

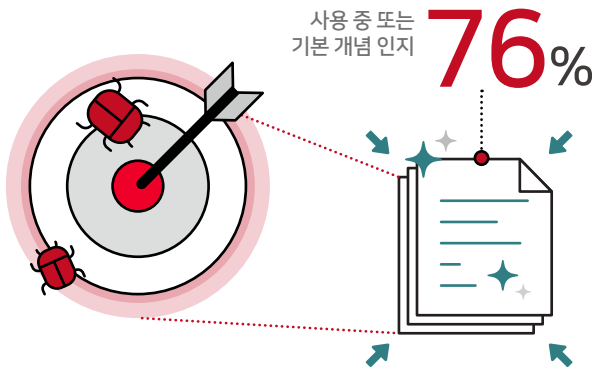
2019

- 기업 APT 대응 보안 현황 설문 조사 결과 -

공통 설문

01

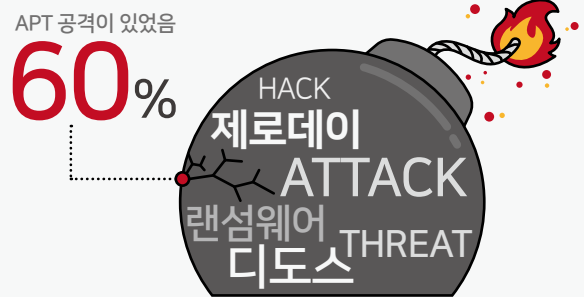
기존 샌드박스의 대체재, 보완재로 주목받고 있는 차세대 APT 대응 기술인 CDR기술에 대해 알고 계십니까?



설문 고객 중 76%(198명)가 차세대 APT 대응 기술인 CDR 기술을 도입 후 사용 중이거나, 기본 개념을 인지했거나, 한 번쯤 들어본 것으로 나타났습니다.

02

귀사는 제로데이, 랜섬웨어, 디도스 등 APT 보안공격으로 피해를 입은 적이 있습니까?



설문 고객 중 60%(157명)가 'APT 공격이 있었다'고 답했으며 '공격이 없었다'와 '공격이 있었는지 모르겠다'라는 응답을 한 40% (134명)는 APT 공격에 취약한 상태로 볼 수 있어 보안사고가 발생할 위험성이 높음을 인지할 필요가 있습니다.

03

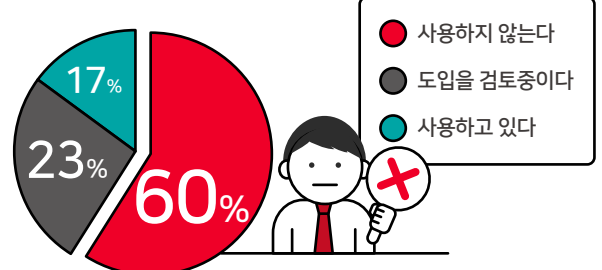
내부 인프라시스템 중 보안이 취약하다고 생각하는 구간은 어디입니까?



설문 고객 중 45%(157명)가 이메일이 가장 보안에 취약하다고 응답하였고, 이어 웹, 망연계 구간, 대외 접점 서비스(게시판, 채용 사이트 등)가 외부 공격의 타겟이 되는 구간이라고 생각한다고 답했습니다. 메일 보안, 웹 방화벽 및 망연계 구간에 전용 보안 솔루션을 적용하여 보안을 강화시킬 필요가 있습니다.

04

APT 대응을 위해 샌드박스(행위분석) 솔루션을 도입/사용 중입니까?



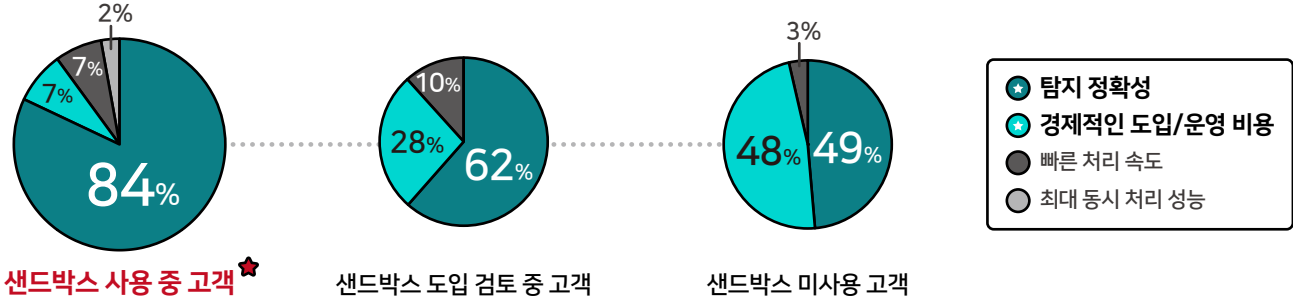
설문 고객 중 60%(155명)가 APT 대응 솔루션을 사용하고 있지 않다고 응답하여 현재 기업의 낮은 보안 인식 수준이 확인되었습니다. 중소기업의 경우 보안에 특히 더 취약한 만큼 보안 수준을 강화할 필요가 있습니다.

“중소기업 해킹 피해 급증...보안수준 강화해야”

기업 사이버 침해사고 건수 중 중소기업 비중 98%

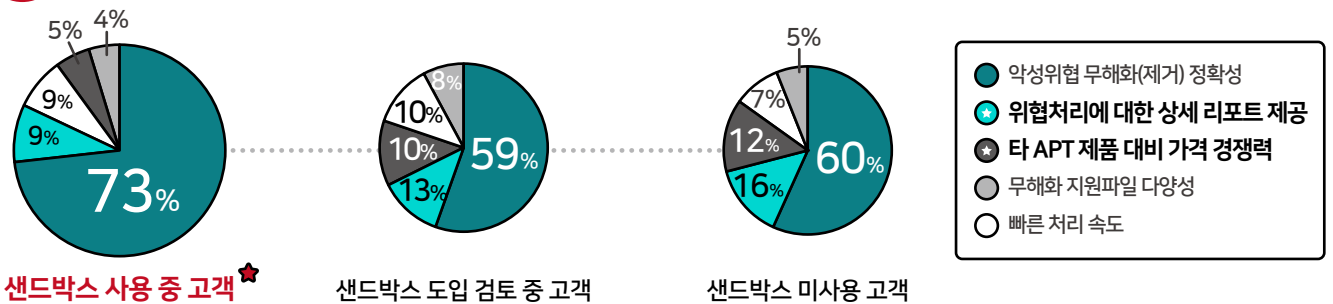
• 개별 설문 •

01 샌드박스(행위분석) 도입 시 가장 중요하게 고려하는 사항은 무엇입니까?



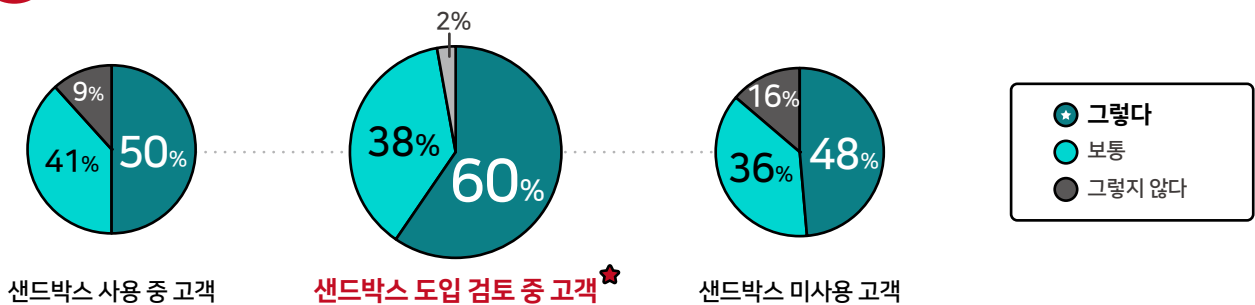
↳ 샌드박스 솔루션을 사용하고 있는 응답자 중 84% 가, 샌드박스 도입을 검토 중인 응답자 중 62% 가, 샌드박스 솔루션을 사용하지 않는 응답자 중 49%가 탐지 정확성이 샌드박스 솔루션의 가장 중요한 기능으로 응답하여 보안 솔루션 본연의 기능을 중시함을 확인하였고, 이어 경제적인 도입/운영 비용이 중요하다고 응답하였습니다.

02 차세대 APT 대응 기술인 CDR의 장점 중 IT관리자로서 가장 관심이 가는 특징점은 무엇입니까?



↳ 차세대 APT 대응 기술인 CDR의 장점을 묻는 질문에 샌드박스 솔루션을 사용하고 있는 응답자 중 73% 가, 샌드박스 도입을 검토 중인 응답자 중 59% 가, 샌드박스 솔루션을 사용하지 않는 응답자 중 60%가 악성코드 무해화(제거) 정확성에 가장 관심이 간다고 응답하였으며, 이어 보안솔루션의 본연의 기능인 보안 기능 외에 위협처리에 대한 상세 리포트 제공에 대한 부분과 타 APT 제품 대비 가격 경쟁력 역시 높은 응답율을 보였습니다.

03 귀하가 뽑은 특징점을 충족한다면, APT 대응 기술·솔루션으로 CDR을 검토하시겠습니까?



↳ 차세대 APT 대응 기술, 솔루션으로 CDR 검토 의사를 묻는 질문에 이미 APT 솔루션을 잘 알고 있는 응답자의 과다수가 적극적으로 검토의사를 밝혔고, 특히나 APT 대응 솔루션 도입을 검토 중인 고객에서 CDR 기술에 매우 높은 관심을 보였습니다. APT 솔루션에 소극적인 응답자 중 36%가 검토하겠다는 응답을 하였습니다. 보통이라고 응답한 대부분의 응답자들은 현재 CDR이라는 개념에 대한 이해도가 높지 않은 것이 가장 큰 이유라고 해석됩니다.

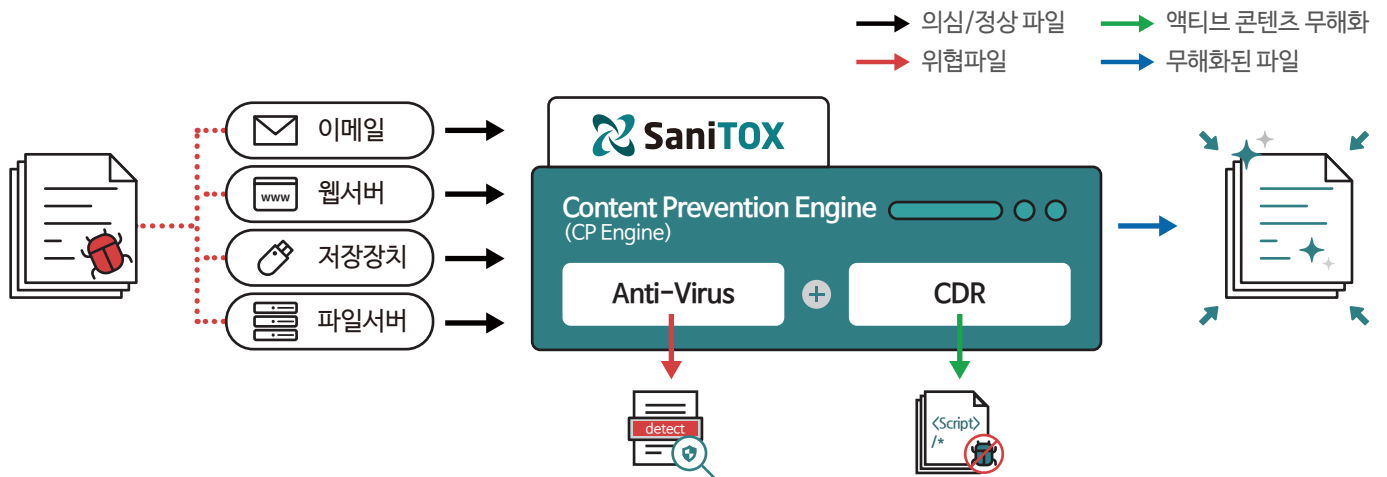


- Summary -

- ✓ 내부 인프라 중 가장 취약하다고 여기는 부분은 **이메일!**
- ✓ APT 공격에 대한 **미흡한 방안 및 낮은 보안인식 수준!**
- ✓ 차세대 APT 대응 기술 CDR 솔루션에 기대하는 기능은 보안기능 외 **위협처리 상세 리포트 및 타 제품 대비 가격 경쟁력!**



SaniTOX 는 지란지교시큐리티가 자체 개발한 CDR 기술을 통해 파일 내 실행 가능한 액티브 콘텐츠(Macro, JavaScript, 임베디드 객체(버튼, OLE 객체))를 원천 제거 후 안전한 파일로 재조합하여 알려지지 않은 보안 위협에 대응할 수 있는 **콘텐츠 악성코드 무해화 솔루션**입니다.



스팸스나이퍼 APT 바로가기

CDR 무료 체험하기