




사이버 AI를 통한 미래업무환경 보안

운용관


한국총괄영업대표

디지털 협업의 빠른 확산




Seat increase
↑58M↑
 Microsoft 365

90% Mobile apps for
business as a
category up

200 MILLION
↑  **zoom**
User Growth
10 MILLION

 Suite **20%** **↑**
adoption increase

 Microsoft Teams
270% Daily users
increase

 **↑25%**
Google Meet User increase

“

1/3 이하의 기업이 클라우드 환경에서 비정상적인
업무 행위를 모니터링하고 있습니다. 클라우드 앱 및
공동 작업 플랫폼의 사용량이 크게 증가하고 있
다는 점을 고려하면 이는 놀라운 일입니다.



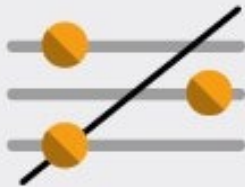


- Cybersecurity Insiders

”



다크트레이스의 위협 통계

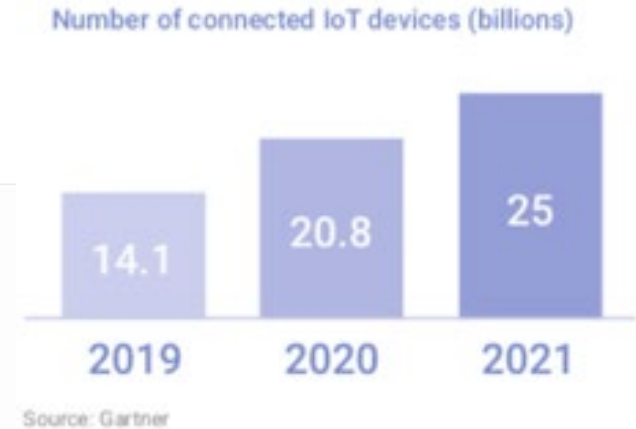


공 요 요 요	위협 통계				
	시간 초과 OUT OF HOURS	랜섬웨어 RANSOMWARE	내부 확산 LATERAL MOVEMENT	SaaS 계정 탈취 SaaS ACCOUNT HIJACKS	뱅킹 트로이목마 BANKING TROJANS
배 배					
	6월 내 탐지된 9% 이상의 위협은 주말 혹은 공휴일에 발생	약 2%의 보안 침해 유형 잠재적인 암호화를 나타내는 비정상적인 확장자 또는 파일 이름을 사용하는 의심스러운 파일 쓰기와 관련하여 6월에 발생	2/3이상의 경고 발생 유형 공격자가 정찰, 타 디바이스 감염 시도가 탐지	다수의 경고 발생 유형 SaaS 이용과 관련한 초기 IOC(침해지표)가 되는 이상한 위치에서의 로그인 비정상적인 계정관리가 발생	6월에 Darktrace는 소수의 클라이언트에게 새로운 Quakbot 감염 에 대해 경고. 뱅킹 트로이 목마는 랜섬웨어, 크립토 마이닝 및 데이터 유출과 같은 다른 형태의 공격과 함께 볼 수 있으며, 트로이 목마의 초기 발견은 추가 감염을 방지



동적인 조직 인력

- 디지털 트랜스포메이션 프로젝트의 가속화
- 직원이 멀웨어 및 취약점을 가져 오거나 비승인 기술을 실수로 사용
- 유동적인 작업 환경과 시간
- 사무실과 재택근무 환경 간의 분할된 하이브리드 작업 패턴
- 파괴와 변화를 통해 번성하는 잘 드러나지 않는 사이버 범죄자





새로운 업무 패턴에 적응한 인공지능



- 속도와 규모에서 직원의 새로운 정상행위 학습
- 안심할 수 있는 **통합적이고 일관된** 사이버 보호
- 보안 팀의 업무 플로우 간소화
- **자율** 탐지, 분석 및 대응 기능을 통해 인간은 **전략적 업무에 집중**
- ‘**위험적인**’ 행위에 대한 동적인 이해





ENTERPRISE
IMMUNE SYSTEM

탐지 Detect



CYBER AI
ANALYST

조사 Investigate



DARKTRACE
ANTIGENA

대응 Respond

DARKTRACE IMMUNE SYSTEM

World-leading Cyber AI • Cloud-Native

세계최고의 Cyber AI • 클라우드 네이티브



EMAIL



Suite
Microsoft 365



SaaS



box
SharePoint

CLIENTS



CLOUD



aws
Microsoft
Azure

NETWORK



SCADA



OT DEVICES



WORKFORCE

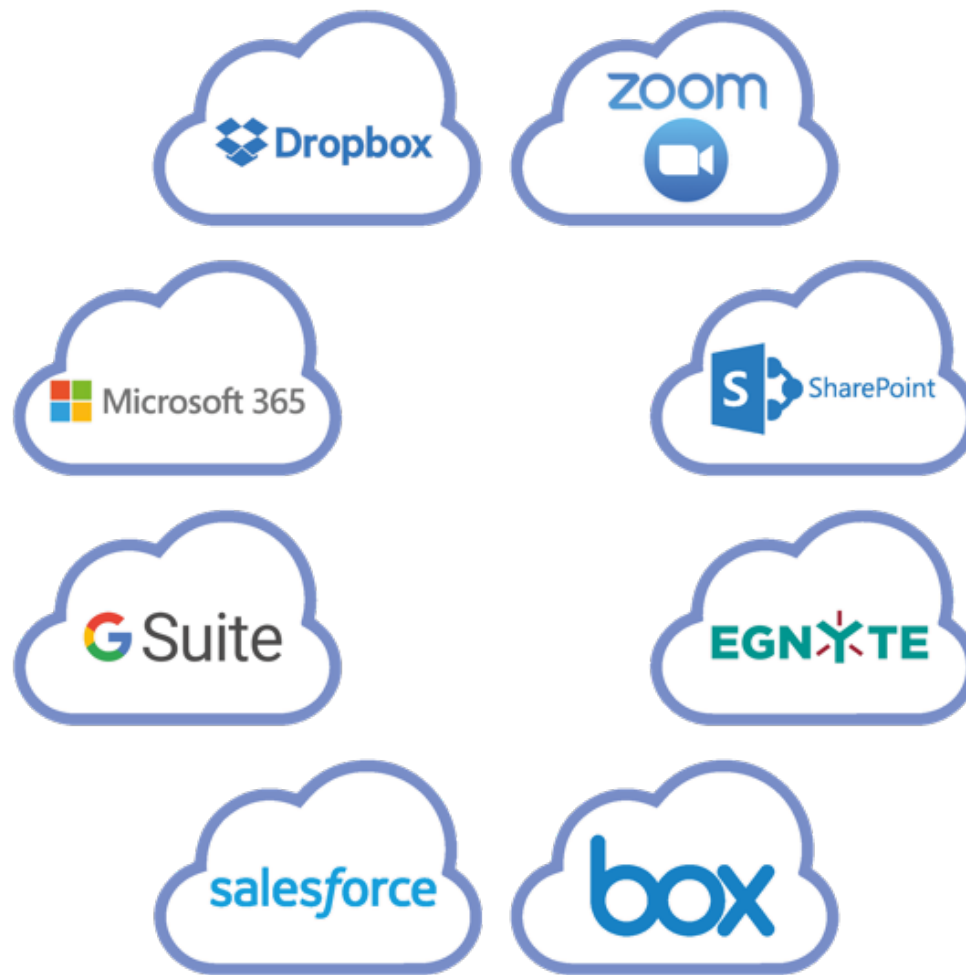
INFRASTRUCTURE

INDUSTRIAL

동적인 조직 인력 보호를 위한 사이버 AI



- 엔드포인트, 이메일, SaaS 환경의 **가시화**
- 전체 디지털 조직에 대한 **문맥 이해**
- **모든 범위의 위협 탐지**-
계정 탈취 및 악의적인 내부자에서부터
중대한 설정 오류 까지
- 공격이 어디에 있든 **자율적으로**
조사하고 대응





이메일을 위한 사이버 AI



- 악성 이메일을 식별하기 위해 **자가 학습**
- 각 사용자를 **단순한 이메일 주소가 아닌 동적인 개인**으로 취급
- 개인 및 피어 그룹을 위해 진화하는 **‘삶의 패턴’** 생성
- 모든 범위의 이메일 위협 탐지
 - 사회학적 엔지니어링
 - 기업 이메일 침해
 - 데이터 손실
 - 스피어 피싱

1 in every 99 emails is a Phishing Attack



Source: Avanan

“Antigena Email이 Gartner Magic Quadrant의 리더가 놓친 스피어 피싱 캠페인을 포착했을 때 우리는 확신했습니다.

- CIO, Numeris

”

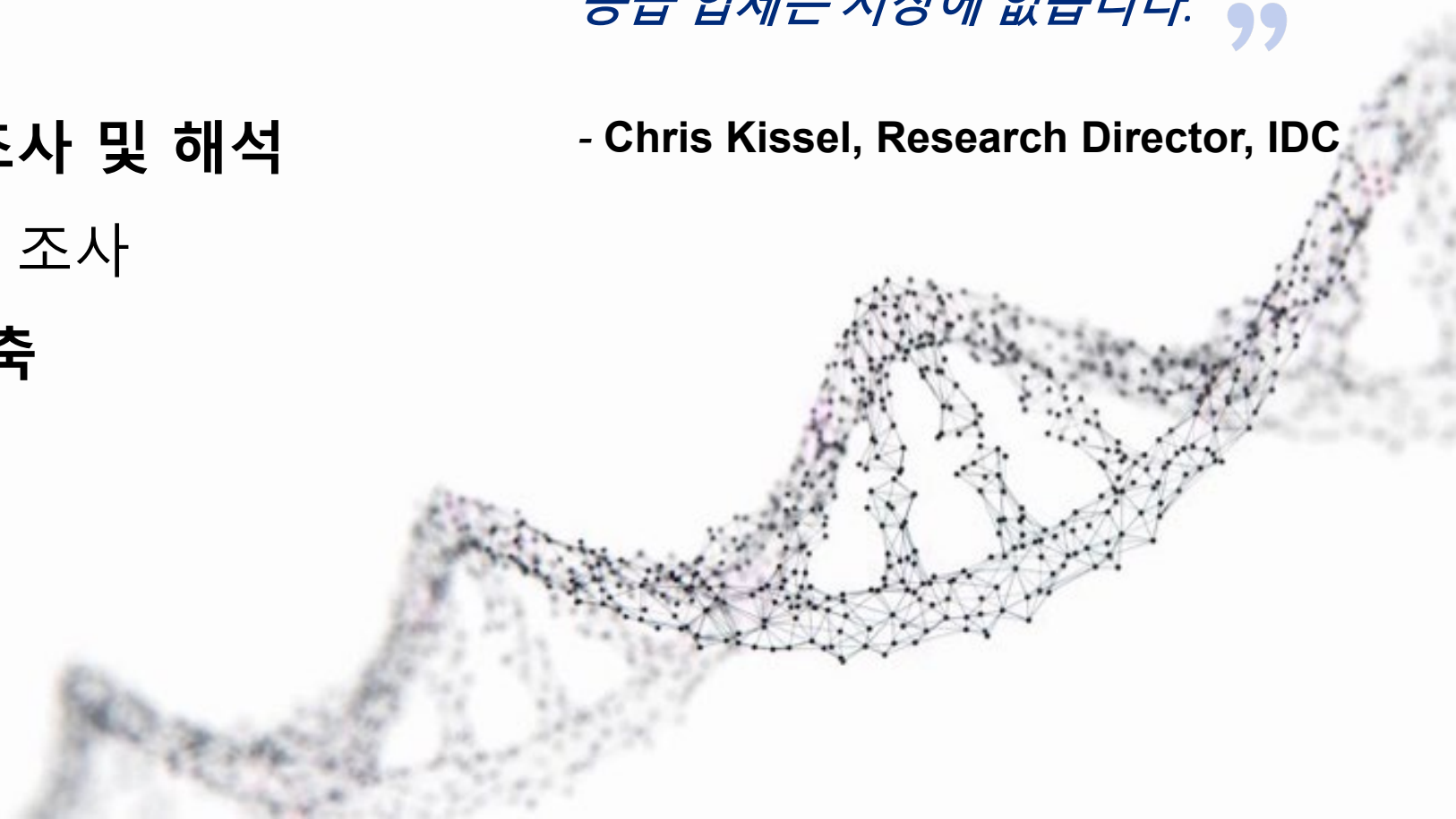
인공지능 분석가: 중요한 시간 절약



- 자율적 위협 탐지를 넘어서 위협을 이해하고 **인간 가설을 모방하며** 탐지된 내용을 이해
- **자동화된 사이버 위협 조사 및 해석**
- 모든 위협을 지속적으로 조사
- **조사 시간 최대 92% 단축**

“사이버 위협에 대해 동일한 AI 기반 조사 및 분석을 제공할 수 있는 **다른 공급 업체는 시장에 없습니다.**”

- Chris Kissel, Research Director, IDC





반격: 자율 대응



- 자율적, 외과적인 공격 중단
- 인간보다 **빠른** 반응
- 정상적이고 적법한 평소 업무에 **영향을 미치지 않음**
- SOC에서 다른 톨의 기능 향상
- 담당자가 **중요한 일에 집중**할 수 있게끔
- 매 **3 초**마다 위협에 대응

“Antigena는 진행중인 공격을 자율적이고 정확하게 대응할 수 있습니다. Darktrace는 시스템 방어 방식을 근본적으로 변화시키고 있습니다.”

- Layton Construction



69% 기업에서 인공지능이 사이버 공격에 대응하기 위해 필요하다고 판단합니다.

Source: Capgemini Research Institute

You can't bring a human to a machine fight

Q&A



“저희팀은 이제 SaaS 애플리케이션과 클라우드 컨테이너 전반에 걸쳐 완전한 실시간 커버리지를 확보했습니다.”
-라스베가스 최고정보관리자(CIO)

“Darktrace AI는 현업에 적응하여 네트워크와 클라우드 인프라의 가시성을 실시간으로 밝힙니다.”
- CISO, Aptean

“Darktrace의 OS 센서를 활성화했을 때 마치 어두운 방에서 스위치를 켜는 것과 같습니다.”
- 최고정보위협관리자, TRJ 텔레콤

“Darktrace는 디지털 공간에서 일어나는 변화에 뒤처지지 않도록 도움을 줍니다
-McLaren 최고정보관리자(CIO)

“다크트레이스는 우리가 완전히 인지하지 못했던 위협과 취약점을 알려주었습니다.”
- CTO, Bunim/Murray

“Darktrace는 이 불확실성의 시대에 우리 조직과 함께 발전해 나갈 수 있을 것이라 확신합니다.”
- Ali Khan, Better.com
최고정보보호책임자(CISO)



감사합니다

30 일 체험 Proof of Value을 원하시면, darktrace.com,
방문 혹은 info@darktrace.com 로 이메일 주십시오.