opentext™

기업의 데이터 보호를 위한 플랜 B: 백업

Carbonite Backup for M365

2020.12 | OpenText Korea

opentext™

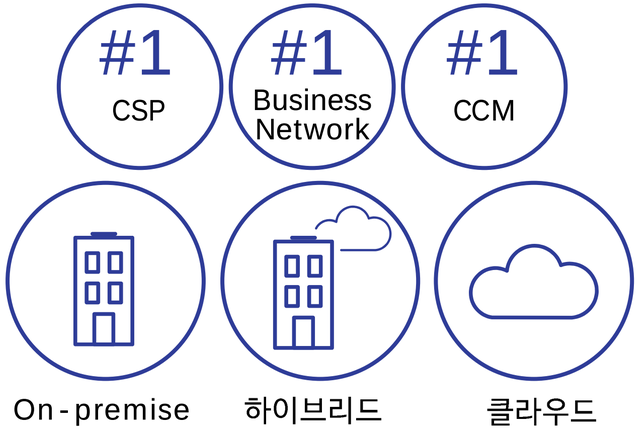
NASDAQ, TSX: OTEX
A TSX-60 Company

OpenText는 기업 소프트웨어 및 클라우드 솔루션을 위한 EIM 업계의 선두주자로서,
조직 내외부의 다양한 정보를 원활히 연결하여 똑똑하게 일할 수 있는 환경 조성을 지원합니다.

#1

EIM

클라우드 및 On-premise



$3.1 B
FY20 매출

14,400+
임직원

100M
사용자

75,000
엔터프라이즈 고객

80%
포춘 1000대 기업

60M
Secured IDs

29년
혁신의 시간

16,000+
파트너

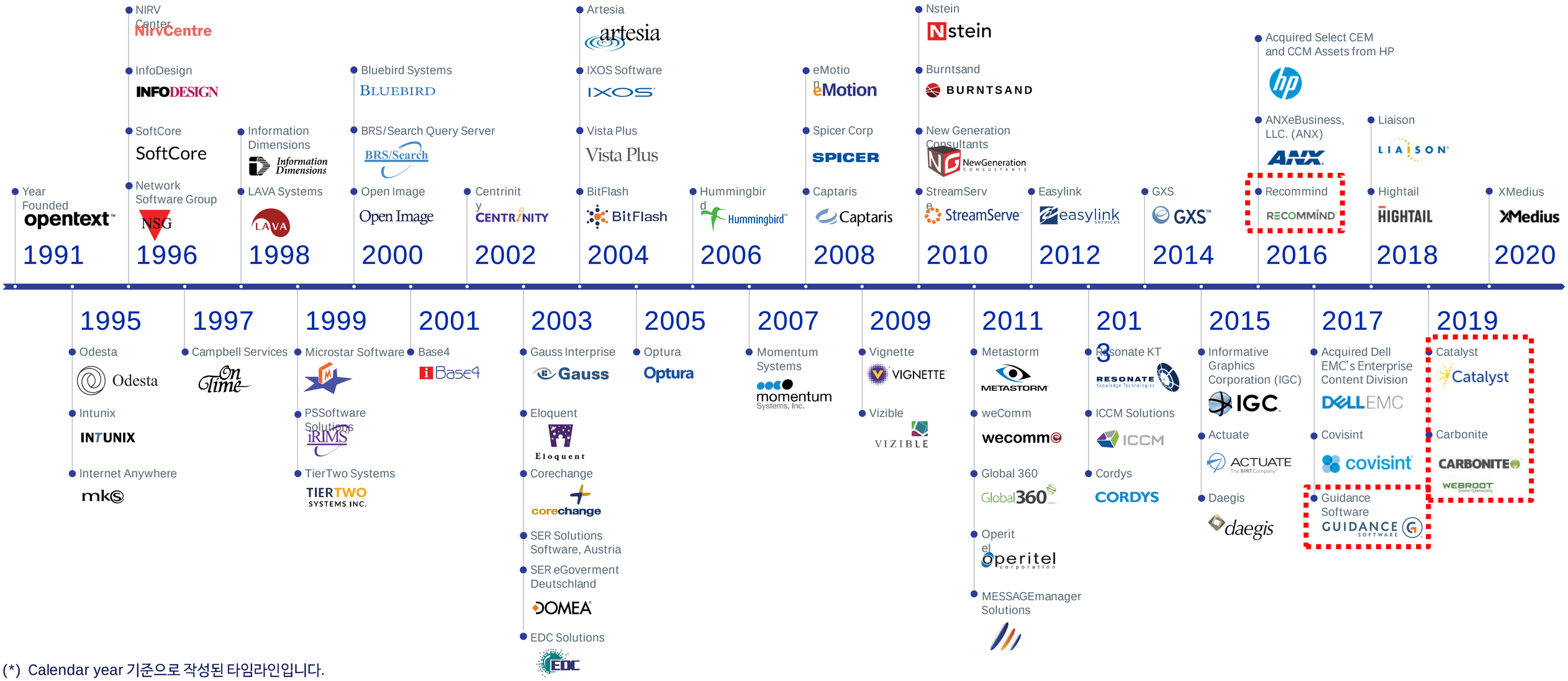
250M
안전한 엔드포인트

11M
클라우드 구독자

35개
국가

3 Exabyte
관리 중인 데이터

OpenText 인수 기업*



(*) Calendar year 기준으로 작성된 타임라인입니다.

OpenText 보안 포트폴리오

Train | Block | Protect | Backup | Recover

WEBROOT®
an opentext™ company

- Security Awareness Training
- BrightCloud Threat Intelligence
- DNS Protection
- Business Endpoint Security

opentext™

- Core Share
- Core Signature

GUIDANCE SOFTWARE
an opentext™ company

- EnCase Security
- EnCase Forensic
- Tableau

CARBONITE®
an opentext™ company

- Backup for M365
- Server Backup
- Recover
- Availability
- Migrate

디지털 위협의 증가

코로나 19

글로벌 팬데믹을 악용한 보안 위협이 증가하고 있으며, 그 중 약 92%의 공격이 스팸 메일을 통해 전파

Source – 트렌드마이크로 2020 상반기 리포트

원격 근무

83.4% 개인 소유 기기를 업무에 사용.
51% 업무 관련 문서를 개인 PC 혹은 외장매체에 저장.

Source - 이스트시큐리티

코로나19 관련 사이버공격 급증...90% '마스크 피싱'

뻥 뚫린 원격근무 "백신? 모르겠다...문서저장 내 PC에"

[데이터뉴스]코로나19, 디지털 전환 빨라진다

발행일 : 2020.08.25

기사만 콕

전세계 의료업계 랜섬웨어 '주의보'…이달에만 71% 급증

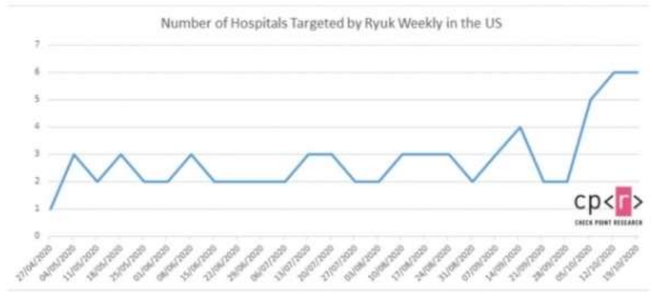
최은정 기자 입력 2020.10.31 09:42 | 수정 2020.10.31 09:57

미국에 집중, '듀크' 랜섬웨어 공격 두드러져…체크포인트

[아이뉴스24 최은정 기자] 이달 의료업계를 대상으로 한 랜섬웨어 공격이 전세계적으로 크게 증가한 것으로 나타났다.

31일 체크포인트에 따르면 이달 미국에서 탐지된 랜섬웨어 공격은 전체 산업군 중 의료부문에 가장 집중됐다. 지난달 대비 공격 건수가 71% 늘어났다.

또 아시아태평양(APAC)과 유럽과 중동·아프리카(EMEA) 지역의 경우 의료 산업계 대상 공격이 전월 대비 각각 33%, 36% 올랐다. 특히 아태 지역의 경우 싱가포르(133%)와 인도(20%)가, 유럽 지역에서 독일과 벨기에를 대상으로 한 공격이 약 200% 씩 증가했다는 게 회사 측 분석이다.



류크 랜섬웨어 공격을 받은 미국 병원 수 [출처=체크포인트]

[본문]
- 신천지 비상연락망 위장
- Bisonal 원격 제어 악성코드 유포

[코너]
- 마스크 관련 내용 위장
- 원격 제어 악성코드 유포

디지털 전환

36.2% 기업들 코로나19 이후 IT투자 증액 계획.
35.4% 금융사들 사이버보안에 추가 투자 계획.

Source - JP 모건

랜섬웨어

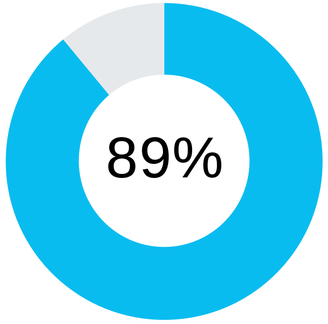
랜섬웨어에 대한 공격 전년 대비 35% 이상 증가.
IoT, 의료 기기 등 랜샘웨어에 의한 공격 증가.

Source - 트렌드마이크로, 체크포인트

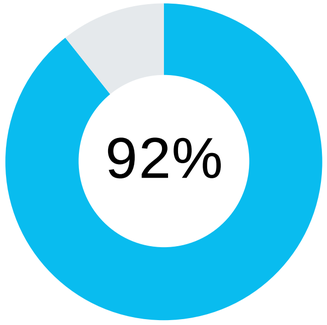
2020년 랜섬웨어와 악성 코드

1억 2천만+
Case

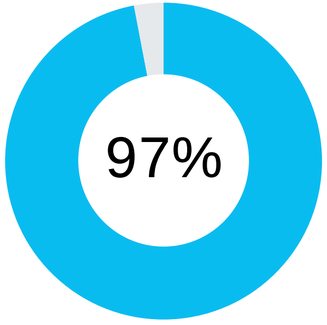
랜섬웨어 공격*
2020년 상반기 기록
(2019년 대비 20% 증가)



코로나19 사태를 활용한
악성 코드 유포 ±



지난 12개월 동안 디지털 공격이
증가하였다고 보고 ±



지난 12개월 동안 기업들이 디지털 공격에
의해 피해를 봤다고 보고 ±

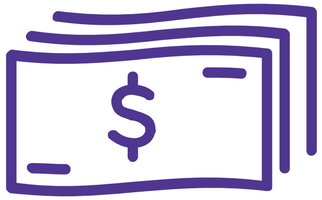
∞ 2020년 2월과 3월 사이 미디어 사이트를 중심으로 한 피싱 공격의 증감률:

NETFLIX	525%
YouTube	3,064%
twitch	337%
HBO	525%

Source: *SonicWall Capture Labs, plus ± VMware/Carbon Black Global Threat Report June 2020 and ∞ Webroot RTAP

2020년 최악의 악성 코드

랜섬 비용 및 다운타임으로 인한 손실 증가



평균 몸값 지불 금액

2020 1월:

$84,116

평균 몸값 지불 금액

2020 6월:

$178,254

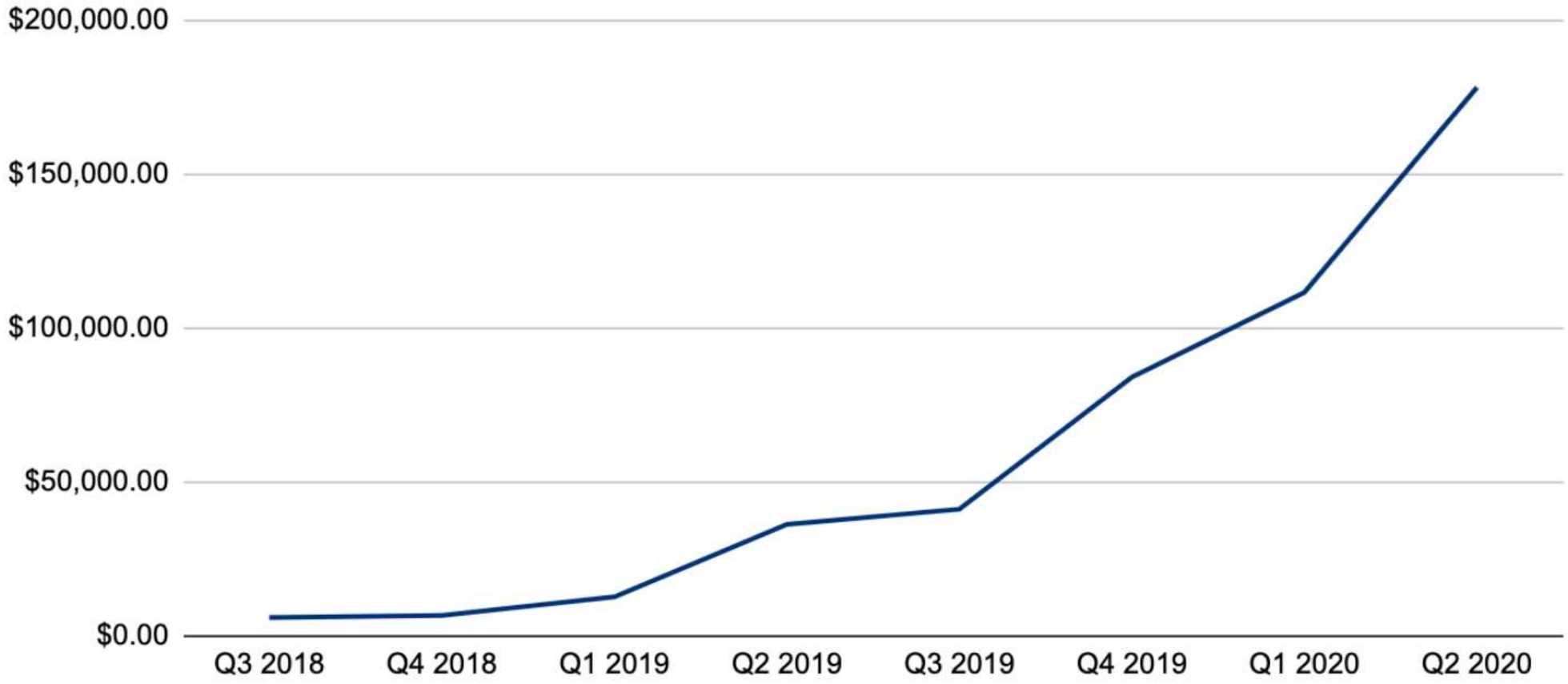
랜섬웨어로 공격으로 인한 평균 서비스 다운 타임

16.2 days

https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report
Source: Coveware Q4 2019 Ransomware Marketplace Report (January 2020)

Average Ransom Payment by Quarter

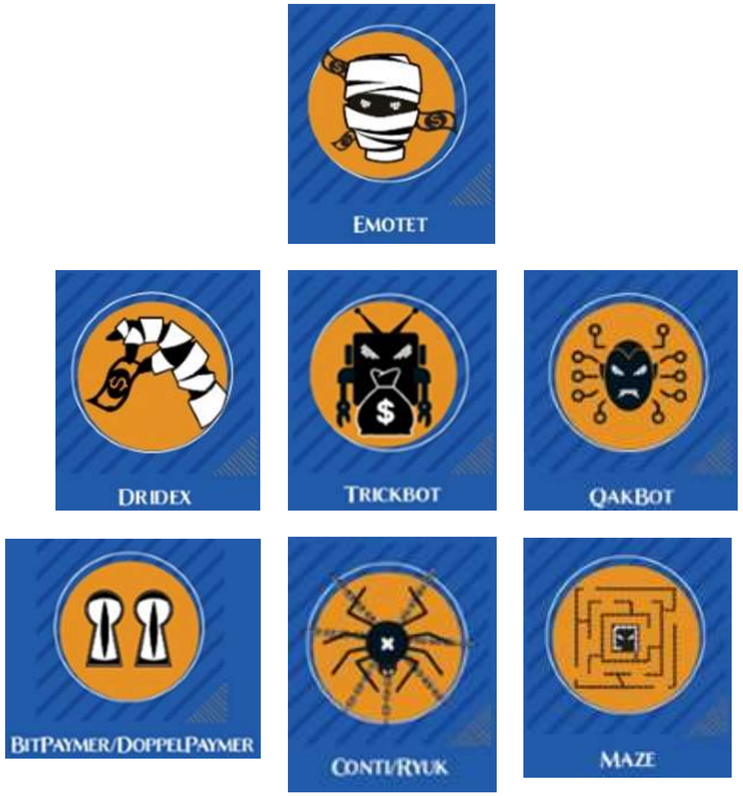
Amounts are in USD



COVEWARE

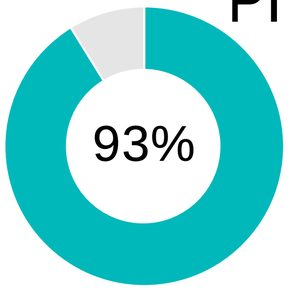
2020 공격 현황

봇넷을 활용한 랜섬웨어 배포

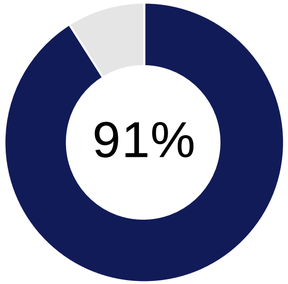


RDP

Phishing



of breaches are caused by phishing and scams[1]

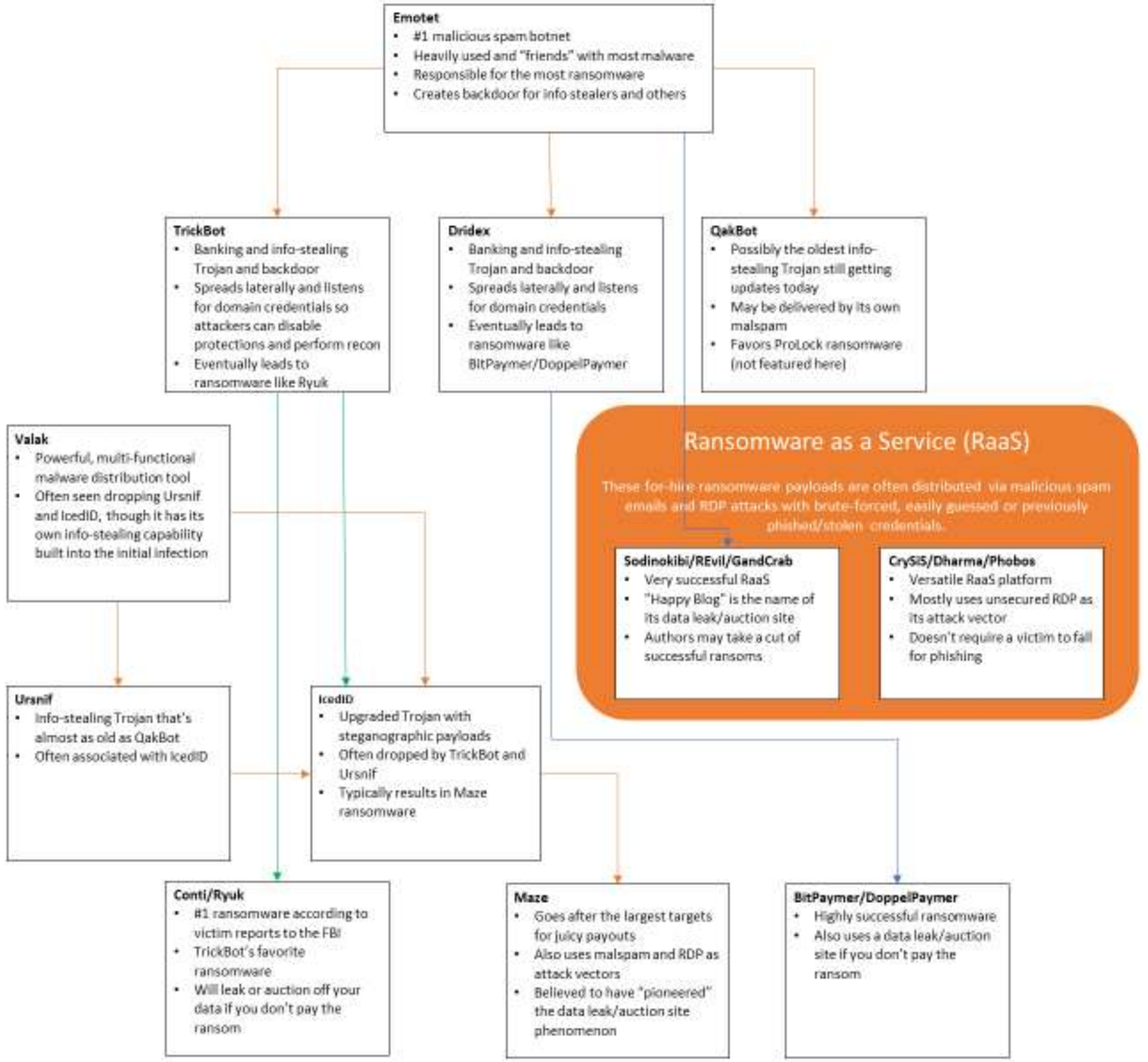


of cyberattacks start with phishing email[2]

Ransomware as a Service

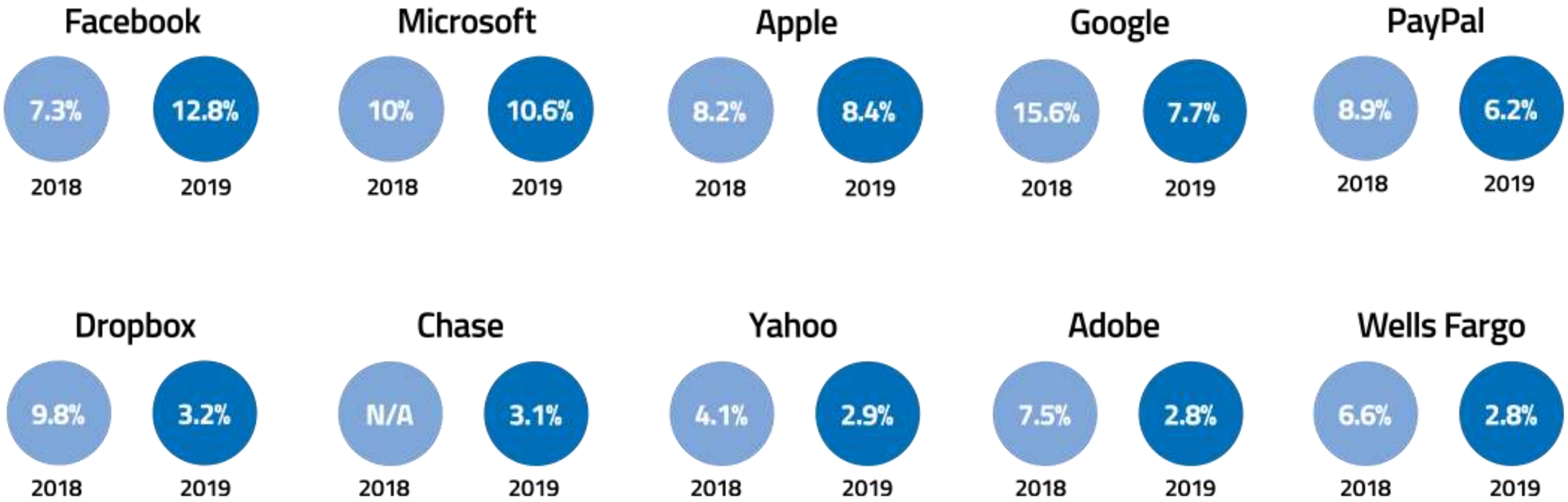
[1] 2018 Verizon Data Breach Investigations Report
[2] https://blog.knowbe4.com/bid/252429/91-of-cyberattacks-begin-with-spear-phishing-email

사이버 공격(랜섬웨어)의 기업화



2019년 기업을 가장한 Phishing 사이트 Top 10

Phishing URL들이 연간 640% 증가

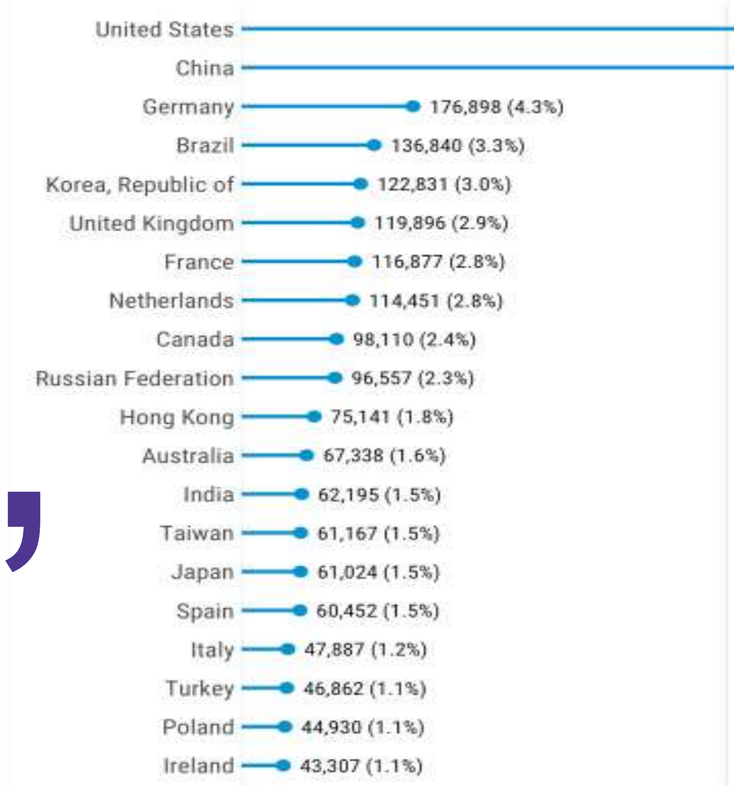


Webroot 2020 Threat Report

RDP 취약점을 활용한 공격

Rapic7 bi-annual National Exposure Index scans

Rapid7에서 실시한 인터넷 스캔에서 3389/TCP 포트가 열려 있는 온라인 장비가 1,100만 대 이상이었고, 그 중 410만 대가 RDP 프로토콜을 사용하고 있었다.



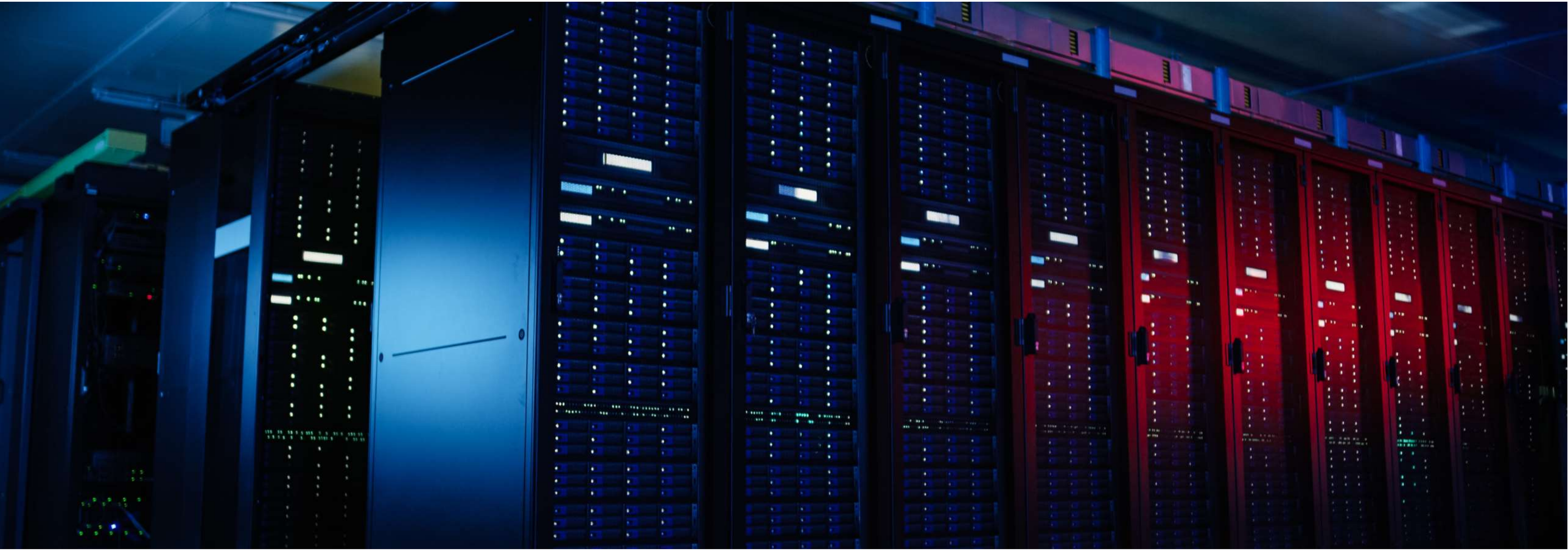
Webroot 위협 보고서에 따르면 RDP 프로토콜의 취약점을 활용한 랜섬웨어 공격이 기존 스팸 캠페인을 통한 전파를 압도하고 있다.

Shodan.io

Carbonite Backup for Microsoft 365

Overview

예전의 백업 목적



도난 사고

자연 재해

하드 디스크 파손

오늘날의 백업 목적

악성 코드

파일 삭제

내부자 위협

사용자 부주의

해킹

관리자 부주의

영향

38%
2010년 이후 다운타임에 의한 비용 증감

$10K+
기업들이 데이터 복구를 위해 랜섬웨어에 지불하는 몸값

65%
지난 한달 이내에 다운타임에 대비하여 계획을 세운 SMB 기업들

46%
기업들이 다운타임으로 인한 “매출 감소”를 걱정함

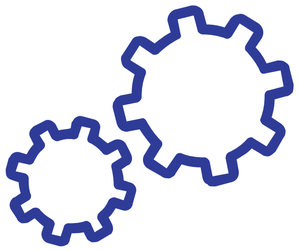
51%
기업들이 다운타임으로 인한 “고객 신뢰 감소”를 걱정함

Out of business
많은 기업들이 재해에 대비하지 못하고 있음

Source: "Cost of Data Center Outages," Ponemon Institute, 2016
Source: Enterprise Strategy Group Master Survey Results, 2018

주요 고객 과제

Microsoft는 실제 데이터 손실을 감지하지 않으며, 고객 데이터에 대한 책임을 지지 않음



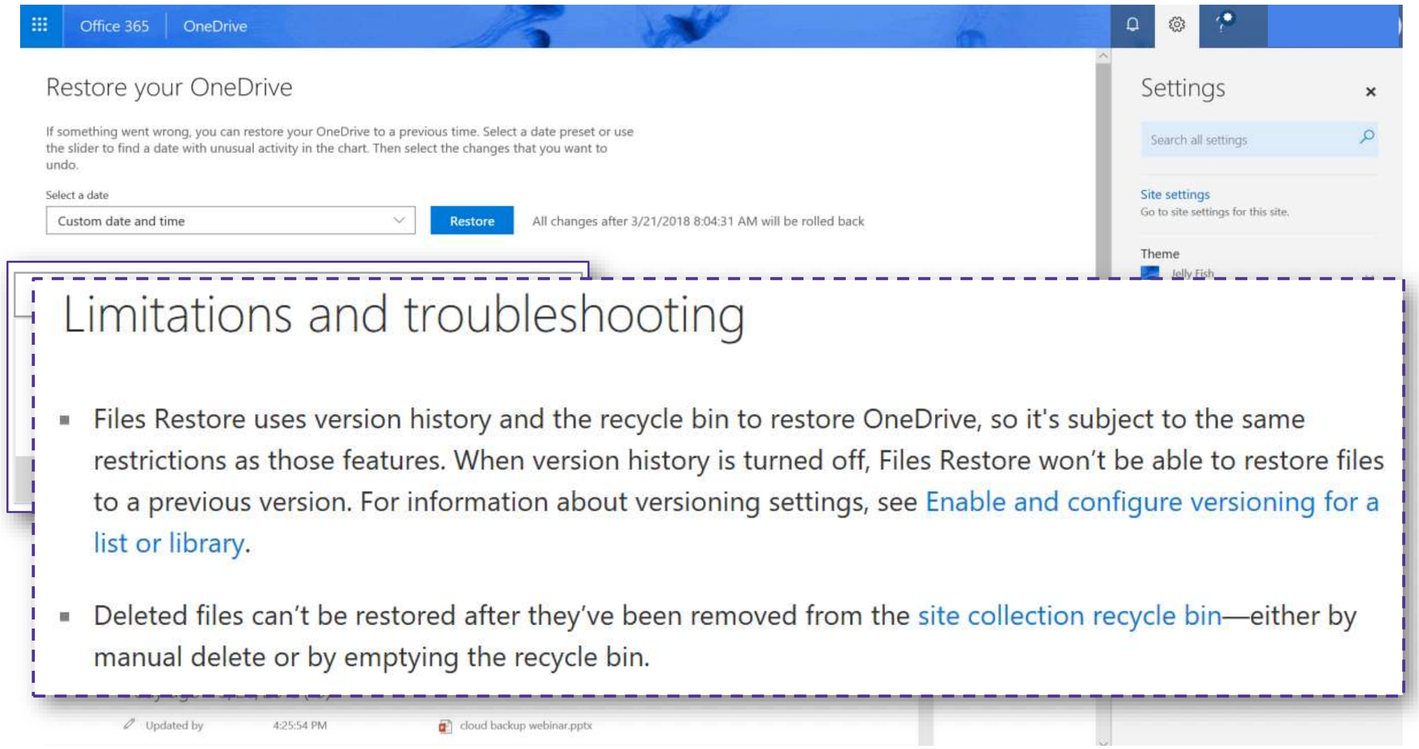
때로 복구 프로세스가 수동으로 처리되거나 많은 시간을 소모하게 됨

최근 기업의 최우선 과제는 Cyber resilience를 확보하는 것에 있음

Source: Naveen Chhabra, Back up your SaaS Data, Forrester Inc. Jan 2018
ESG 2019 Technology Spending Report

충분한 데이터 백업이 필요

- OneDrive에만 적용이 되고, 다른 SharePoint 사이트들이나, 그룹들 혹은 다른 Microsoft 365 서비스에는 적용 안됨
- 파일 별 혹은 폴더 별 세분화된 복구 기능을 제공하지 않음
- 지정한 날짜로 OneDrive 폴더 통째로 롤백하는 것만 제공
- 원본 컨텐츠와 버전을 삭제함 (destructive restore only)
- 30일까지만 저장



사용자 책임의 과중

Microsoft**가 보장**

- ✓ 하드웨어 혹은 인프라 장애로 인한 **서비스** 장애
- ✓ 자연 재해 혹은 데이터 센터 중단으로 인한 **서비스** 장애
- ✓ **단기적(30일)** 사용자 부주의로 인한 휴지통/버전 기록에 대한 복원 (OneDrive "Files Restore"도 포함)
- ✓ **단기적(14일)** 관리자 부주의로 인한 그룹, 사서함 삭제 혹은 서비스 중심의 롤백에 대해 지원

사용자 책임

- ❑ 직원 퇴사 및 계정 비활성화로 인한 데이터 손실
- ❑ 악의적인 내부자로 인한 데이터 손실 혹은 해킹으로 인한 컨텐츠 삭제
- ❑ 랜섬웨어 혹은 악성 코드로 인한 데이터 손실
- ❑ 장기적인 데이터 센터의 중단으로부터의 복구
- ❑ 사용자 부주의로 삭제된 데이터의 복구를 위해 장기적이고 선택적인 롤백

Source: Naveen Chhabra, Back up your SaaS Data, Forrester Inc. Jan 2018

Carbonite® Backup for Microsoft 365

모든 Microsoft 365 어플리케이션을 위한 포괄적이고 엔터프라이즈급 백업 제공

- **포괄적인 플랫폼 보호**
  재해 및 일상적인 데이터 손실로부터 Teams, Yammer 및 Planner 등을 포함한 모든 Microsoft 365 제품군 보호
- **복원 세분화**
  Microsoft 365에서 개별적 아이템을 복구. 사서함, 대화, 프로젝트, 작업, 일정 및 파일 등
- **백업 및 보존**
  유연한 보존 옵션으로 하루에 최대 4회 자동 백업 지원
- **데이터 손실 보호**
  일상적으로 발생하는 데이터 손실의 방지

Carbonite 주요 장점

- 클라우드 기반 솔루션으로 가용성을 보장하고, 복잡성 및 비용을 감소 (nothing on prem)
- 하나의 관리 공급 업체
- 사용자 부주의에 의한 삭제 및 랜섬웨어에 대한 리스크 감소
- 비즈니스에 맞게 솔루션을 쉽게 확장할 수 있음
- 무제한의 저장소 사이즈 제공
- 30분 이내의 솔루션 셋업
- 고객들이 가지고 계신 Azure Key Vault를 이용하여 암호화 가능
- Microsoft 365에 상세 복원 혹은 Tenant 사용이 불가할 경우 로컬에 저장
- 더 이상 Microsoft 365 라이선스가 없는 퇴사자의 데이터를 손 쉽게 복원

Microsoft 365의 모든 것을 백업 가능

Office 365

Microsoft Teams | Skype for Business | Exchange Online | SharePoint Online | Planner | Yammer The Enterprise Social Network

사용자들이 인지하는 Microsoft 365

- Team Chat
- Team Channel
- MS Teams Voice, Video, Meetings
- IM
- S4B Broadcast
- User Mailboxes
- Calendars
- Group conversations
- Group mailboxes
- Sites, Lists, Libraries
- Microsoft 365 Video Portal
- User OneDrive's
- Group Files
- Group Notebooks
- Plans
- Buckets
- Tasks
- Teams Planner
- Teams Files
- Internal Networks
- External Networks
- Yammer Notes and Files

실제 컨텐츠가 저장되어 있는 Microsoft 365 서비스들

Carbonite Backup for Microsoft 365

적용 필요 사례

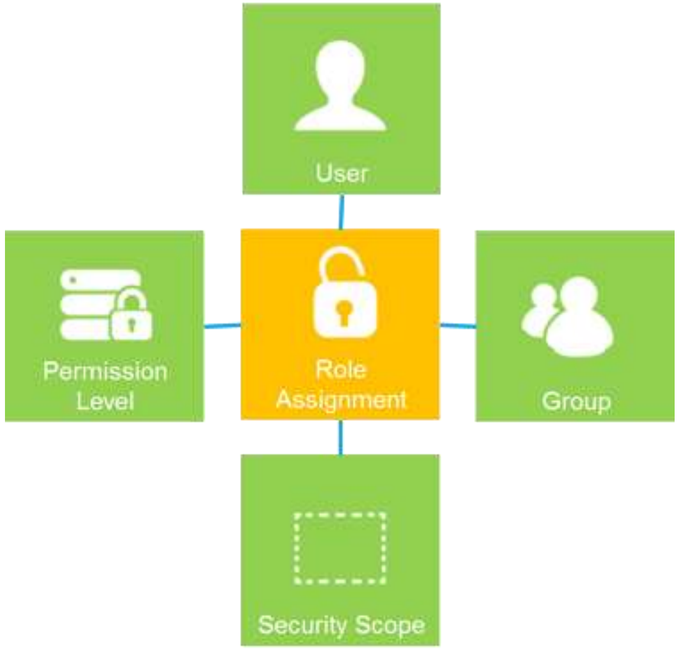
Use case: 권한만 복원

문제점

- 사용자가 손 쉽게 OneDrive, SharePoint 그리고 Teams의 권한을 변경할 수 있음
- 이는 중요한 비즈니스 데이터를 외부에 노출시키거나, 불필요한 내부 접속을 방치할 수 있음
- Office365 기능에서는 권한에 대한 롤백을 지원하지 않음

해결 방안

- Carbonite Backup for Microsoft 365 는 컨텐츠는 그대로 보존하면서 보안 설정을 특정 시점으로 복원함으로써 권한만을 복원 시킬 수 있음



Use case: **퇴사 직원의 데이터 복원**

문제점

- 직원이 퇴사하게 되면, 일반적으로 해당 직원의 Microsoft 365 라이선스가 다른 직원으로 이관되게 되고, 이로 인하여 퇴사 직원의 데이터에 접근할 수 없음

해결 방안

- 백업 시스템을 통해 퇴사 직원의 데이터를 복구 (Microsoft 365 라이선스 불 필요)
- 파일과 이메일을 지정된 새로운 사용자에게 복원

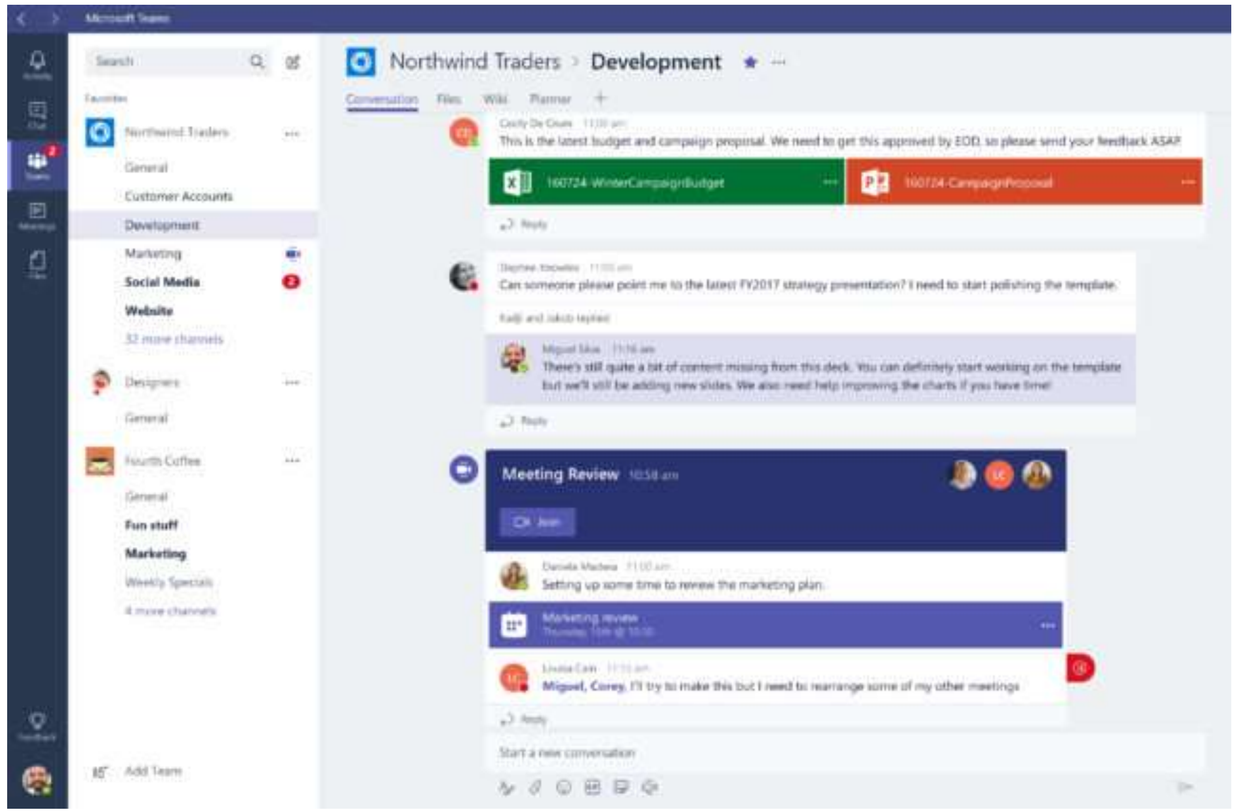
Use case: Teams 복원

문제점

- 비즈니스에서 Teams의 사용 비중이 높아지고 있음
- 비즈니스의 컨텐츠는 파일, 일정 보드, 그룹 그리고 대화 등에 저장되고 있음
- 사용자들 부주의 등으로 인한 이유로 Teams 내의 컨텐츠를 삭제할 수 있음

해결 방안

- Teams를 백업하고 복구할 수 있어야 하며, 이는 대화창도 마찬가지로 지원되어야 함



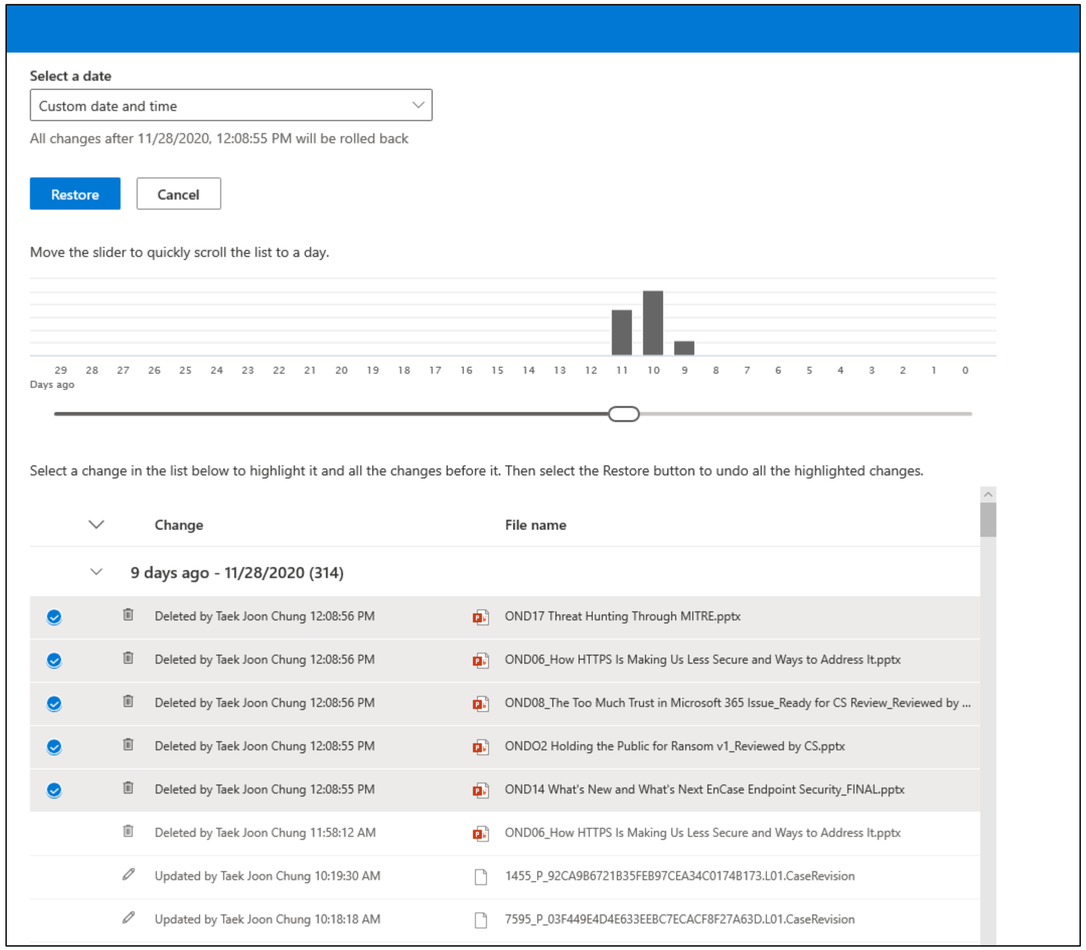
Use case: SharePoint 데이터의 복원 세분화

문제점

- 보관된 이전 프로젝트의 대규모 SharePoint 사이트가 존재할 경우
- 혹은 사용자가 새로운 프로젝트를 위해 몇 개의 중요 문서만 필요할 경우

해결 방안

- 원본 SharePoint 사이트에서 파일별로 세분화하여 OneDrive로의 복원이 필요
- SharePoint 사이트를 전체 복원할 필요가 없어, 빠르고 안정적으로 복원 필요



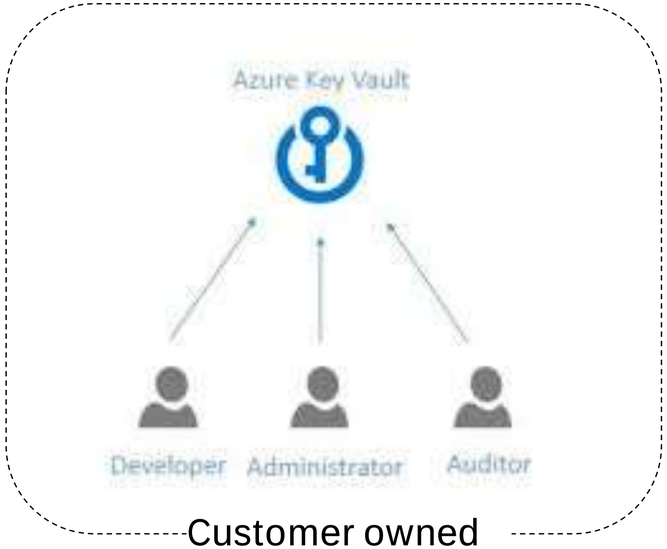
Use case: 고객이 사용중인 암호화 키 사용

문제점

- 내부 규정에 따라 고객의 암호화 키의 소유권을 유지해야 함

해결 방안

- Carbonite를 사용하면 고객이 관리하는 Azure Key Vault를 활용하여 BYOK (Bring Your Own Key)를 사용할 수 있음
- 고객이 관리하는 키를 활용하여 데이터를 암호화하고 오직 고객만이 복호화를 진행할 수 있음
- 고객별 내부 규정에 맞게 키 사용을 모니터링 및 관리할 수 있음



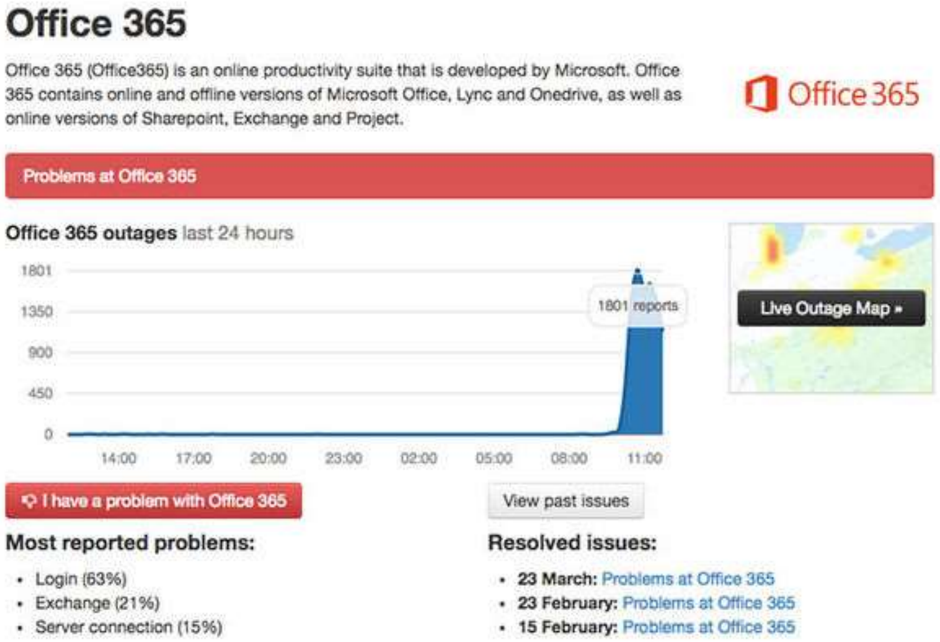
Use case: Microsoft 365의 서비스 중단 시, 주요 파일들에 대한 복원

문제점

- 갑작스러운 Microsoft 365 서비스 중단 시, 주요 문서들(법률 문서, 재무 문서 등)에 대한 접근이 어려움

해결 방안

- 백업 저장소의 추출 옵션을 사용함으로써 주요 파일들을 다운로드



Carbonite Endpoint

Overview

주요 고객 과제

45%의 비즈니스 데이터

기업이 통제하지 못하는 디바이스에 존재

72%의 임직원

허가되지 않은 무료 파일 공유 서비스를 사용함

분실 혹은 도난 당한 디바이스에 의한 손해:

연간 40억원

사이버 보안

데이터 보호를 위한 최우선 과제

Source: Pushan Rinnen & Robert Rhame, Critical Capabilities for Enterprise Endpoint Backup, Gartner, Inc., 2015

Carbonite® Endpoint

Carbonite® Endpoint는 고객의 Endpoint의 데이터를 효과적으로 보호

- **유연한 적용 옵션**
  On-prem 혹은 퍼블릭 클라우드 또는 Carbonite 클라우드에 백업
- **빠른 캐쉬 기능**
  분산된 네트워크에서 대역폭 소비 최소화
- **글로벌 위치 추적**
  분실 혹은 도난 당한 Endpoint의 위치 추적
- **데이터 손실 최소화**
  원격으로 분실 혹은 도난 당한 Endpoint의 데이터 삭제
- **강력한 암호화 및 중복 제거**
  Private Key를 활용하여 저장되거나 이동 중인 데이터를 암호화하여 데이터 보호

보안을 위한 핵심 요점 정리

01 입증되고 체계적인 사이버 보안 전략 수립 및 사용

02 사용자 보안 교육은 필수

03 원격 연결에 대한 모니터링 및 정책 수립

04 사용하지 않는 것에 대해 비활성화

05 저장소 및 패치 관리

06 다중 백업

07 강력한 암호 정책

08 끊임 없는 위협 관련 정보 습득

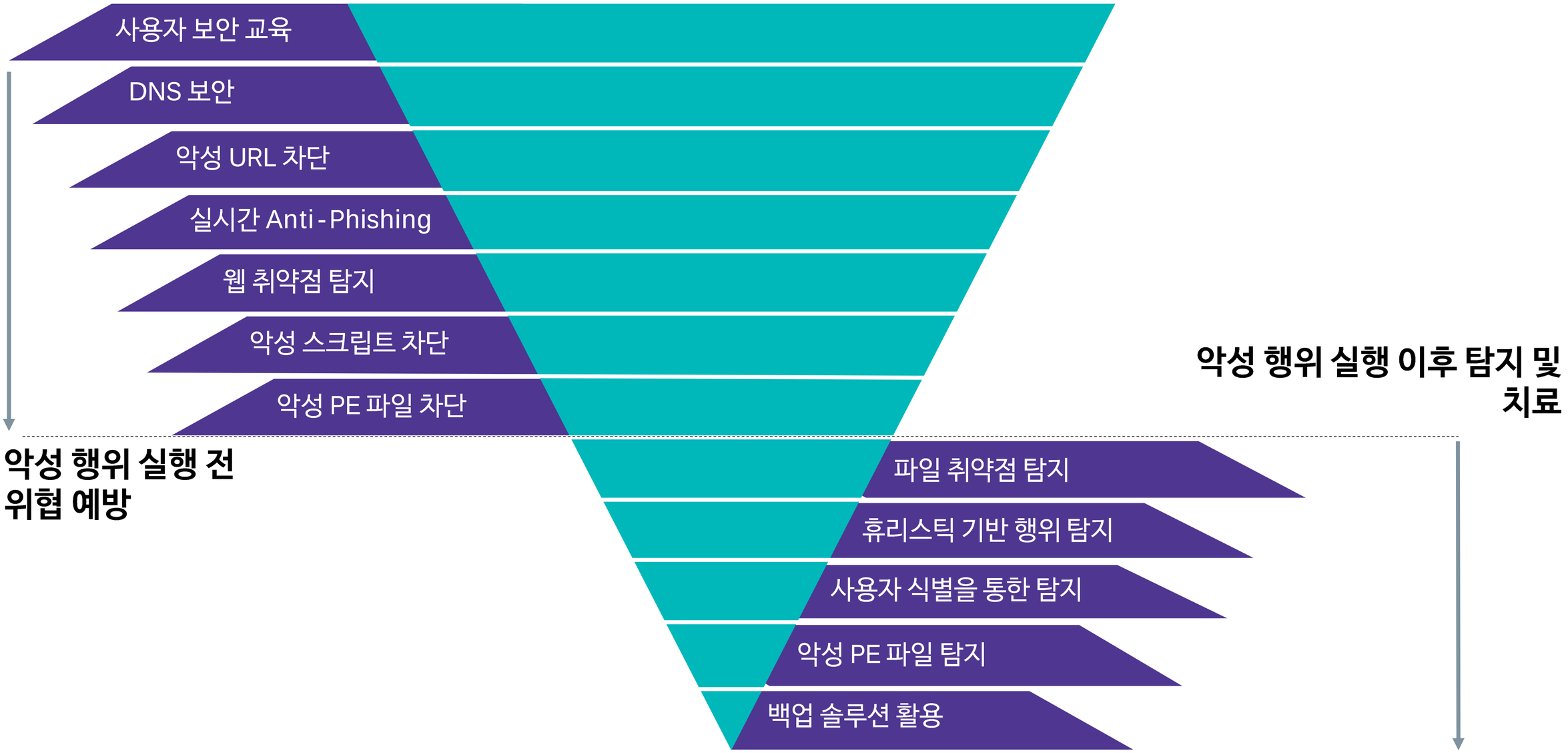
사용자 부주의로 인한 공격

01 Necessary:
"사람"이 보안에 있어서 가장 취약한 부분임

02 Proven:
사용자 교육은 리스크를 줄여주는 효과가 있음

03 Best Practice:
사용자 보안 교육은 많은 기업들에게 **필수** 사항임

Multi-Layered 보안 정책



opentext™

감사합니다

Contact

Phone 02-2185-1054

Mail krmarketing@opentext.com

twitter.com/opentext

facebook.com/opentext

linkedin.com/company/opentext

opentext.com