Google Workspace

보안, 임계점에 도달하다

점진적인 개선으로는 더 이상 효과가 없는 이유

2024년 10월

Google의 환영 인사

업무 방식과 업무 공간의 변화로 비즈니스 환경이 지속적으로 재편됨에 따라 전 세계의 조직은 급격히 증가하는 보안 위협에 직면하고 있습니다. 최근 Mandiant M-Trends 보고서에 따르면 2023년에만 보더라도 대규모 정부 및 영리 기업을 겨냥한 국가 차원의 후원을 받는 스파이 활동과 상업적 목적의 랜섬웨어 공격이 증가했으며 통신부터 엔터테인먼트 업종에 이르기까지 모든 분야에서 계속해서 데이터 유출 사태가 이어지고 있습니다.

조직이 새로운 보안 위협 환경에 효과적으로 대응할 수 있도록 지원하기 위해 Google은 최근 Hypothesis Group과 협력하여 글로벌 보안 연구를 의뢰했습니다. 이 연구에서는 중견기업 및 대기업의 의사 결정권자 2,000여 명과 인터뷰를 진행해 보안 접근 방식, 현재 겪고 있는 변화, 향후 계획에 대해 논의했습니다.

연구를 수행하는 과정에서 Google은 이미 도래한 미래의 업무 환경이 새로운 보안 위험의 시대를 초래한다는 점을 확인했습니다. 하지만 많은 조직이 새로운 시대에 적응하기보다는 기존 전략과 도구에 더 투자하고 있는 것으로 나타났습니다. 그리고 그 결과 비즈니스 운영을 방해하고 고객 데이터에 영향을 미치며 기업 평판을 손상시키고 비용 부담이 큰 보안 사고가 증가하고 있습니다. 현재의 보안 관행으로는 충분하지 않습니다. 이제는 근본적으로 향상된 새로운 접근 방식이 필요한 때입니다.

비즈니스에는 더 많은 보안 제품이 필요한 것이 아니라 더 안전한 제품이 필요합니다. Google은 보안 사고와 데이터 유출이 일상적인 일이 아닌 예외적인 사례가 되어야 한다고 생각합니다. 또한 설계부터 보안이 내재화된 솔루션을 통해 조직이 자신 있게 선제적으로 공격을 차단할 수 있도록 지원하고자 합니다.

이번 연구가 귀사의 보안 니즈에 대해 나눌 지속적인 대화의 첫걸음이 되기를 바라며, Google Workspace가 보다 안전한 업무 환경을 조성하기 위한 귀사의 여정에서 전략적 파트너가 될 수 있기를 기대합니다.

앤디

앤디 웬

Google Workspace 보안 부문
제품 관리 수석 이사

목차

소개

업무 환경은 끊임없이 변화하고 있습니다. 수백만 명의 직원에게 하이브리드 업무가 표준으로 자리 잡고, AI가 더욱 발전함에 따라 이를 악용하려는 보안 위협 역시 점점 더 정교해지고 규모 또한 커지고 있습니다. 조직은 이러한 새롭고 규모가 증가하는 위협을 인식하고 있지만 보안 환경을 진정으로 안전하게 만들기 위해 과감한 결정을 내리는 데에는 주저하는 경우가 많습니다.

이 백서에서는 오늘날 비즈니스 환경의 핵심적인 긴장 관계를 상세하게 살펴봅니다. 일부 리더들은 자신의 전략에 자신감을 보이고 있지만, 보안 사고의 지속성과 심각성은 인식과 현실 사이에 존재하는 간극을 드러냅니다. 기존의 방식에 투자하기보다 변화의 필요성을 받아들이는 것이 이러한 간극을 메우고 보안 문제에 보다 효과적으로 대응할 수 있는 길을 열어줄 것입니다.

현 상황을 더 잘 이해하고 조직의 보안 태세를 강화하기 위해 무엇을 할 수 있는지 알아보기 위해 Google Workspace는 Hypothesis Group(인사이트, 디자인, 전략 전문 기업)과 협력하여 다각적인 연구를 진행했습니다. 이 이니셔티브에는 다음이 포함됩니다.

- 미국, 영국, 인도, 브라질의 중견기업(직원 수 300~999명) 및 대기업(직원 수 1,000명 이상) 조직에 속한 IT, 비즈니스, 보안 의사 결정권자 2,000여 명을 대상으로 2024년 7월 22일부터 8월 8일까지 실시한 정량적 설문조사 결과
- 2024년 8월 22일부터 26일까지 실시한 미국 의사 결정권자 6명과 정성적 인터뷰
- 다음의 업계 전문가와의 대화를 통한 현재 동향과 미래 보안 현황에 대한 논의

존 맥컴버
전 NIST(미국 국립표준기술연구소) 공동 의장 및 Gartner 이사, 현 보안 칼럼니스트

조슈아 스카르피노 박사
TrustEngine 정보 보안 부문 부사장, Assessed Intelligence CEO

레이첼 토백
SocialProof Security CEO, Women in Security and Privacy(보안 및 개인 정보 보호 업계의 여성) 이사회 의장, CISA(사이버 보안 및 인프라 보안국) 기술 자문 위원회 자원봉사자

주요 인사이트

보안은 지금 임계점에 도달하고 있습니다. 현재의 접근 방식이 지속 불가능하고 비용이 많이 드는 것으로 입증됨에 따라, 조직이 진화하는 위협에 대응하고 앞서 나가기 위해서는 빠르게 변화를 수용해야만 합니다.

빠르게 증가하는 위협 환경은 보안에 대한 새로운 접근 방식을 요구하지만, 혁신적인 변화에 투자하는 기업은 거의 없습니다.

1. **기존 방식은 더 이상 지속될 수 없습니다.**
   조직들은 자사의 보안 태세에 대한 자신감을 보이지만 위험한 행동은 여전히 만연하고 보안 리더들의 우려도 점점 늘고 있습니다.

2. **조직은 보안 강화의 필요성을 인식하고 있지만 기존 방식만으로는 한계가 있습니다.**
   보안을 강화하려는 노력의 일환으로, 리더들은 보안 조치를 추가하는 방식(도구 추가, 투자 확대, 보험료 증대)으로 변화를 시도하고 있습니다. 그럼에도 불구하고 보안 사고는 여전히 빈번하게 일어나고 있으며 그로 인한 비용 손실이 발생하고 있습니다.

3. **미래에 대비하기 위해서는 변화가 필요합니다.**
   리더들은 보안 접근 방식을 간소화하고 AI를 활용하여 조직을 보호하려는 명확한 의지를 보이고 있습니다. 근본적인 비효율성을 해결한 조직이 임시방편적인 해결책에 의존하는 조직보다 더 나은 성과를 거두고 있습니다.

보안 문제에 대응하는 조직의 접근 방식은 조직 규모와 지역에 따라 다르지만, 모든 조직은 변화의 필요성을 인식하고 있습니다.

4. **중견기업(300~999명) 부문은 혁신의 기로에 서 있습니다.**
   기존 기술과 조직의 복잡성에 대한 부담으로 인해 리더들은 미래에 대한 불안감이 큽니다. 그래도 대부분의 리더는 보안 접근 방식을 적극적으로 재고하고 있으며, 변화에 대해 열린 자세를 보이고 있습니다.

5. **전 세계 각 지역은 각기 다른 도전 과제에 직면해 있으며, 이에 따라 보안 문제를 해결하기 위한 개별적인 접근 방식이 필요합니다.**
   전 세계의 리더들은 업무 환경이 지속적으로 변화할 것이라는 점을 인식하고 있습니다. 하지만 모든 국가가 성공적이거나 지속 가능한 보안 전략을 갖추고 있는 것은 아니기 때문에 광범위한 재평가가 진행되고 있습니다.

1

기존 방식은 더 이상 지속될 수 없습니다

조직은 보안과 업무 방식에 대해 자신감을 보이지만 실제 행동에는 여전히 많은 취약점이 드러나며, 이로 인해 보안 의사 결정권자들의 우려가 계속되고 있습니다.

조직은 보안에 대해 많은 자신감을 느끼고 있지만 업무 방식의 변화는 보안을 위협합니다

대부분의 조직은 보안에 문제가 없다고 생각합니다. 적어도 이론적으로는 그렇습니다. IT, 비즈니스, 보안 리더를 포함한 의사 결정권자의 **96%**는 데이터, 애플리케이션, 기기, 생성형 AI와 같은 신기술에 대한 조직의 보안 관리 능력에 대해 높은 자신감을 표명합니다. 하지만 이러한 자신감은 실제 업무 방식의 변화와는 괴리가 있으며, 업무 방식의 변화는 하이브리드 업무의 확대부터 생성형 AI와 같은 새롭고 다양한 도구의 도입에 이르기까지 다양한 형태로 나타나고 있습니다.

74%

업무 방식이 크게 변화했다고 응답한 비율

> *"우리는 변화의 중심에 서 있습니다. 수많은 도구를 사용할 수 있는 시대입니다. 하지만 사용 정책은 물론 새로운 도구를 다루기 위한 계획도 없다고 느껴지기에 걱정이 많습니다."*
>
> - 제약 분야 연구 책임자

위험한 도구와 위험한 행동이 만연합니다

대부분의 의사 결정권자는 조직을 위험에 노출시키는 여러 관행을 다음과 같이 지적합니다.

- 응답자의 **56%**만이 IT 정책을 준수한다고 답변
- 조직 내에서 사용되는 도구의 **19%**는 라이선스가 없는 도구(즉, 조직에서 검토하거나 승인을 받지 않은 도구)
- 절반에 가까운 응답자(**44%**)가 라이선스 없는 도구가 '완벽히 안전'하다고 생각
- 응답자 3분의 2(**63%**)가 라이선스 없는 생성형 AI 도구가 매주 사용된다고 보고
- 의사 결정권자의 절반(**48%**)이 라이선스 없는 생성형 AI 도구를 신뢰

조직의 말과 행동 사이의 괴리는 현재 보안 태세에 내재된 위험을 잘 보여줍니다. 게다가 흔히 사용되며 보안이 취약한 비공식 IT 서비스를 사용하면 보안 사고는 물론 규정 준수 위반의 위험도 커집니다.

> *"새로운 기술이 어떤 위험을 가져올지를 조직에서 언제나 알 수 있는 것은 아닙니다. 때문에 보안 리더들은 위험과 계속 술래잡기를 해야 하는 어려움에 처해 있습니다."*

— 조슈아 스카르피노 박사
Assessed.Intelligence CEO

보안 리더들 사이에서 불안감이 고조되고 있습니다

보안 의사 결정권자(SDM)가 이러한 위험을 모르는 것은 아닙니다.

63%

조직의 기술 환경이 과거보다 덜 안전하다고 여기는 비율

4개 중 1개의 도구는 위험하다고 간주

"조직의 보안 환경이 덜 안전하다는 생각은 통제와 지식이 부족하다는 느낌에서 비롯된 것으로 보입니다. 우리가 사용하고 있는 모든 도구가 어디에서, 어떻게 사용되고 있는지, 또 어떤 방식으로 보안에 위협이 될 수 있는지 파악하는 것은 우리 모두의 과제입니다."

— 존 맥컴버

전 NIST 공동 의장 및 Gartner 이사, 현 보안 칼럼니스트

이러한 위험한 행동으로 인해 보안 의사 결정권자의 **93%**가 보안 사고에 대해 걱정하는 등 불안한 분위기가 조성되고 있습니다. 이러한 불안감의 원인은 분명합니다. 보안 의사 결정권자들은 취약성과 외부 공격(예: 생성형 AI 공격이나 미래에 발생할 수 있는 데이터 유출)에 가장 큰 우려를 표명하고 있지만 의도적이거나 비의도적인 사용자 부주의에 대해서도 걱정하고 있습니다.

> *"의사 결정권자들은 걱정으로 밤잠을 설치고 있다고 말합니다. 기술 도구는 완벽하지 않으며 사람의 감독이 많이 필요하기 때문에 의사 결정권자들이 큰 스트레스를 받고 있습니다."*

— 레이첼 토백

SocialProof Security CEO

93%

보안 사고에 대해 우려를 표명한 보안 의사 결정권자의 비율

주요 공격/유출 우려사항

생성형 AI 공격	**31%**
데이터 유출	**30%**
사이버 갈취	**26%**

최종 사용자와 관련된 주요 우려사항

승인되지 않은 액세스	**24%**
직원 과실	**20%**
인증 정보 보안 침해	**17%**

2

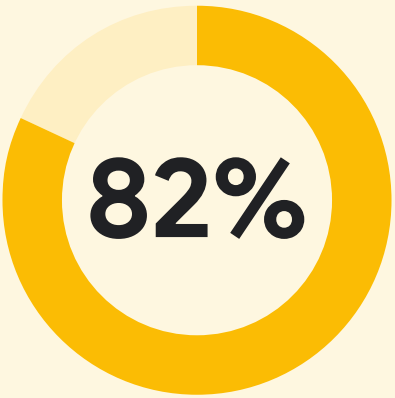
조직은 보안 강화의 필요성을 인식하고 있지만 기존 방식만으로는 한계가 있습니다

보안 강화 조치의 필요성이 그 어느 때보다 절실해졌습니다. 보안 의사 결정권자들은 현재의 전략이 한계에 다다랐음을 잘 알고 있으며 광범위한 개선이 필요하다는 것을 인식하고 있습니다. 그러나 많은 조직에서 취하는 접근 방식은 충분하지 못하다고 입증되고 있으며 자주 역효과를 낳고 있습니다.

보안 강화 조치에 대한 명확한 요구

82%의 보안 의사 결정권자는 보안 조치를 개선해야 한다고 응답했습니다. **절반이 넘는** 응답자는 복잡한 현대의 업무 환경이 보안을 유지하는 데 걸림돌이 된다고 답했습니다. 또한 **59%**는 구식 기술에 의존하는 탓에 미래 보안 니즈 충족을 위한 준비가 부족하다고 시인합니다.

> *"저희는 수년 동안 다양한 보안 솔루션을 갖춰 왔지만 일부 솔루션은 최소한 교체하거나 재평가해야 할 정도로 오래된 도구입니다."*
>
> - IT, 미디어 및 엔터테인먼트 부문 부사장



조직의 보안 조치를 개선해야 한다고 응답한 보안 의사 결정권자의 비율

점진적인 변화만으로는 충분하지 않습니다

보안 의사 결정권자의 절반은 지난 2년 동안 사이버 보안 전략에 중요한 변화가 있었다고 답했지만, 그 변화는 혁신적이라기보다는 점진적인 경우가 많았습니다. 실제로 대부분의 조직은 단순히 기존 방식을 그대로 고수하고 있는 것으로 보입니다.

지난 2년간의 주요 보안 변경사항

사이버 보안 보험 증대	**37%**
사이버 보안에 대한 투자 확대	**35%**
라이선스 업그레이드	**34%**
신규 사이버 보안 공급업체 추가	**31%**

이러한 조정은 어느 정도 도움이 될 수 있지만 이는 전략의 근본적인 변화라기보다는 기존 관행을 개선하는 것에 가깝습니다.

> *"사람들은 같은 수준의 여러 보호 조치에 투자합니다. 제 동료와 고객은 '많은 돈을 투자했지만 실제로 문제를 해결하는 데 도움이 되지 않았다'고 이야기합니다. 큰 비용이 드는 플랫폼에 투자하려고 하지만 실상은 조직에 비밀번호 관리자조차 없습니다. 이는 마치 방탄 유리창에 투자해 놓고 문은 활짝 열어 놓은 것과 같죠."*
>
> **— 레이첼 토백**
> SocialProof Security CEO

62%
새로운 기능이 필요할 때 도구를 확장한다고 답한 보안 의사 결정권자의 비율(나머지는 기존 도구를 교체한다고 응답)

10
기업 조직에서 평균적으로 사용하는 보안 도구의 개수

61%
2년 전보다 더 많은 보안 도구를 사용하고 있는 조직의 비율

27%
중복되는 보안 도구의 비율

과잉이 초래하는 함정으로 인해 보다 일관성 있는 전략이 필요합니다

전체 조직의 3분의 2 이상이 보안을 강화하기 위해 그 어느 때보다 많은 시간과 비용을 투자하고 있지만, 여전히 큰 비용이 드는 사고가 자주 발생하고 있습니다.

81%
1년에 한 건 이상의 사고를 경험하는 조직의 비율

8 **연간 보고된 사고 건수 평균**

미화 488만 달러
2024년 유출로 인한 전 세계 평균총비용[1]

하지만 보안 도구 수가 적은 조직이 더 나은 성과를 보이고 있습니다. 10개 이상의 보안 도구를 사용하는 조직의 경우 보안 사고 발생 빈도가 더 높지만, 비용도 더 많이 소요된다고 응답했습니다.

10개 이상의 보안 도구를 사용하는 조직	10개 미만의 보안 도구를 사용하는 조직
연간 보안 사고 발생 건수	
14	6
연간 보안 사고에 25만 달러 이상을 지출한 조직	
34%	19%

"보안의 모든 부분에 대해 각기 다른 공급업체를 이용하는 것은 관리가 매우 어렵고 비용 효율적이지 않습니다. 그 수를 줄이고 통합해야 지속가능성을 확보할 수 있습니다."

- IT, 미디어 및 엔터테인먼트 부문 부사장

1. IBM – Cost of a Data Breach Report 2024(2024년 데이터 유출 비용 보고서)

3

미래에 대비하려면 변화가 필요합니다

Google의 연구에 따르면 보안 의사 결정권자는 새로운 방식으로 보안에 접근할 준비가 되어 있으며, 새로운 전략과 기술을 적극적으로 도입하는 조직이 더 앞서가고 있습니다.

변화에 대한 열망

현재의 환경으로 인해 조직들은 보안 전략에 대해 다시 생각하고 있습니다.

78%

현재의 사이버 보안 환경을 고려하여 조직의 보안 접근 방식을 재고 중인 조직의 비율

73%

비용과 관계없이 새로운 보안 접근 방식을 수용할 준비가 된 조직의 비율

의사 결정권자들은 점점 더 간소화된 보안 솔루션에 주목하고 있으며, 그 중 **65%**는 통합 보안 시스템에 관심을 보이고 있습니다. 이들은 단일 인터페이스 내에서 다양한 데이터 소스를 통합하는 플랫폼이 프로세스 간소화, 운영 개선, 여러 도구 관리 부담 해소, 시간 절약 등 실질적인 이점을 제공할 것이라는 데 동의합니다.

보안 의사 결정권자의 **59%**가 진화하는 위협에 대응하기 위한 핵심 도구로 생성형 AI를 점점 더 주목하고 있습니다

> *"AI가 보안에 미치는 가장 큰 영향은 이벤트에 대응하고, 현재 보유한 도구를 활용하며, 이를 적절하게 조정하여 대응, 보고, 해결할 수 있는 능력입니다."*

— 존 맥컴버

전 NIST 공동 의장 및 Gartner 이사, 현 보안 칼럼니스트

59%

생성형 AI를 데이터 보안을 위한 핵심 도구로 간주하는 보안 의사 결정권자의 비율

생성형 AI 채택 주요 이유

데이터 개인 정보 보호 강화	**43%**
위협 인텔리전스 강화	**37%**
보안 운영 개선	**36%**
위협 방지	**33%**

변화에 투자할 때 얻을 수 있는 효과

새로운 접근 방식에 대한 강한 관심에도 불구하고, 보안 의사 결정권자의 **38%**만이 구식 도구를 적극적으로 교체하고 있으며, **62%**는 현재 시스템을 확장하고 있습니다.

기존 도구를 대체하는 보안 의사 결정권자(기존 도구를 확장하는 보안 의사 결정권자 대비)

↓

연간 **보안 사고 건수 20% 감소**

↓

2년 전보다 **동일하거나 적은 수**의 보안 도구를 사용할 가능성이 더 높음
(44% VS. 36%)

↓

업무 환경 보안에 **소요되는 시간이 줄었다**고 응답한 비율이 더 높음
(33% VS. 28%)

> *"조직은 구매한 도구를 철저히 점검해 이미 보유하고 있는 기능을 파악하여 중복된 보호 기능이 있는 도구를 반복 구매하는 일을 방지해야 합니다. 이미 보유한 기능과 보안이 취약한 영역을 명확히 이해하면 조직은 도구 이해도를 높이고, 궁극적으로 보안 사고와 문제를 줄일 수 있습니다."*

— **레이첼 토백**
SocialProof Security CEO

4

중견기업은 혁신할 준비가 되어 있습니다

중견기업 조직(직원 수 300~999명)은 보안 역량을 충분히 발휘하지 못하고 있다는 사실을 분명히 인식하고 있습니다. 복잡한 현대의 업무 환경과 씨름하는 중견기업의 우려는 대기업(직원 수 1,000명 이상)보다 훨씬 큽니다.

특히 중견기업의 의사 결정권자는 빠르게 변화하는 기술 환경에 점점 더 큰 불안감을 느끼고 있으며, 생성형 AI의 급속한 도입으로 불안은 더욱 커지고 있습니다.

73%

생성형 AI의 사용 증가가 조직 내 보안 사고의 증가로 이어졌다고 응답한 비율

(대기업 조직의 경우 58%)

중견기업이 직면한 문제

	대기업과의 격차
71% 구식 기술 사용으로 인해 미래를 위한 준비가 부족하다고 답한 비율	+23pp
63% 복잡한 업무 방식이 보안 유지에 걸림돌이 된다고 답한 비율	+11pp
73% 생성형 AI의 사용이 보안 사고 증가에 기여했다고 답한 비율	+15pp

중견기업의 인식

	대기업과의 격차
63% 보안 사고 발생 가능성에 대해 큰 불안을 느끼는 비율	+13pp
63% 기술 환경이 과거보다 덜 안전하다고 답한 비율	+12pp
36% 보안팀이 보안 위협으로 인한 압박을 받고 있다고 답한 비율	+16pp

새로운 접근 방식에 대한 열린 태도

82%의 중견기업 보안 의사 결정권자는 조직이 보안 접근 방식을 적극적으로 재검토하고 있다고 보고합니다. 중견기업 의사 결정권자의 **81%**가 클라우드 네이티브 앱이 기존 데스크톱 애플리케이션보다 더 안전하다고 응답하며 클라우드 네이티브 솔루션의 이점에 대해 확신을 가지고 있는 것으로 나타났습니다. 클라우드 기술에 대한 이러한 자신감은 중견기업들이 변화의 필요성을 인식하고 있을 뿐만 아니라 더 혁신적인 솔루션을 받아들일 준비가 되어 있음을 시사합니다.

> *"중견기업 조직은 빠르게 프리미엄 시장으로 진입하기 위해 규모를 키우려 한다는 고유한 특성이 있습니다. 경쟁에서 크게 뒤처지고 우려했던 바가 현실화되지 않도록 그 전에 기반을 공고히 해야 합니다."*

— 조슈아 스카르피노 박사
Assessed.Intelligence CEO

82%

보안 접근 방식을 적극적으로 재검토하고 있는 중견기업 보안 의사 결정권자의 비율

5

전 세계 각 지역은 보안 문제를 해결하기 위해 각기 다른 접근 방식을 취하고 있습니다

의사 결정권자들은 모두 지난 1년 동안 업무 방식이 크게 변화했다는 사실을 인정하지만, 이러한 변화에 대처하는 방식은 특히 보안 측면에서 국가마다 큰 차이가 있습니다.

모든 지역 전반에서 의사 결정권자들은 1년 전과 비교해 업무 환경이 변화했다고 응답했으며, 각 시장의 보안 의사 결정권자들은 보안에 대한 접근 방식을 재고하고 있습니다.

"12개월 전과 비교했을 때 업무 방식이 매우/약간 달라졌다"고 응답한 비율"

인도	85%
브라질	74%
영국	73%
미국	62%

"조직이 보안에 대한 접근 방식을 재고하고 있다고 응답한 비율"

인도	83%
브라질	76%
영국	82%
미국	71%

인도

복잡성에 압박을 느끼지만 변화를 갈망

인도의 보안 환경은 매우 복잡하고 다양한 도구가 넘쳐나는 것이 특징입니다. 그럼에도 불구하고 인도의 조직들은 보안 개선과 새로운 해결책 모색에 대해 매우 열려 있으며, 많은 조직이 변화에 적극적으로 대응하려는 자세를 보이고 있습니다. 인도는 분명 변화의 임계점에 도달하고 있으며, 의사 결정권자들은 보다 간소화되고 효과적인 보안 전략의 필요성을 인식하고 있습니다.

보안 개요	전 세계 평균과의 격차
도구 35개 평균적으로 사용되는 개수(제품, 서비스, 앱 등)	+11
보안 도구 19개 평균적으로 사용되는 개수	+9
67% 복잡한 업무 방식이 보안 유지에 걸림돌이 된다고 답한 비율	+10pp

변화에 대한 열망	
82% 조직의 보안에 개선이 필요하다고 여기는 기업의 비율	+8pp
81% 비용과 관계없이 새로운 보안 접근 방식을 수용할 준비가 된 기업의 비율	+8pp

브라질

높은 수준의 불안감을 느끼지만 특정 위협에는 덜 주목

브라질의 의사 결정권자들은 보안 사고와 그 결과에 대해 높은 불안감을 표명하고 있습니다. 그러나 보안 문제의 구체적인 원인에 대해서는 상대적으로 불안감이 적으며, 이는 결과에 대한 두려움은 크지만 사고를 일으키는 취약점에 대한 인식은 부족함을 나타냅니다. 브라질의 조직은 변화를 원하고 있으며, 생성형 AI 도입에 대한 관심(71%, 전 세계 평균은 62%)이 특히 높습니다.

보안에 대한 불안감	전 세계 평균과의 격차
41% 보안 사고에 대해 지속적으로 걱정한다고 답한 비율	+19pp
42% 보안 사고로 인한 신뢰 상실을 걱정하는 기업의 비율	+8pp
37% 보안 사고로 인한 고객 이탈을 걱정하는 기업의 비율	+7pp
39% 보안 사고로 인한 브랜드 이미지 손상을 걱정하는 기업의 비율	+5pp

특정 문제에 대한 낮은 우려	
40% 구식 기술 사용으로 인해 미래를 위한 준비가 부족하다고 답한 비율	-19pp
48% 생성형 AI의 사용이 보안 사고 증가의 원인이 되었다고 답한 비율	-17pp
44% 복잡한 업무 방식이 보안 유지에 걸림돌이 된다고 답한 비율	-13pp

영국

새로운 기술에 대한 우려는 크지만 대응은 느림

영국의 의사 결정권자들은 새로운 기술이 보안에 미치는 영향, 특히 기존 시스템 및 생성형 AI 위협과 관련하여 깊은 우려를 느끼고 있습니다. 그러나 영국은 이러한 위험을 완화하기 위한 정책을 신속하게 시행하지 못하고 있으며, 그로 인해 의사 결정권자들은 더 심각한 수준의 번아웃을 경험하고 있습니다. 이러한 어려움에도 불구하고 영국의 조직들은 새로운 보안 접근 방식을 채택하는 덜 개방적이며, 보안 침해를 불가피한 것으로 인식하는 경향이 강합니다.

기술에 대한 우려	전 세계 평균과의 격차
75% 구식 기술 사용으로 인해 미래를 위한 준비가 부족하다고 답한 비율	+16pp
77% 생성형 AI의 사용이 보안 사고 증가의 원인이 되었다고 답한 비율	+12pp

어려움에도 불구하고 변화에 대한 개방성 부족	
43% 보안 위협으로 인해 보안팀이 과중한 업무와 번아웃에 시달리고 있다고 답한 비율	+15pp
44% 보안 침해를 불가피한 것으로 보는 비율	+14pp
27% 생성형 AI 관련 보안 정책을 도입한 비율	-14pp
60% 비용과 관계없이 새로운 보안 접근 방식을 수용할 준비가 된 기업의 비율	-13pp

미국

과신이 근본적인 위험을 가릴 수 있음

미국의 의사 결정권자들은 보안 상황에 대해 높은 자신감을 보이며, 특히 생성형 AI와 관련된 데이터 유출에 대해 크게 걱정하지 않습니다. 이러한 낙관적인 태도는 긍정적인 요소이지만, 미국 조직이 빠르게 증가하는 위협 환경을 과소평가하고 있을 가능성도 배제할 수 없습니다. 특히 미국은 데이터 유출 비용이 세계에서 가장 높은 국가로, 새로운 위험에 대한 명확한 대응이 부족하다면 과신으로 인해 일부 조직이 향후 공격에 취약해지는 결과를 초래할 수 있습니다.

보안 환경에 대한 자신감	전 세계 평균과의 격차
10% 보안 사고에 대해 지속적으로 걱정한다고 답한 비율	-12pp
55% 생성형 AI의 사용이 보안 사고 증가의 원인이 되었다고 답한 비율	-10pp
52% 기술 환경이 과거보다 덜 안전하다고 답한 비율	-4pp

가장 높은 데이터 유출 비용	
미화 936만 달러 2024년 데이터 유출 평균 비용[1]	+5백만 달러

1. IBM – Cost of a Data Breach Report 2024(2024년 데이터 유출 비용 보고서)

주요 요점

"조직 전체가 보안 위험을 이해하도록 하는 것이 중요하지만 경영진은 보안의 가치를 이해하지 못하는 경우가 많습니다. 하지만 보안 전문가는 '위험은 이렇고 해결책은 이렇습니다'라고 간단하게 설명할 수 있어야 합니다."

조슈아 스카르피노 박사
Assessed.Intelligence CEO

❶ 보안 의사 결정권자와 비즈니스 리더는 힘을 모아야 합니다

보안 의사 결정권자와 고위 경영진은 성공적인 보안 전략을 수립하기 위해 원활한 의사소통과 강력한 위험 관리 프로세스를 기반으로 협업해야 합니다. 보안 의사 결정권자에게 있어 이해관계자의 지지를 얻고 더 긴밀한 파트너십을 구축하는 것은 보안이 생산적으로 작동하느냐 아니면 긴장 요소로 작용하느냐를 결정짓는 중요한 요소가 될 수 있습니다.

❷ 데이터 유출이 발생하기 전에 혁신을 추진해야 합니다

데이터 유출과 같은 위기 상황은 보안 의사 결정권자가 필요한 보안 조치에 대한 승인을 얻는 데 효과적인 촉매제가 될 수 있습니다. 그러나 랜섬웨어와 같은 사이버 공격이 거의 모든 기업의 운영을 단 하루 만에 마비시킬 수 있다는 점에서, 필요한 변화를 사전에 준비하고 실행하는 것이 그 어느 때보다 중요해지고 있습니다. 대부분의 기업의 경우 데이터 유출은 '발생 여부'가 아니라 '언제 발생할지'의 문제입니다.

❸ 공격이 시작되는 지점을 효과적으로 관리해야 합니다

Mandiant의 최신 M-Trends 보고서에 따르면 2023년 성공적인 침해의 72%가 신원 정보 도용(예: 피싱 또는 도용된 사용자 인증 정보)이나 소프트웨어 취약점 공격에서 시작되었습니다. 이는 해당 취약점을 개선하는 것만으로도 조직에 상당한 이점을 가져올 수 있음을 보여줍니다. 예를 들어, Google Workspace와 같은 제품은 피싱 방지 2단계 인증을 제공하고 스팸, 피싱 시도, 멀웨어의 99.9% 이상을 사용자가 접하기 전에 자동으로 차단합니다. 또한 데스크톱 클라이언트 앱이나 온프레미스가 필요 없어 패치나 업데이트의 부담도 없습니다.

"사람들은 '크고 비싼 프로그램이나 도구를 구매해야 효과적이다. 수십만 달러의 비용은 들여야 제대로 된 효과를 볼 수 있다'라고 생각하죠. 하지만 조직의 정책과 문화가 뒷받침된 변화야말로 실로 가장 효과적입니다."

레이첼 토백

SocialProof Security CEO

"AI는 보안 도구에 통합되어 사고와 위협에 대응하는 능력을 향상시키며, 매우 영향력 있는 기능을 제공할 것입니다. AI의 잠재력은 아직 완전히 실현되지 않았지만 앞으로 더 큰 발전이 있을 것입니다."

존 맥컴버

전 NIST 공동 의장 및 Gartner 이사, 현 보안 칼럼니스트

4 변화는 간단한 단계부터 시작할 수 있습니다

기존 소프트웨어 시스템을 한 번에 현대화하는 것은 조직에 부담이 될 수 있습니다. 단계적인 접근 방식을 취하면 최종 사용자에게 미치는 영향은 최소화하면서도 의미 있는 보안 향상을 이룰 수 있습니다. 예를 들어 Chrome Enterprise를 사용자에게 배포하면 이미 많은 사용자가 잘 알고 선호하는 웹브라우저를 통해 내장된 피싱 및 멀웨어 방어 기능, VPN 없는 제로 트러스트 액세스, 데이터 보호 관리 기능을 제공하는 안전한 검색 환경을 지원할 수 있습니다.

5 생성형 AI는 위험을 초래할 수 있지만 보호 기능을 제공할 수도 있습니다

생성형 AI 도구를 사용할 때는 Gemini와 같이 안전하고 업계 표준을 준수하는 도구를 선택하는 것이 중요합니다. 이렇게 하면 데이터 손실 위험을 줄일 수 있습니다. 또한, 생성형 AI는 새로운 위협으로부터 조직을 보호하는 데도 도움이 될 수 있습니다. 예를 들어, Gmail의 AI 방어 기능은 이미 대규모 언어 모델(LLM)을 활용하여 스팸 및 피싱 시도를 더 효과적으로 방어하고 있습니다. 실제로 LLM 덕분에 Gmail에서 스팸 차단율이 20% 향상되었고, 사용자가 신고한 스팸을 매일 1,000배 더 많이 분석할 수 있게 되었습니다. AI 덕분에 수십억 명의 Gmail 사용자들이 진정으로 개선된 이메일 환경을 경험하고 있습니다.

연구 목표

01
현재 보안 환경(각기 다른 우선순위, 사고방식, 우려사항, 과제)에 대한 이해

02
보안 및 기술이 조직에 미치는 영향, 특히 생성형 AI의 확산과 관련한 평가

03
보안의 미래, 새로운 동향, 조직의 미래 투자 계획 탐색

방법

정량적 설문조사

2024년 7월 22일부터 8월 8일까지 미국, 영국, 브라질, 인도에서 2,025명의 응답자를 대상으로 20분간 온라인 설문조사를 실시했습니다.

설문에 참여하기 위해 응답자는 다음 기준을 충족해야 했습니다.

- 300명 이상의 직원이 근무하는 조직의 근무자
  - 조직 또는 팀 차원의 기술/생산성 제품에 대한 결정권을 가진 비즈니스 및 IT 의사 결정권자 또는
  - 조직의 보안 제품에 대한 결정권을 가진 보안 의사 결정권자
- 비규제 및 규제 산업을 아우르는 다양한 업종의 종사자

지역	(응답자 수)
미국	501
영국	523
브라질	501
인도	500
조직 크기	
중견기업(직원 수 300~999명)	834
대기업(직원 수 1,000명 이상)	1,191
역할	
IT 의사 결정권자	673
비즈니스 의사 결정권자	762
보안 의사 결정권자	590
합계	2,025

심층 인터뷰

2024년 8월 22일부터 26일까지 미국에서 6차례의 1시간 가상 심층 인터뷰가 진행되었습니다. 참가자는 300명 이상 규모의 조직에서 근무하는 C급 또는 C-1급 임원(IT, 비즈니스, 보안 의사 결정권자)들이었습니다.

전문가 인터뷰

주요 프로젝트 단계마다 3명의 보안 전문가(존 맥컴버, 조슈아 스카르피노 박사, 레이첼 토백)가 인사이트, 전문 지식, 사고 파트너십을 제공했습니다.