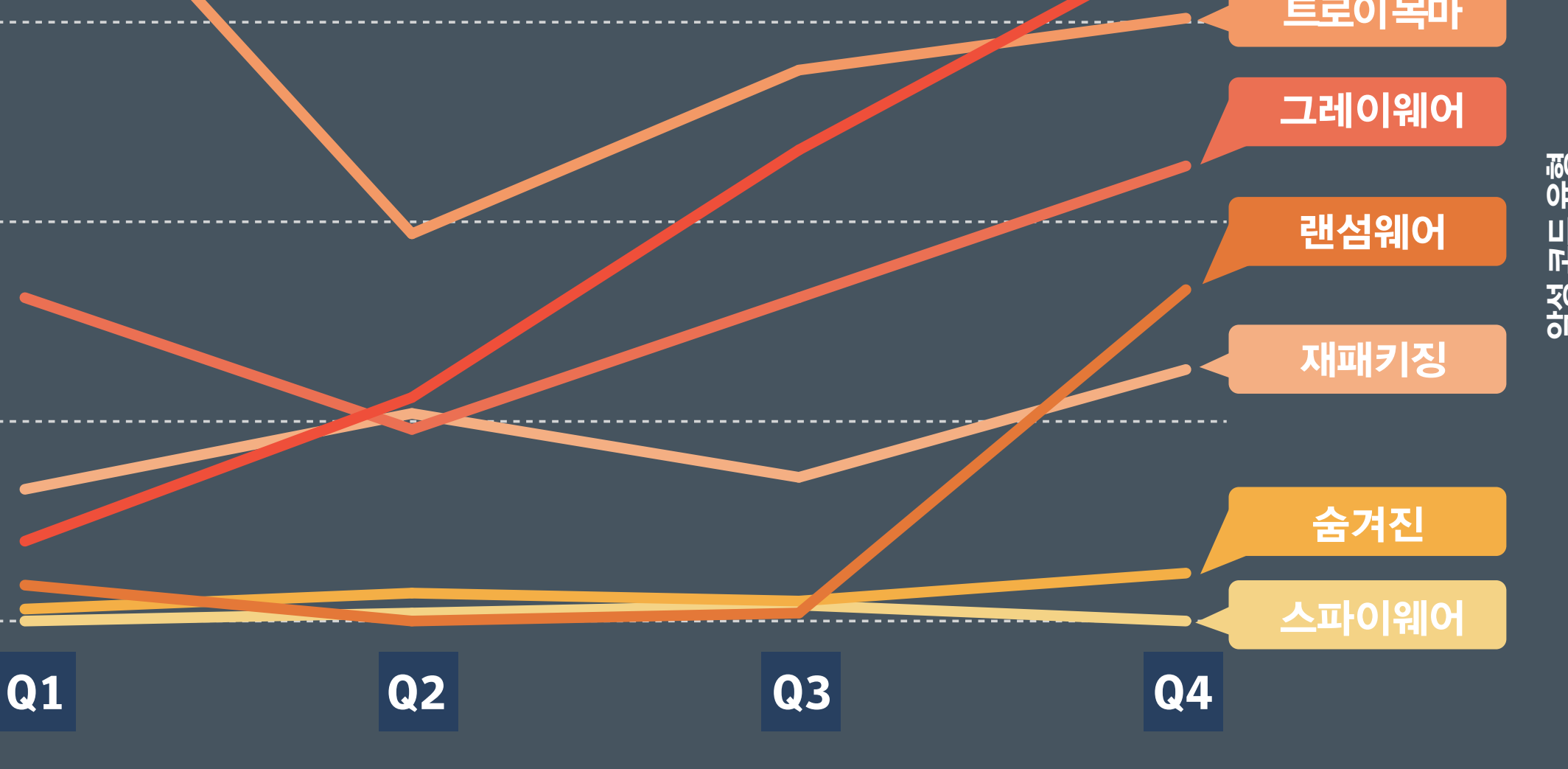
모바일 보안 위협 인텔리전스 리포트

2017년: 결산

이번 리포트는 SEP Mobile 리서치 팀이 2017년 1월부터 12월까지 전 세계에 구축된 모바일 보안 에이전트 및 수백만 건의 월간 보안 테스트로부터 수집한 전 세계 보안 위협 인텔리전스 데이터를 검토합니다.

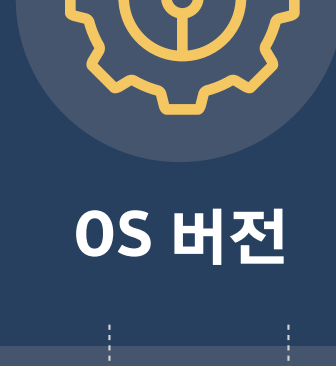
모바일 악성 코드 변종이 2017년에 전년 대비 54% 증가

했습니다. 이 차트는 다양한 모바일 악성 코드 유형의 지난 1년간 발생 빈도 추이를 보여줍니다. 세 번째로 높은 카테고리는 그레이웨어로, 악성 코드가 아닐 수도 있지만 중요 데이터에 대해 불필요한 리스크를 야기합니다. 그레이웨어, 즉 불필요한 애플리케이션이 모든 모바일 보안 솔루션에서 탐지되는 것은 아닙니다.

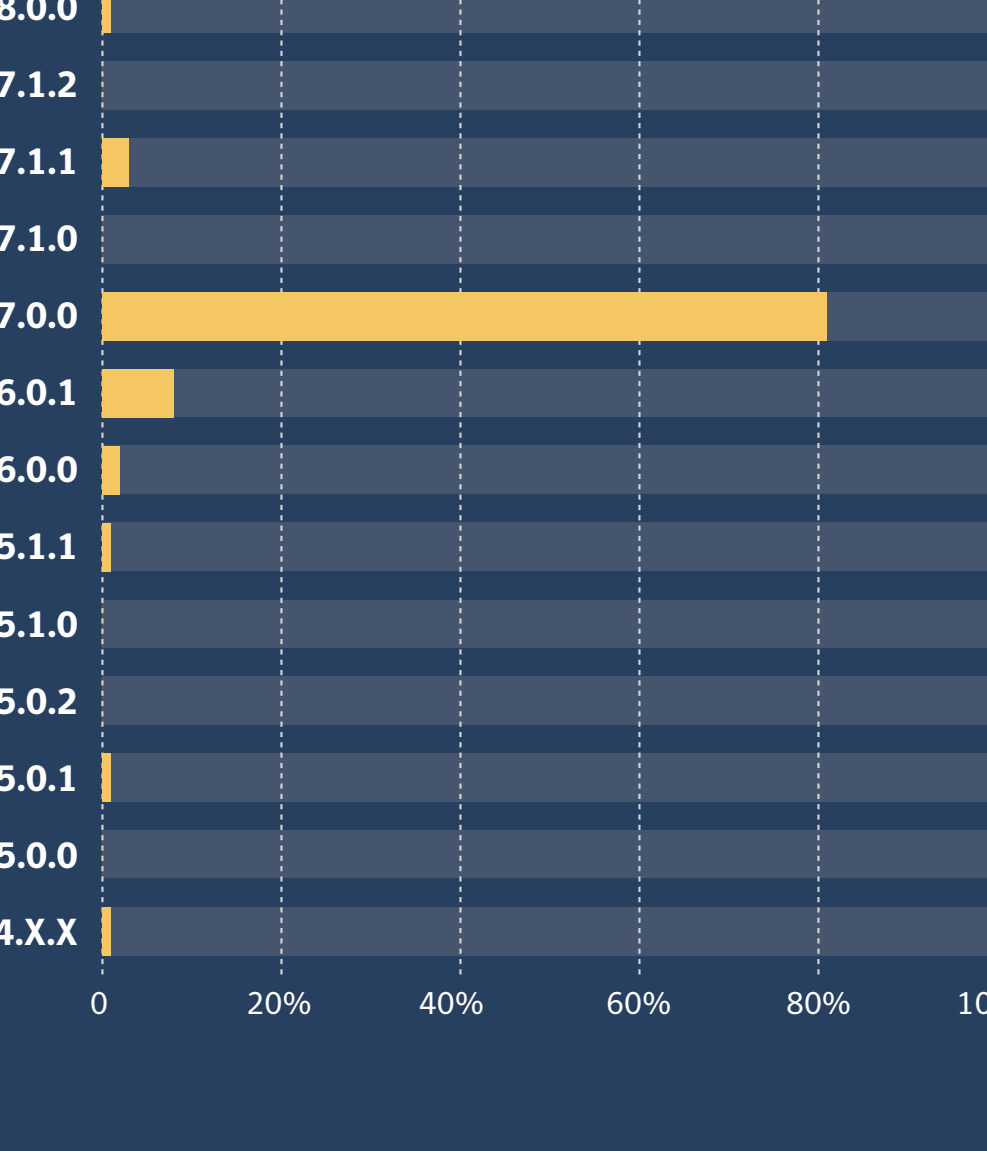


41%의 Android 디바이스가 2개월 이상 된 보안 패치를 실행하고 있습니다.

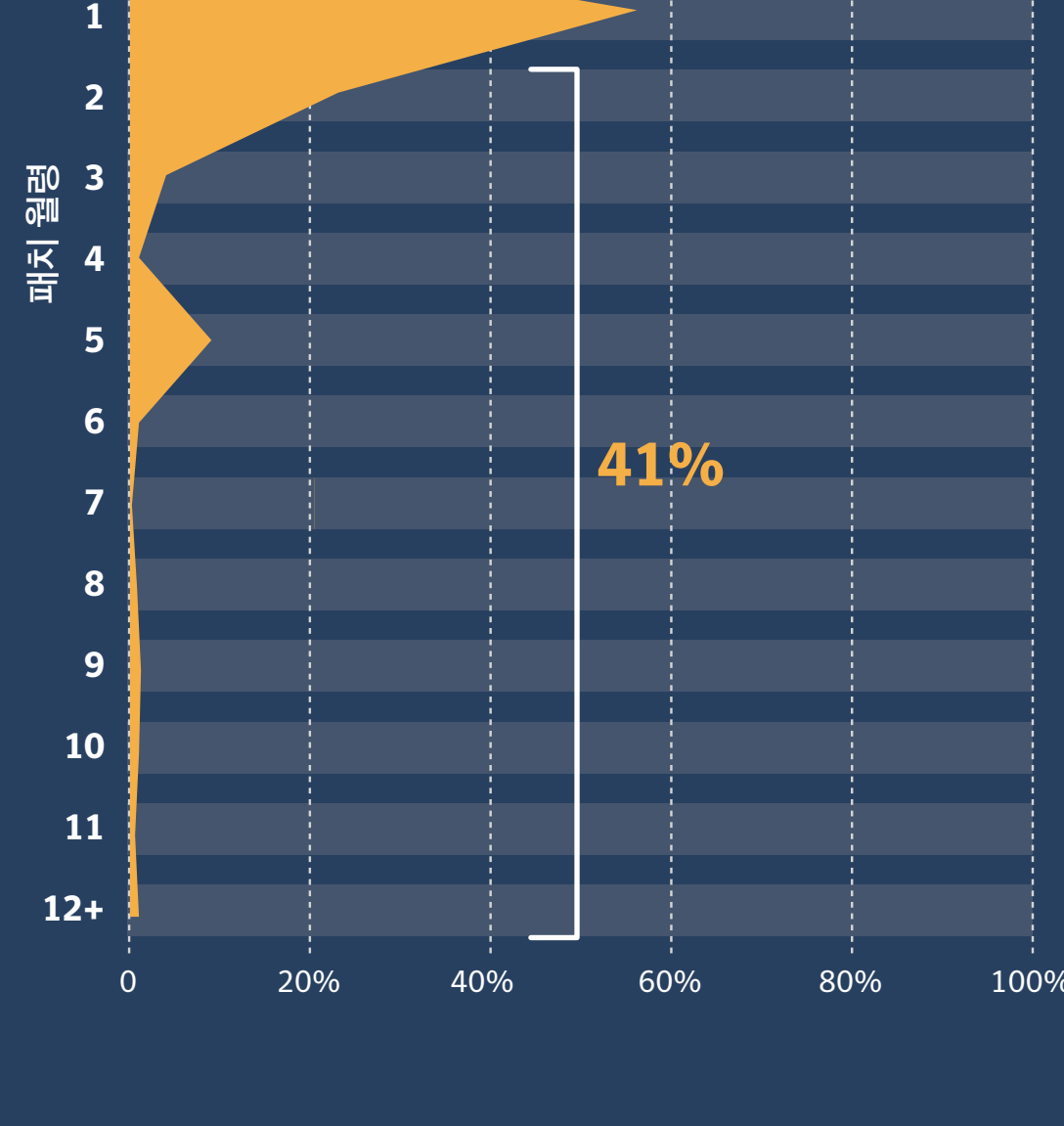
Android 커뮤니티는 특히 활성 상태의 디바이스에서 최신 운영 체제를 실행하지 않는 경우가 매우 많았습니다(최신 주요 버전을 사용하는 경우는 3%에 불과). 그러나 Android가 여러 운영 체제를 지원하는 월간 보안 패치를 발표하기 시작하면서 활성 상태의 취약점이 대폭 줄어들었습니다.



OS 버전



보안 패치 월령

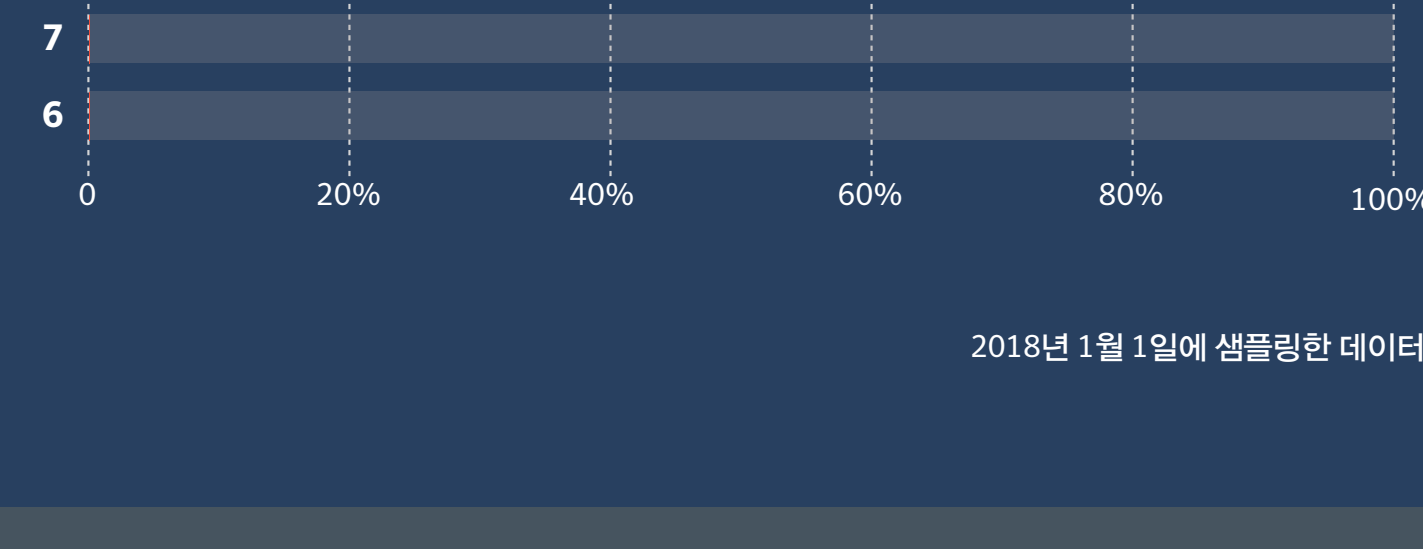


20%의 iOS 디바이스가 오래된 버전을 실행 중입니다.

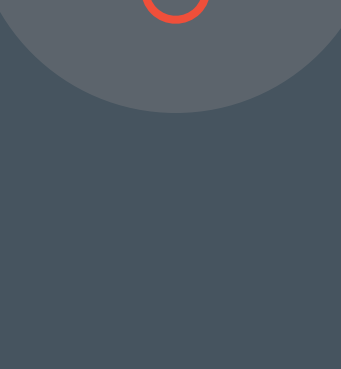
Android와 달리 Apple은 보안 업데이트의 배포 체인 전체를 관리하여 더 신속하게 패치를 적용할 수 있으므로 최신 주요 버전이 아닌 iOS 디바이스는 20%에 불과합니다.



iOS 버전

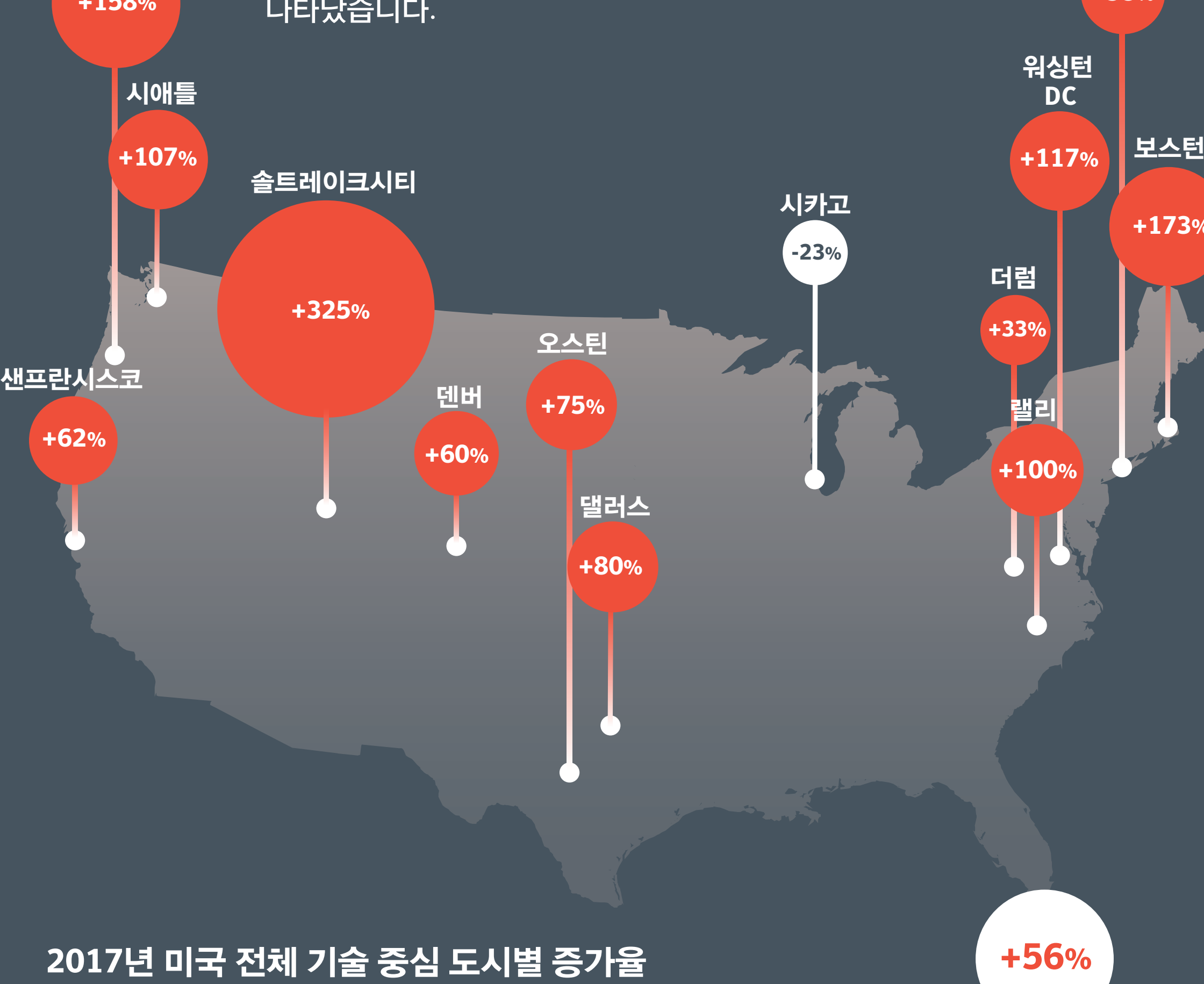


2018년 1월 1일에 샘플링한 데이터

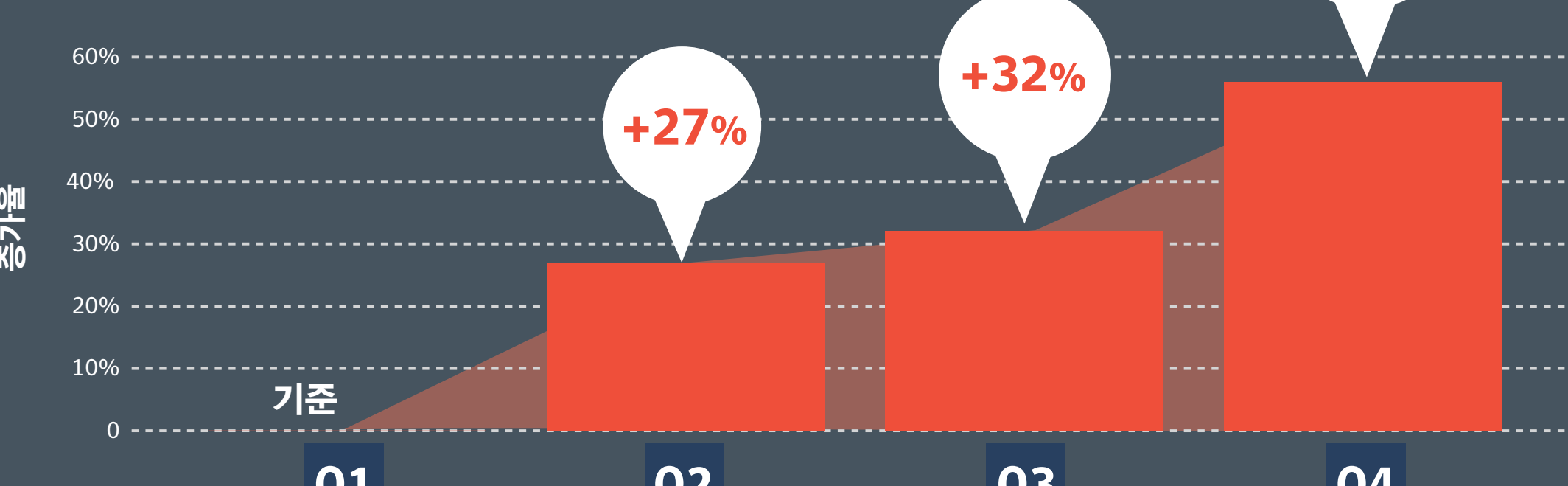


위험한 Wi-Fi 네트워크의 수가 2017년에 56% 증가했습니다.

위험한 Wi-Fi란 요청과 달리 완전한 엔드투엔드 보안 전송을 제공하지 않는 Wi-Fi를 의미합니다. 기업에서 사용자 이동성이 매우 중요한 역할을 담당하는 미국의 대표적인 기술 중심 도시들을 살펴보면 위험한 것으로 분류된 네트워크 수가 증가하는 추세입니다. 시카고는 2017년 말을 기준으로 위험한 Wi-Fi 네트워크가 줄었지만 솔트레이크시티는 4배 이상 늘었고 MITM(Man-In-The-Middle) 공격, 가짜 네트워크, 잘못 구성되어 통신을 제대로 보호하지 않는 액세스 포인트 등 모바일 네트워크 침해 사고도 가장 큰 폭으로 증가한 것으로 나타났습니다.

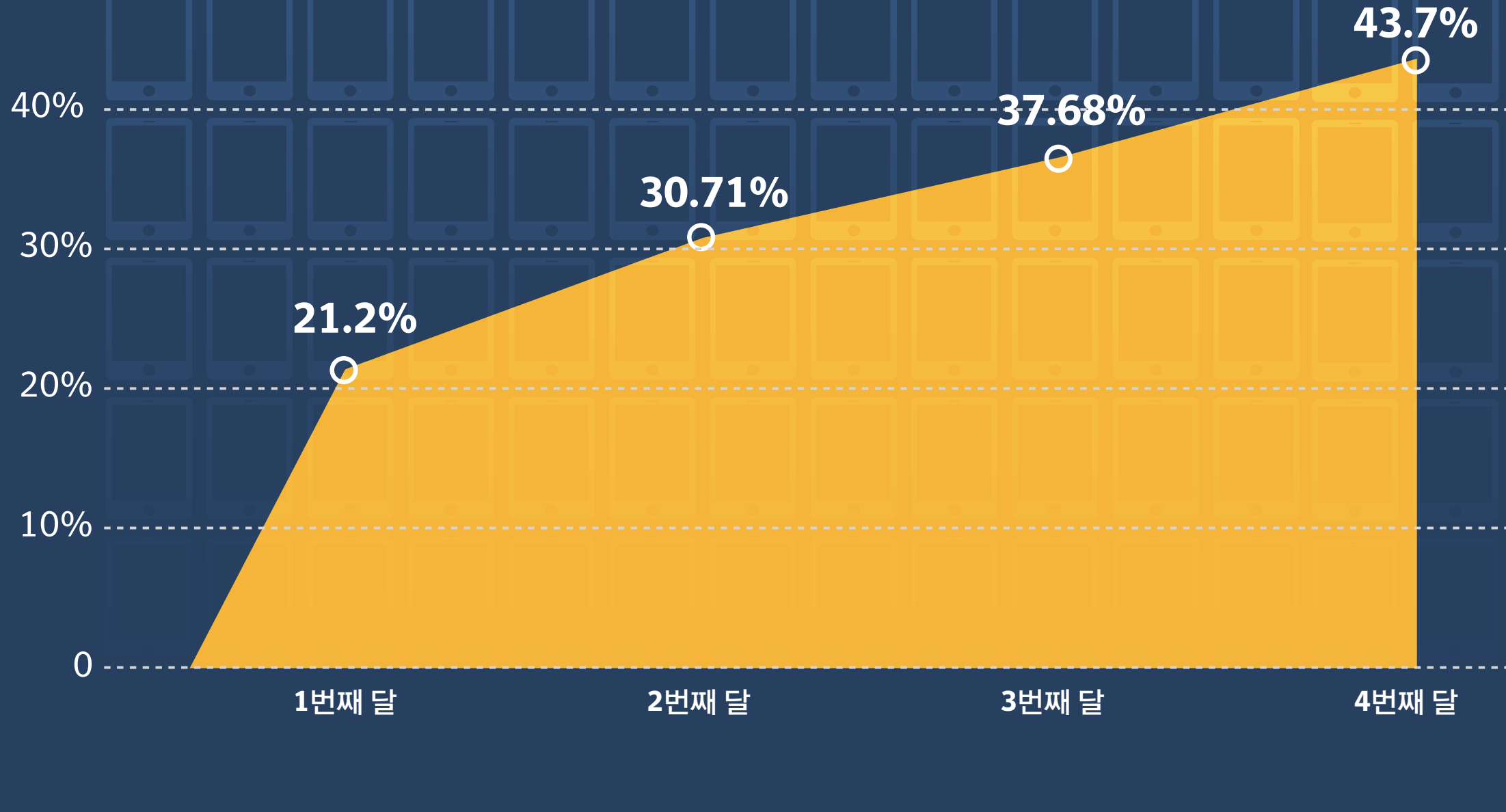


2017년 미국 전체 기술 중심 도시별 증가율



기업에서 모바일 디바이스의 40% 이상이 4개월마다 네트워크 보안 위협에 노출됩니다.

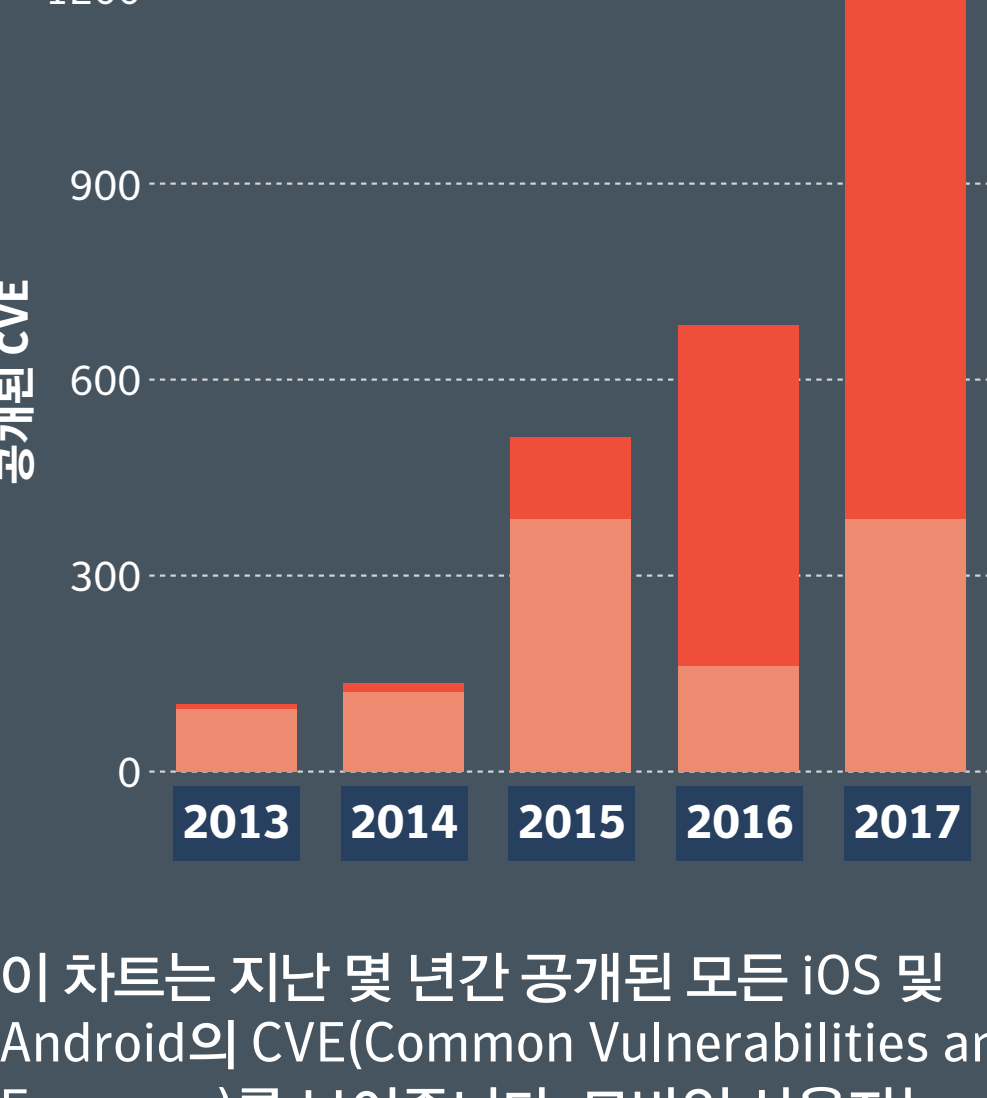
네트워크 보안 위협의 목적이 얼마나 악의적인지에 관계없이 개인과 기업 모두 위험한 네트워크를 피하거나 그러한 위험으로부터 스스로를 지키는 것이 현명합니다.



4개 분기 평균 데이터.

2016년부터 2017년까지 iOS 및 Android 취약점이

80% 증가했습니다.

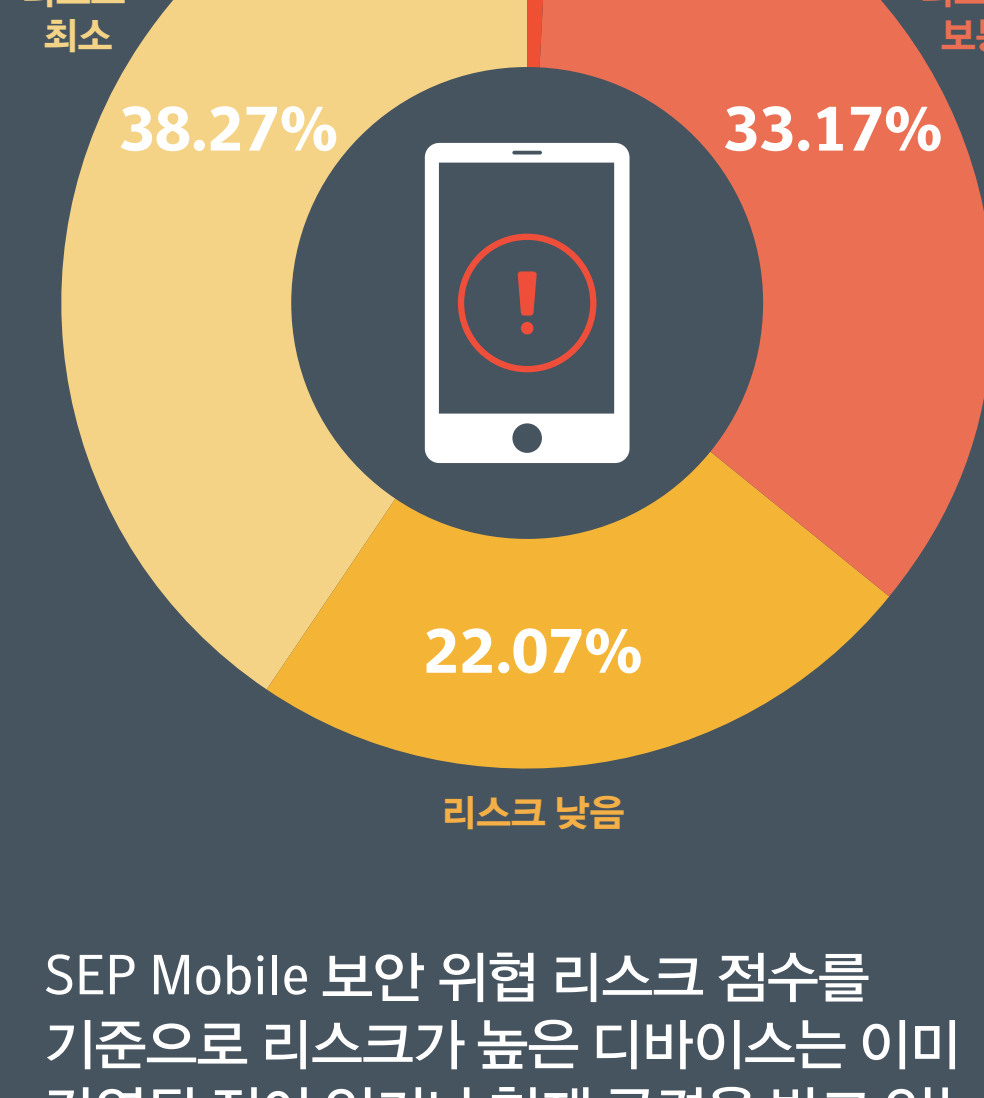


이 차트는 지난 몇 년간 공개된 모든 iOS 및 Android의 CVE(Common Vulnerabilities and Exposure)를 보여줍니다. 모바일 사용자는 최대한 신속하게 최신 보안 패치로 업데이트하여 취약점 윈도우, 즉 해커가 이 알려진 취약점을 이용할 수 있는 기간을 줄이는 것이 중요합니다.

출처: The MITRE Corporation, cve.mitre.org

전체 모바일 디바이스의

34%가 리스크 보통 ~ 높음으로 평가되었습니다.



SEP Mobile 보안 위험 리스크 점수를 기준으로 리스크가 높은 디바이스는 이미 감염된 적이 있거나 현재 공격을 받고 있는 디바이스입니다. 리스크 점수는 디바이스가 노출된 최신 보안 위협, 디바이스 취약점, 구성, 사용자 행위를 반영하여 산정됩니다.

모바일 보안 위협으로부터 귀사를 보호하는 방법에 대해 더 자세히 알고 싶으십니까?

모바일 보안 마스터 무료 과정을 이용하십시오.
9가지 동영상 모듈로 구성되어 있으며 2시간 내에 마칠 수 있습니다.

[과정 수강하기](#)

모바일 보안 위협 인텔리전스 리포트 소개

시만텍 모바일 보안 위협 인텔리전스 리포트는 시만텍이 시만텍 제품 및 서비스를 제공하면서 수집한 전 세계의 보안 위협 인텔리전스 데이터를 검토합니다. 이번 리포트는 2017년 1월부터 12월까지 실시한 수백만 건의 월간 보안 테스트를 기반으로 하여 엔터프라이즈 환경에서 보안 관리 대상 디바이스와 관리되지 않는 디바이스를 모두 포함합니다. 여기에는 SEP Mobile에서만 제공하는 모바일 보안 위협 리스크 점수도 포함되며, 이 점수는 모바일 디바이스에 대한 보안 위협 노출 리스크를 측정하는 신뢰 지수 역할을 수행합니다. SEP Mobile은 기업을 위해 수백만 개의 데이터 포인트를 집약하여 리스크 점수를 산정하며, IT 부서는 이를 바탕으로 전반적인 시스템의 상태 및 디바이스별 리스크를 신속하게 파악할 수 있습니다. SEP Mobile은 매년 전 세계에서 1백만여 개의 애플리케이션 및 2백만 개 이상의 고유 네트워크를 분석합니다.

Copyright © 2018 Symantec Corporation