Trellix

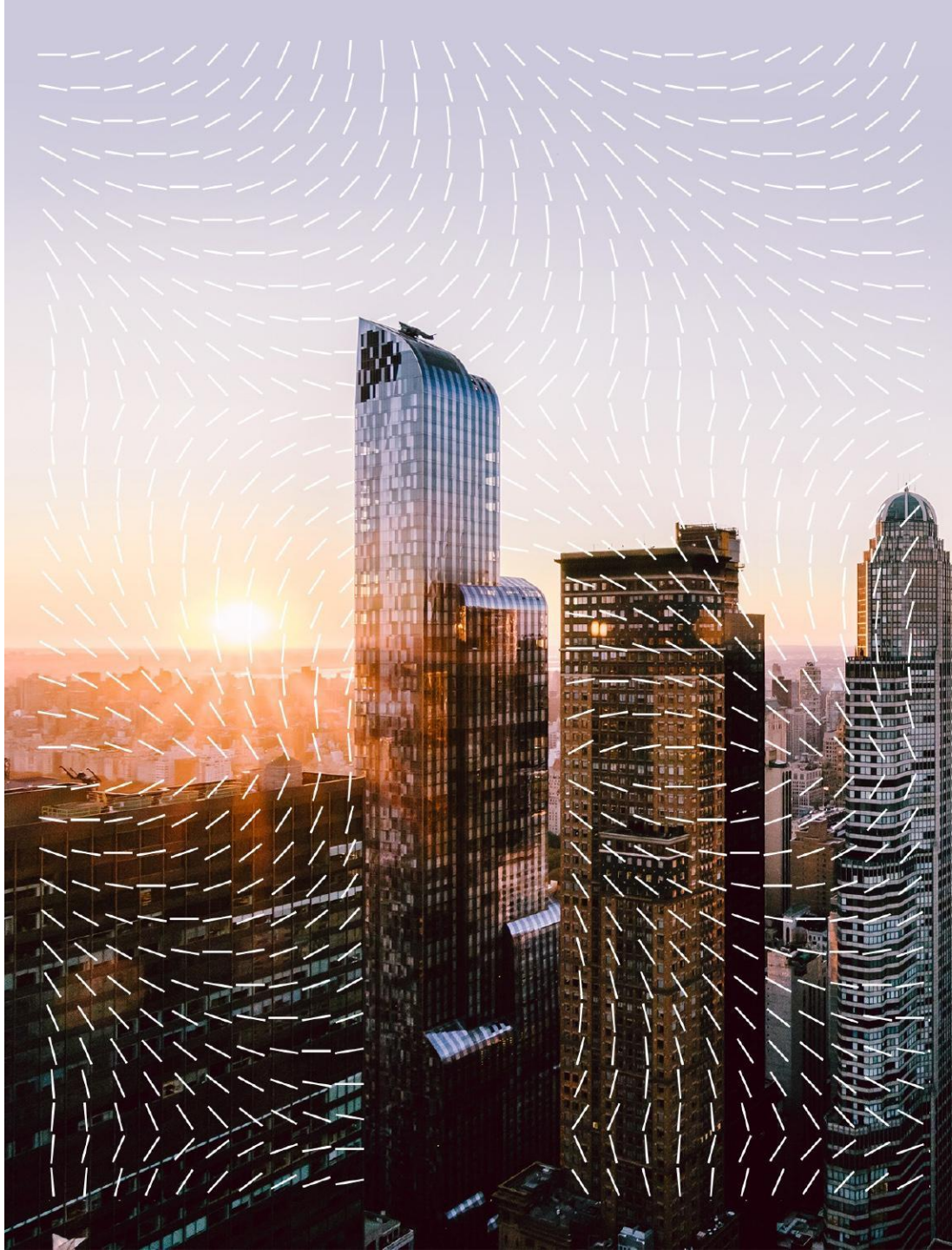
Hướng tiếp cận thành công để bảo vệ, chống thất thoát dữ liệu

Trellix's successful approach to implementing Data Loss Prevention

T.p Hồ Chí Minh 26/8/2022

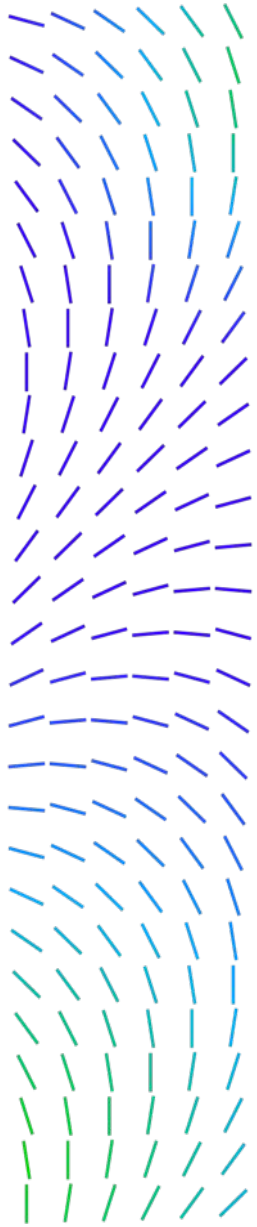
Vũ Ngọc Anh – Senior SE

Trellix Vietnam team



Nội dung

- Số liệu nghiên cứu từ các chuyên gia
- Kiến trúc bảo vệ, chống thất thoát dữ liệu của doanh nghiệp
- Cách tiếp cận để triển khai thành công
- Bảo vệ dữ liệu trong công tác vận hành của SOC



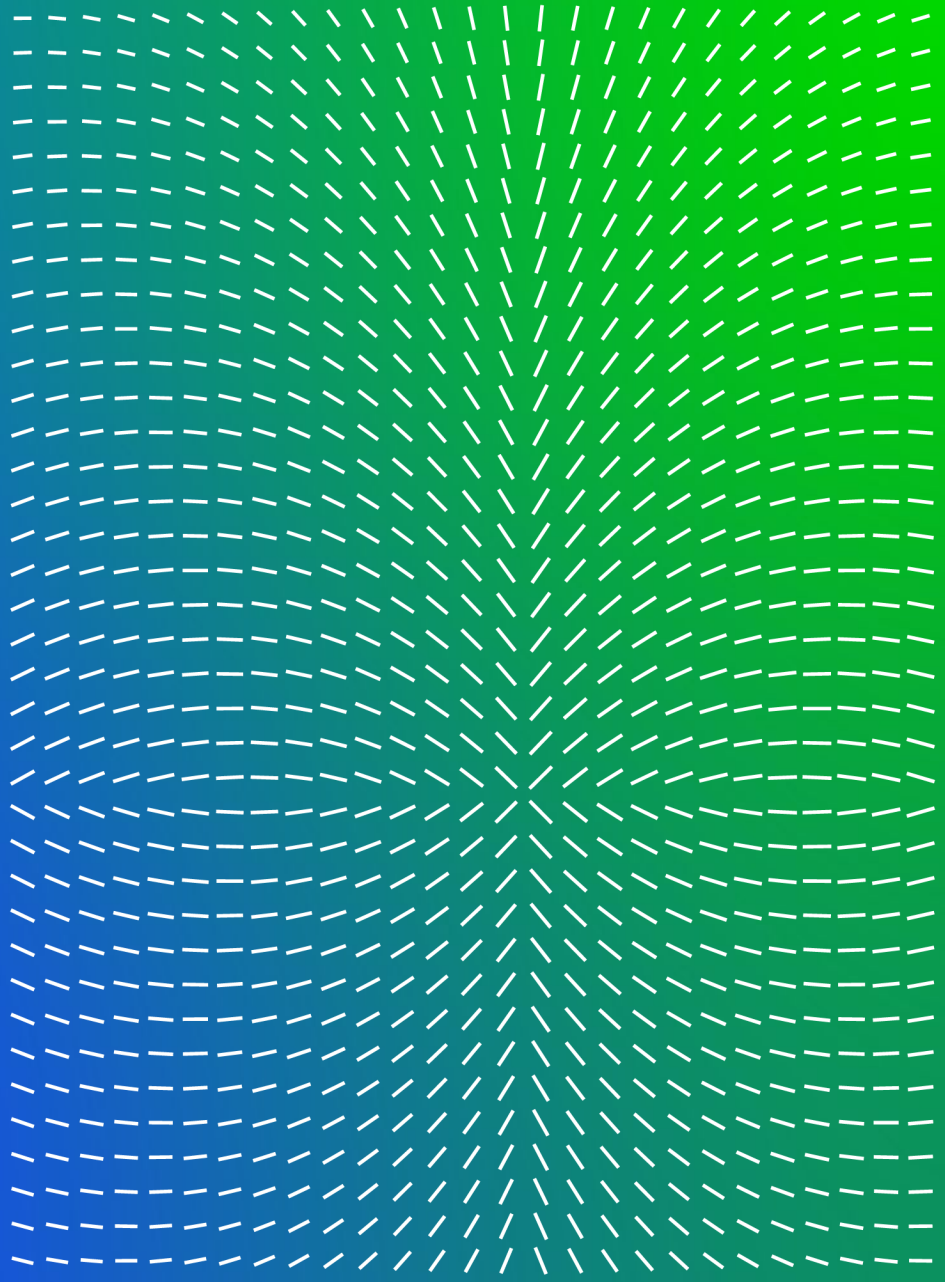
Trellix

Trellix

Số liệu nghiên cứu từ các chuyên gia

Số liệu khảo sát của Học viện Ponemon năm 2018 và 2015 từ hơn 2000 chuyên gia làm bảo mật ở các doanh nghiệp khắp toàn cầu

đã từng có sự cố xâm phạm dữ liệu trên



Trellix | Always Adapting. Always Learning.

Số liệu thống kê từ các chuyên gia

Who wants the data?

57% External actors

43% Internal actors

What external groups were responsible for your data breaches?

What internal groups were responsible for your data breaches?

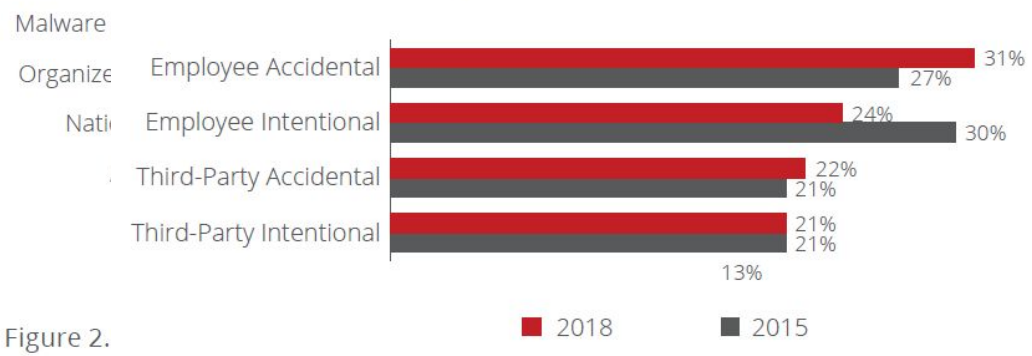
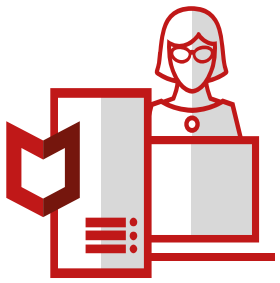


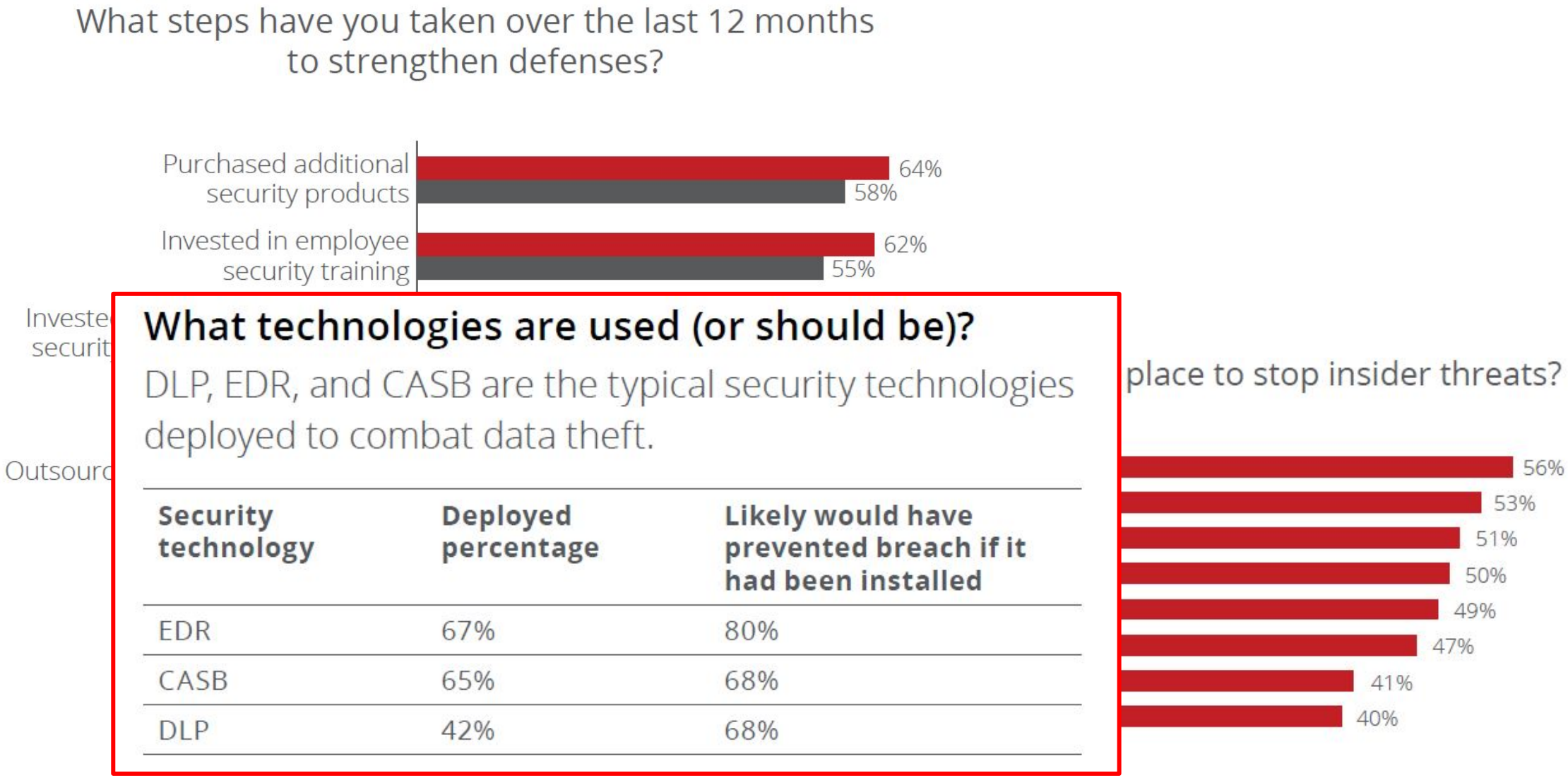
Figure 2.

Ponemon Institute 2018 and 2015 Surveys



Unified anagement

Trellix



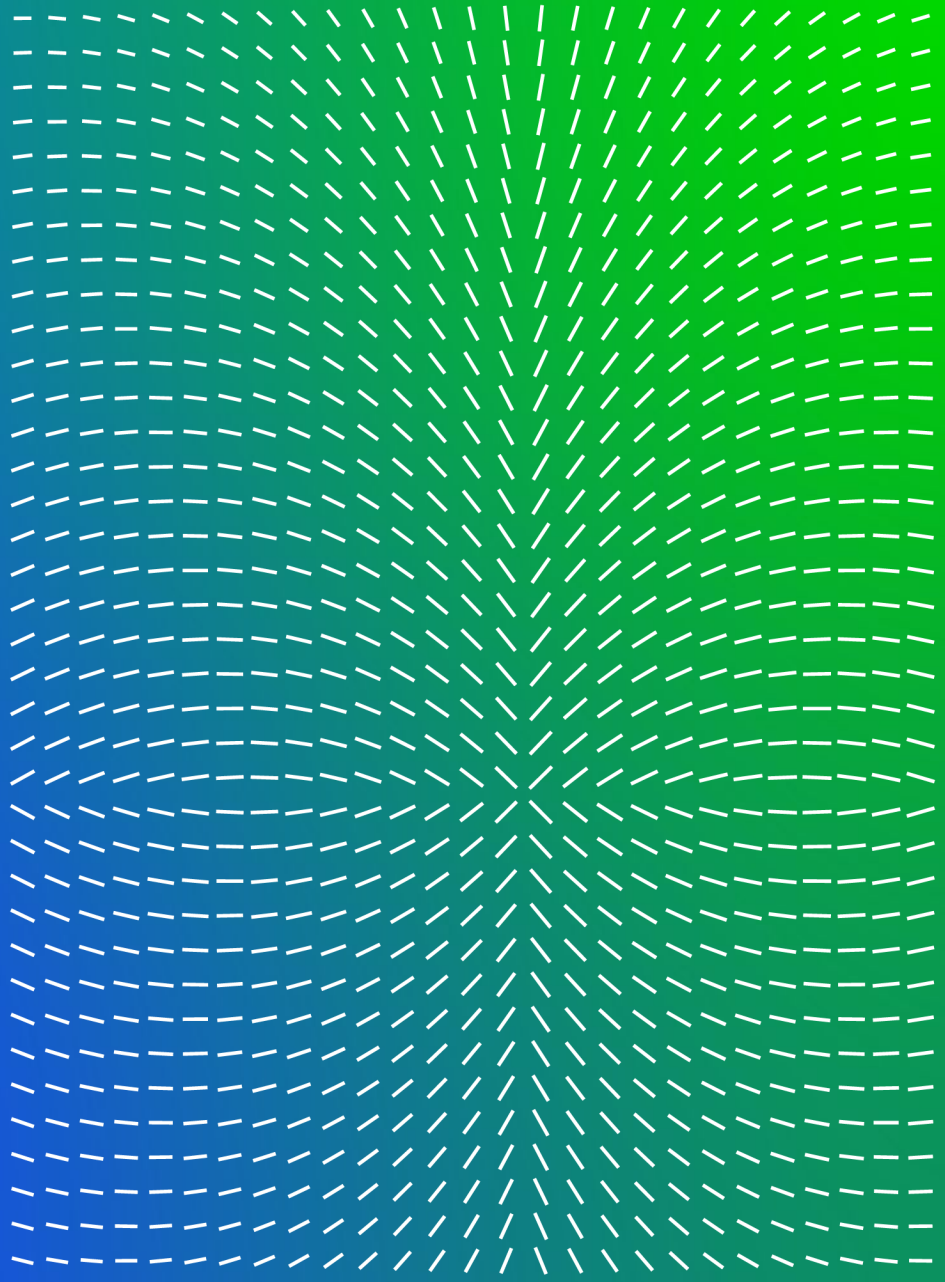
Security technology	Deployed percentage	Likely would have prevented breach if it had been installed
EDR	67%	80%
CASB	65%	68%
DLP	42%	68%

Figure 15. Insider threat detection processes.

Trellix

Trellix

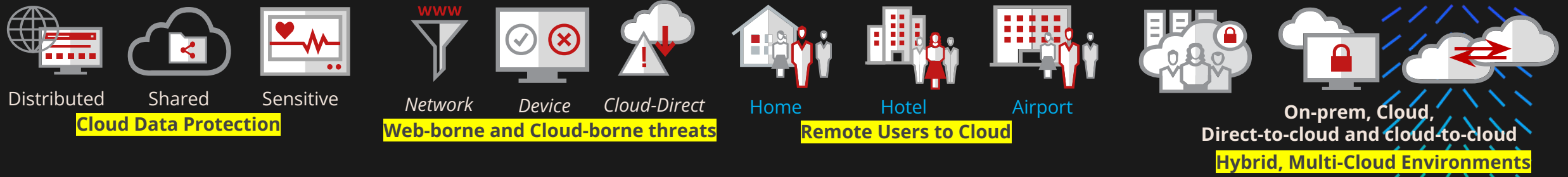
Kiến trúc bảo vệ dữ liệu của tổ chức, doanh nghiệp



Trellix | Always Adapting. Always Learning.

Bảo vệ tổng thể và thống nhất

Increase business agility and resiliency with more effective device-to-cloud security



Consistent across platforms

Threat Prevention

Stop advanced threats before they impact your organization.
(e.g., ransomware, phishing, fileless, apts,...)

Data Protection

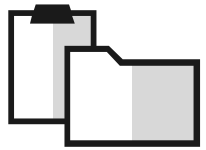
Apply persistent, comprehensive data protection from device to cloud.

Intelligent defense

Proactive Threat Prioritization | Predictive Security Posture Assessment | Preemptive Security Actions

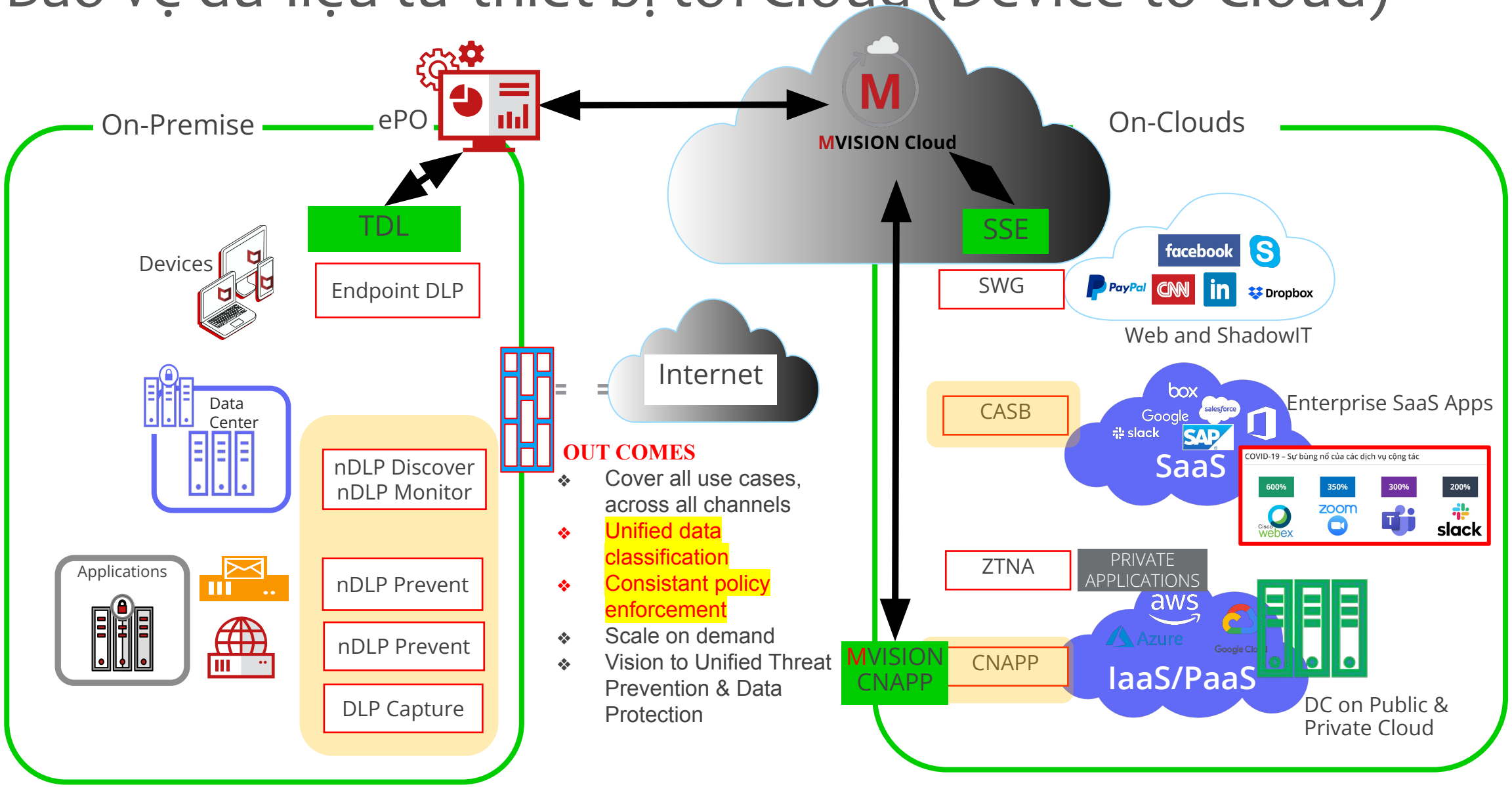
Efficient security operations

Bảo vệ, chống thất thoát dữ liệu trên tất cả các vector

Data Types	Data Loss Vectors				Solution
Data-in-Motion *101101100110101001*	 Email/IM	 Web Post	 Network Traffic	 Cloud	→	DLP Prevent DLP Monitor MVISION Cloud
Data-at-Rest 011001101010011011	 File Share	 Database	 Desktop/Laptop	 Cloud Storage	→	DLP Discover Drive Encryption MVISION Cloud
Data-in-Use 1011011001101001	 Removable/Devices	 Email/IM	 Collaboration	 File & Clipboard	→	DLP Endpoint File and removable Media Encryption Device Control MVISION Cloud

Trellix

Bảo vệ dữ liệu từ thiết bị tới Cloud (Device-to-Cloud)



OUT COMES

- Cover all use cases, across all channels
- Unified data classification
- Consistant policy enforcement
- Scale on demand
- Vision to Unified Threat Prevention & Data Protection

Trellix

Điều tra phân tích và tối ưu chính sách

Forensic and learning ability

Company

Egress Out

DLP Policies

PCI
HIPAA
Intellectual Properties
Acceptable Use

All Matches

Internet

- Mine data with Google-like search capabilities
- **Forensic search** of historical data
- **Bonus** = Help catch theft of critical data

Traditional Vendor

- False negatives destroyed
- Cannot LEARN and adjust policies
- Assumes you know what to protect

Violations Database

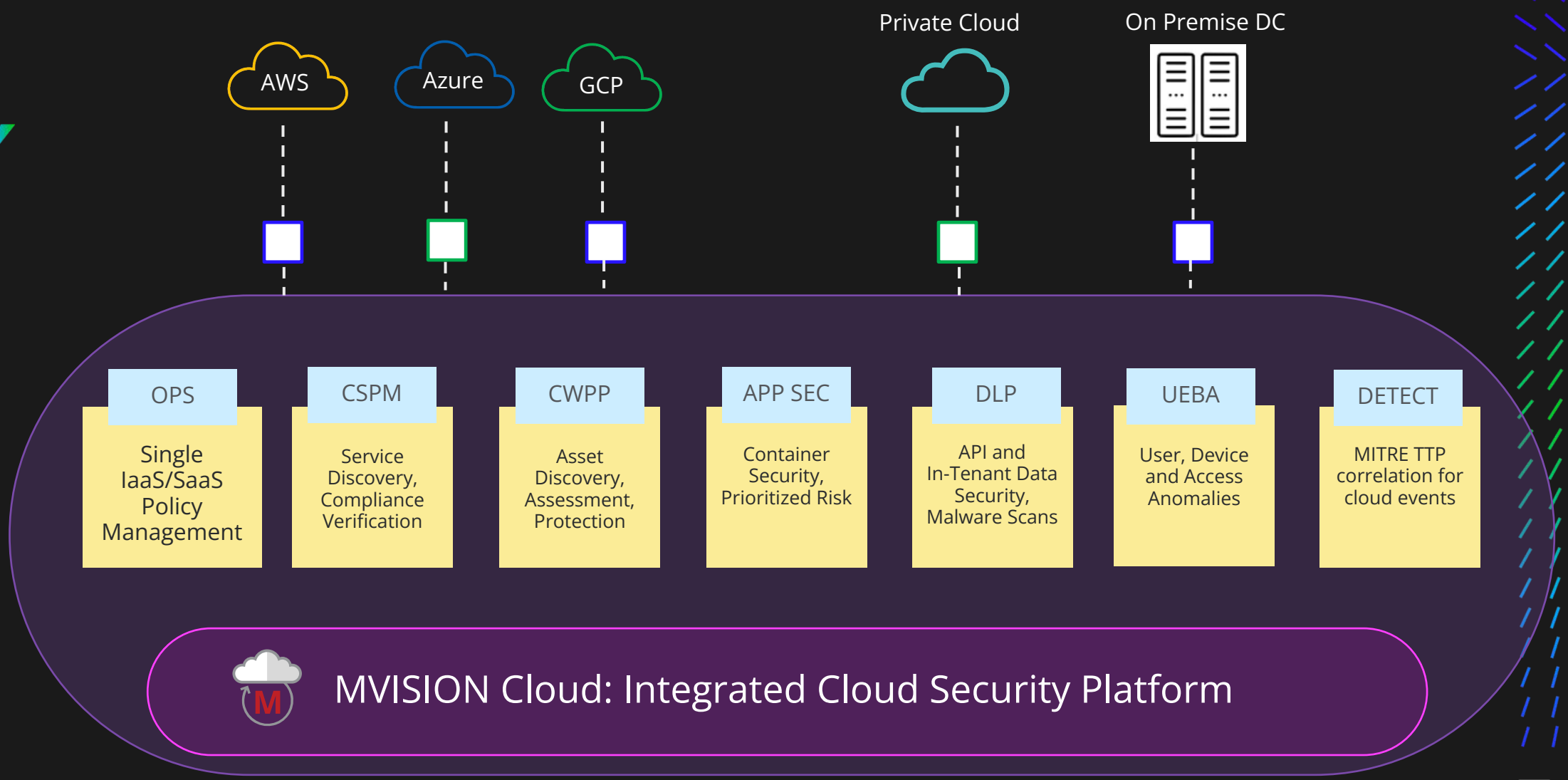
- **Pre-set Policies**
- **Dashboard reports**
- **Distributed notification of violations and reports**

Trellix DLP Capture Database

- **Everything captured**
- **“Information gap” solved**
- **Ability to LEARN from the past**

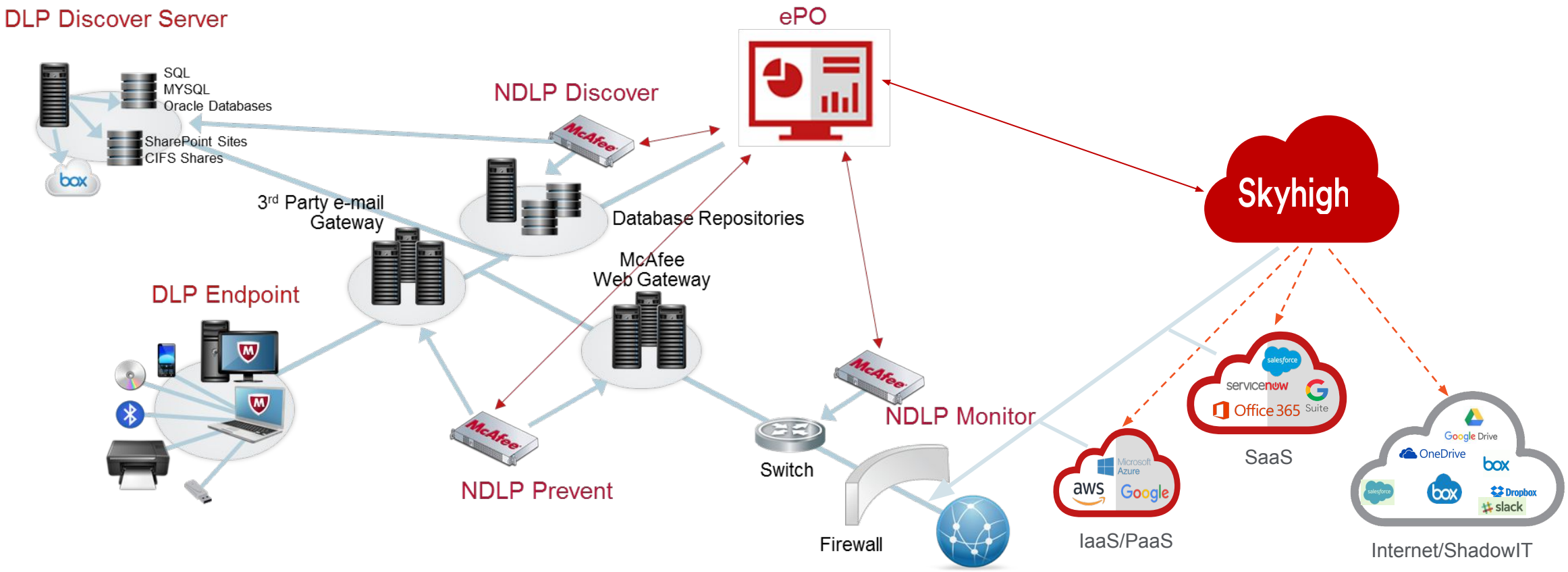
Trellix

Bảo mật tập trung cho nhiều Cloud – MVISION Cloud



Quản trị và vận hành tập trung

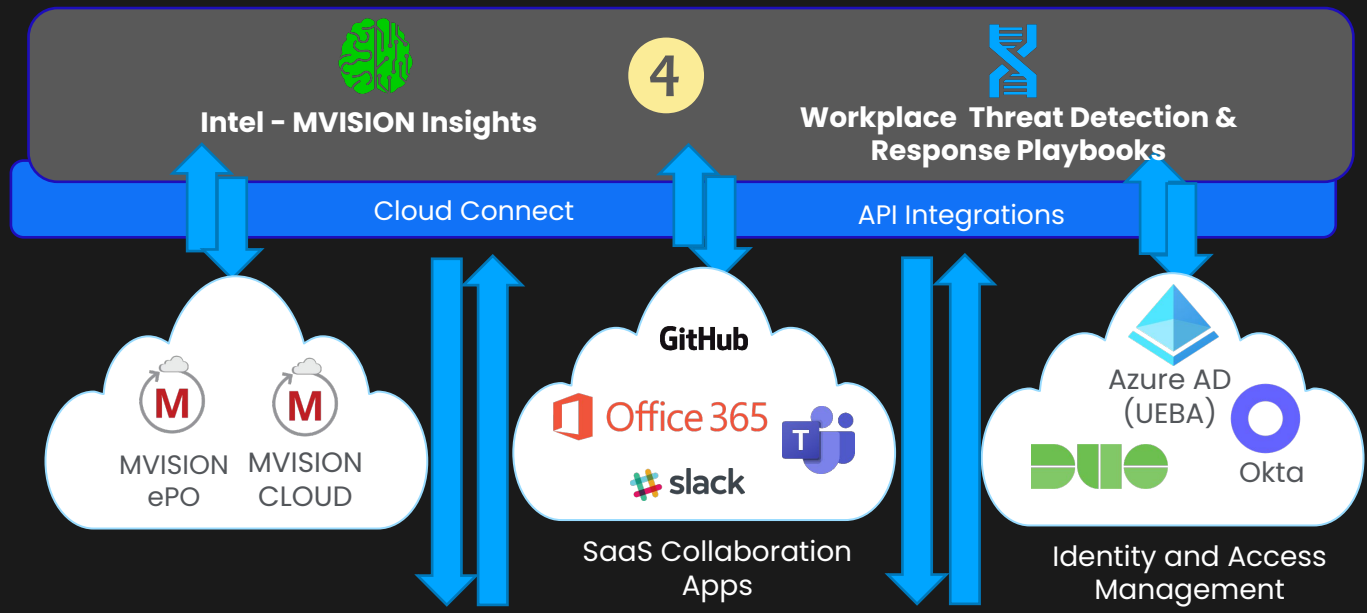
Đơn giản hóa bằng chia sẻ chính sách phân loại và bảo vệ dữ liệu



Trellix

Lộ trình triển khai các giải pháp

Sec Ops Platform (Backend)



Workplace XDR Sensors (Frontend)

1 Endpoint
Endpoint Security & EDR
Mobile Security
Device Control

Detection-on-Demand
Endpoint File Analysis
Messaging Threat Analysis
Collaboration Threat Analysis

1
4
NX/NSP
Network Threat Analysis
Network Intrusion Prevention
Network Anti-Malware

1 Email Security
Business Email Compromise
Phishing and Spam Protection
Email Anti-Malware Protection

2 Data Protection
Data Classification
Endpoint DLP
Network DLP: Discover, Prevent, Monitor, Capture
Encryption and FRP

3 UCE
SSE integration for Cloud access, data and Network Protection

Partners (Not Exhaustive)

Phantom, splunk>, IBM Radar, SWIMLANE, MISP Threat Sharing, MANDIANT, THREATQUOTIENT

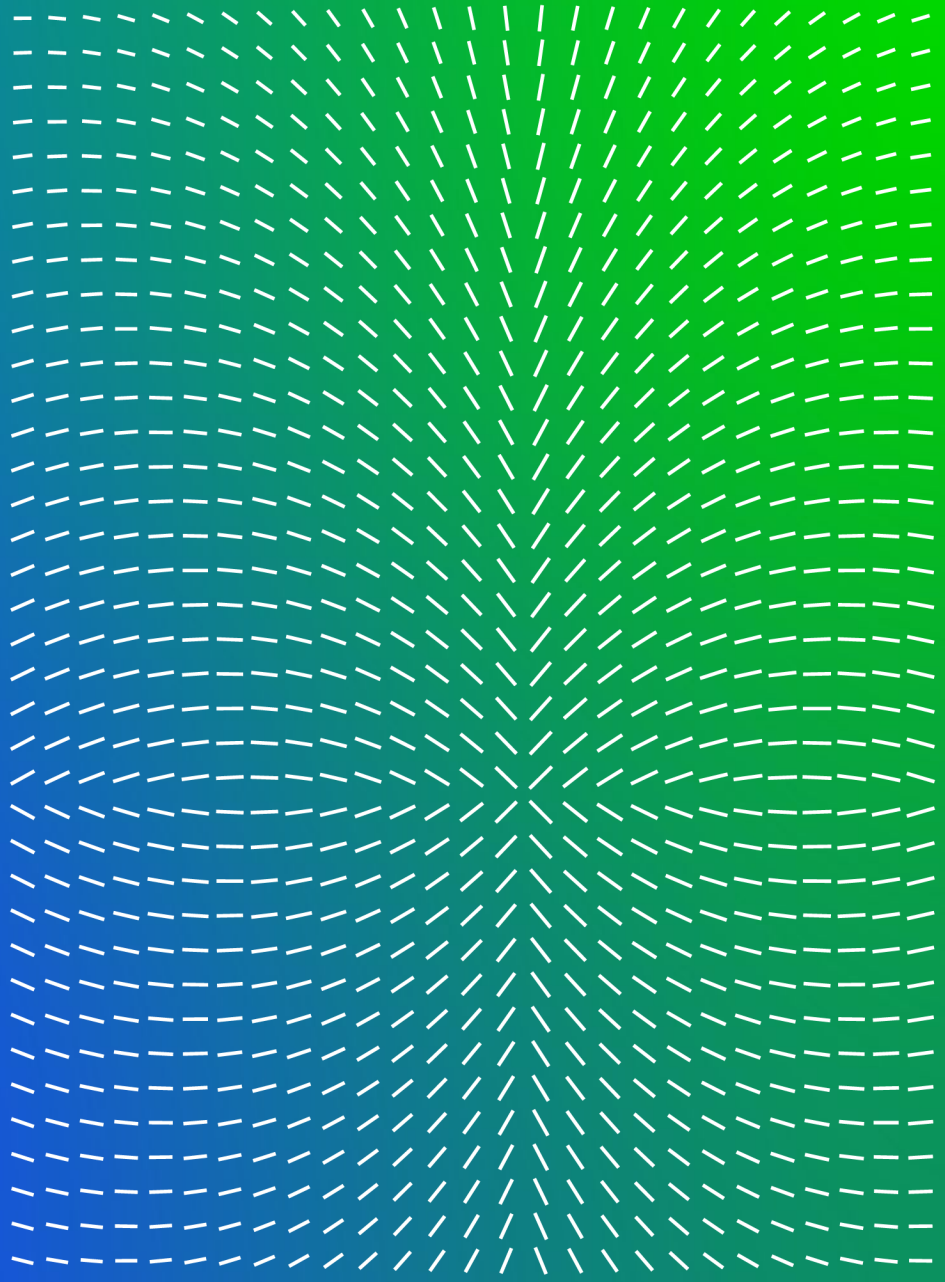
70+ Partners
650+ Parsers
150+ Plug-ins
75+ Cloud Connectors

aws, iboss, Attivo Networks, okta, Microsoft, TheHive, CYBERARK, ixia, slack

Trellix

Trellix

Cách tiếp cận để triển khai thành công



Trellix | Always Adapting. Always Learning.

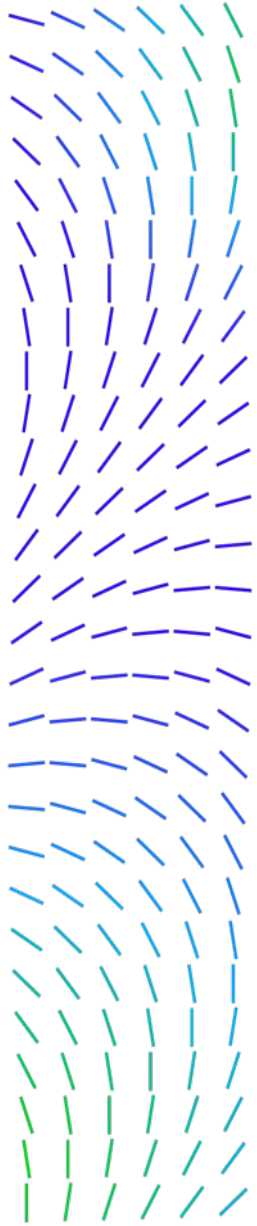
Hướng tiếp cận thành công

Quản lý rủi ro - Risk-based	Rủi ro sẽ không mất đi, chỉ có thể giảm đi, hoặc chuyển đi	Nguyên tắc 80/20	Tập trung: xác định mục tiêu quan trọng nhất, dữ liệu cần bảo vệ nhất, việc làm hiệu quả nhất
Gieo hạt - Seeding	Từ các đơn vị có tài sản/dữ liệu có nhu cầu bảo vệ nhất trước	Từ các đơn vị có tính tuân thủ tốt nhất trước	Triển khai - Giám sát - Tối ưu - Áp dụng
Chính sách, quy trình - Con người - Công nghệ	Chính sách, Quy trình, Hướng dẫn rõ ràng	Đào tạo nhận thức	Công nghệ

Trellix

Các mục tiêu quan trọng

- Kiểm kê, nhận diện, phân loại dữ liệu quan trọng, cần bảo vệ
- Huấn luyện nhận thức cho người dùng
- Bảo vệ các dữ liệu quan trọng nhất: phân loại, mã hóa
- Ngăn chặn việc mất mát dữ liệu hàng loạt
- Ngăn chặn việc lộ lọt dữ liệu qua các kênh chính: email, web, USB
- Ngăn chặn việc lộ lọt dữ liệu do vô ý
- Điều tra việc thất thoát dữ liệu



Trellix

Phương pháp phân loại dữ liệu

Identify how you want to classify information

Organizational level

- Document internal entities (departments, divisions), then expand to external entities (partners, vendors, competitors, and so on)
- Classify information based on the data source and flows between entities

Based on applications

- Document applications used
- Classify information based on the data source and flows for each application; for example, Windows Explorer, web browsers, encryption applications, and email clients

Based on end users and clients (most difficult)

- Document roles and data access points for each individual in the organization; for example, top-down using the organizational chart
- Classify information based on data source and flows for each individual

Trellix DLP Classification *(Automatic Classification, Manual Classification)*

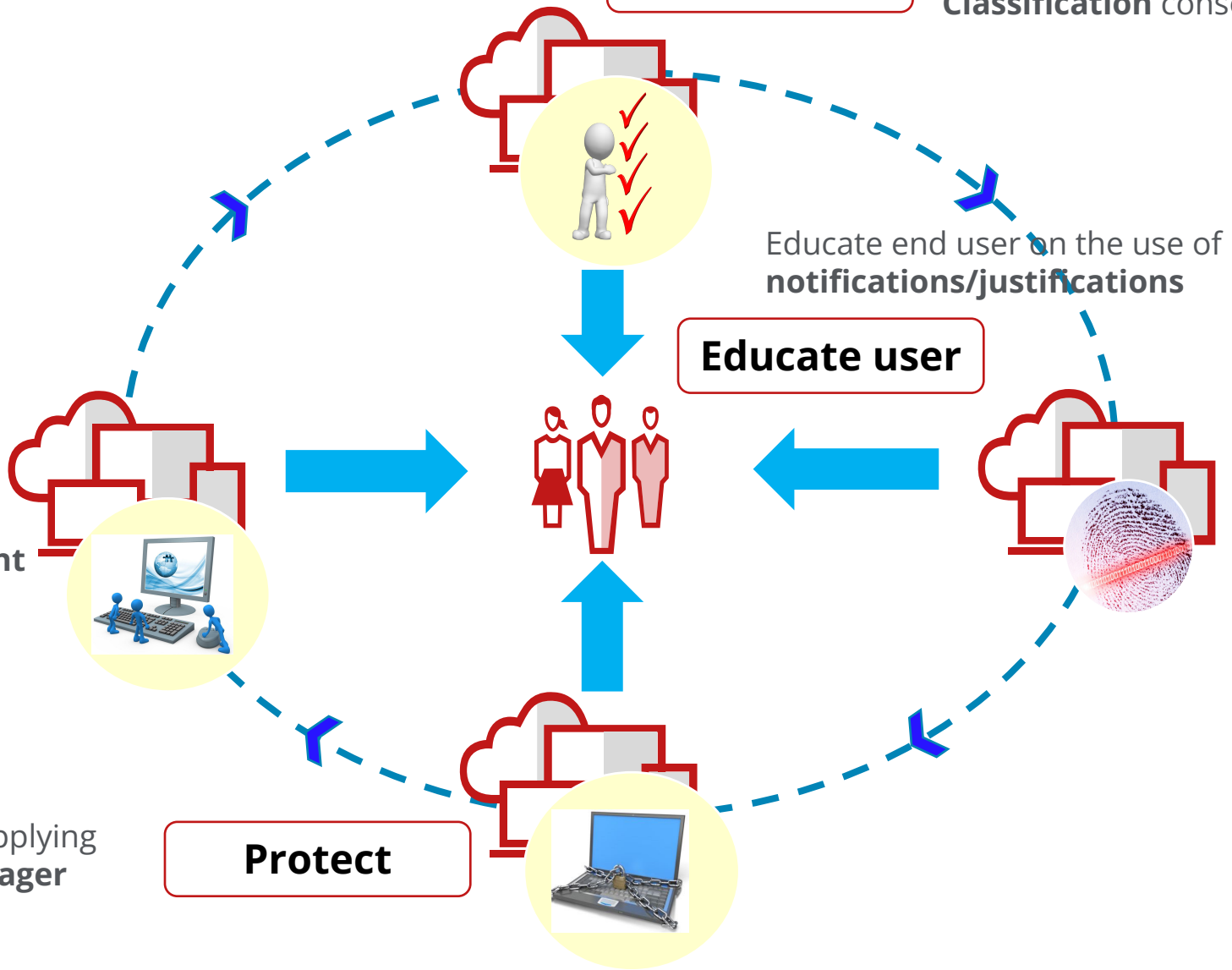
+

Data Classification tools *(Titus, Bolden James, AIP)*

Trellix

Đào tạo, huấn luyện nhận thức của người dùng

Trellix DLP Protection Process



Trellix

Hợp tác để triển khai và vận hành thành công

Customer

- Leader and business sponsor and involving the project
- RISK-BASE APPROACH MIND SET
- HR for Data Governance
- Review Endpoint Spec / OS/ Software
- Policy & Processes

Trellix

- Enterprise Architect and technologies best practice
- Professional Services for Deployment Reviewing and Optimizing
- Data Protection Program

Partner/Disty

- Experience project planning
- Data Classification (A)
- Deployment & Data Classification (B)
- On-boarding and Operation
- Technical Support

Architecting and Roadmap
Deployment Services
Data Classification (A)
Review and Optimize before go-live
Data Governance Workflow
Enhanced Support Program
Data Protection Program (A)

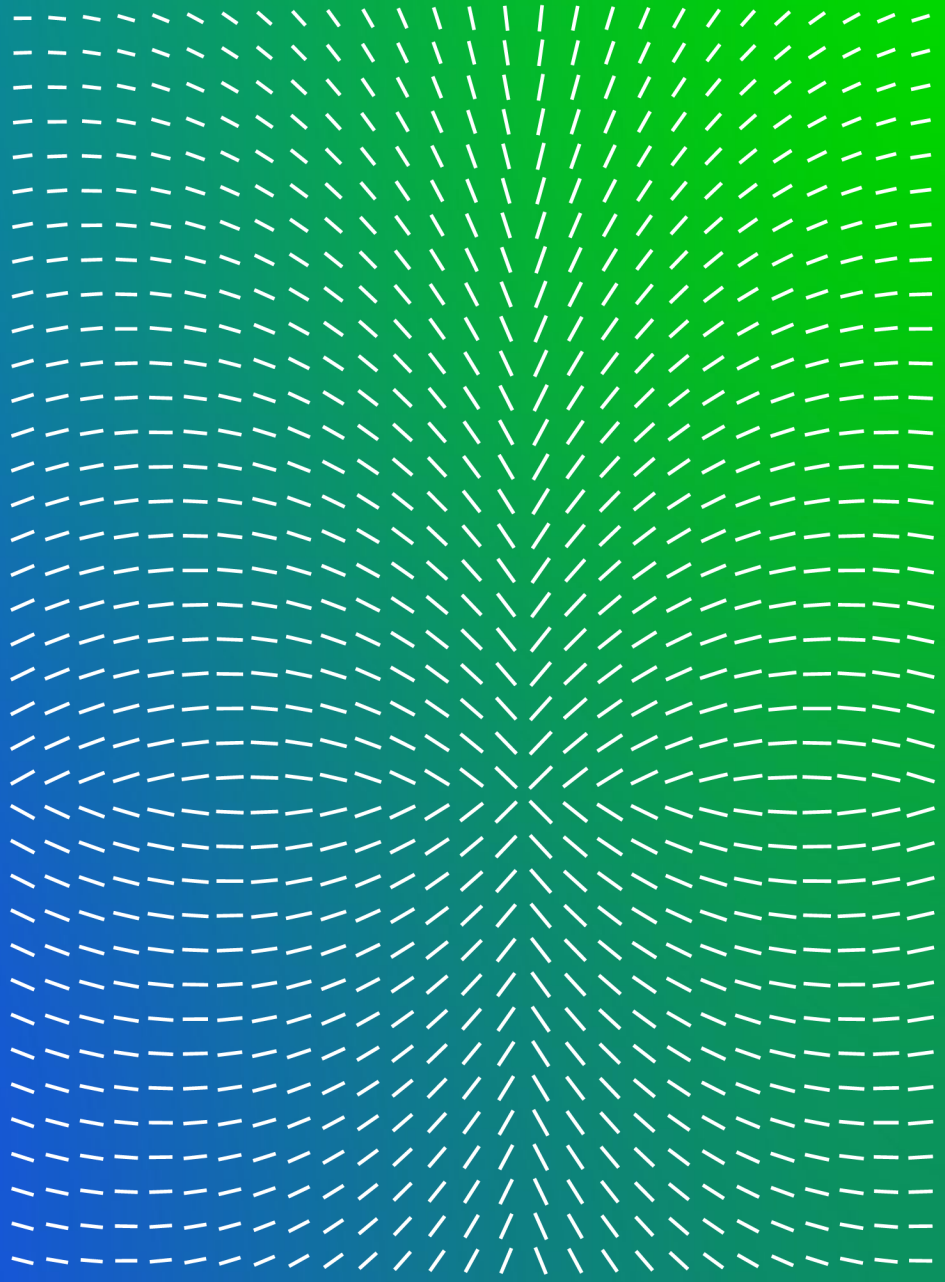
Trellix

Khách hàng và dự án đã triển khai ở Việt Nam

- Cơ quan nhà nước
- Ngân hàng, bảo hiểm, tổ chức tài chính
- Tập đoàn, doanh nghiệp đa ngành: bất động sản, du lịch, dịch vụ y tế
- Tập đoàn, doanh nghiệp sản xuất: phần mềm, ô tô,
- Tập đoàn, doanh nghiệp

Trellix

Bảo mật dữ liệu trong công tác vận hành của SOC



Trellix | Always Adapting. Always Learning.

Bảo vệ dữ liệu trong nền tảng XDR và SOC

Trellix **Unified Consoles**

Trellix **LAB**

- Threat Intelligence
- ML/AI
- Advanced Analytics
- Advanced Groups
- Playbooks

Trellix **Data Lake**

Trellix **Core Engines**

Intelligence Sandboxing - MVX™

- Trellix **Data Security**
- Trellix **Email Security**
- Trellix **Endpoint Security**
- Trellix **Network Security**
- Trellix **Cloud Security**

Trellix **Single Agent + Realtime Threat Intelligence Sharing (Open DXL)**

70+ Vendors
650+ Parsers
150+ Plug-ins
75+ Cloud Connectors

- Atlassian Jira
- AWS GuardDuty
- CB Endpoint
- Cisco Umbrella
- IBM Qradar
- Netskope
- Okta
- Palo Alto Prisma
- ThreatQ
- ServiceNow
- Symc Bluecoat
- Windows Defende

And hundreds more...

Trellix

Các bài toán lớn của vận hành bảo mật

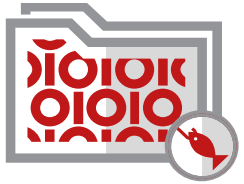
Actionable Threat Intelligence

Nhận diện và đánh giá năng lực phòng vệ, trinh sát và dự báo

Threat Management

Phát hiện và xử lý các mối nguy hại (Threat) – mã độc, tấn công

Pervasive Data Protection



Phát hiện và xử lý các nguy cơ và xâm phạm dữ liệu

Behavioral Analytics

Phát hiện và xử lý các hành vi bất thường, xấu của máy tính và người dùng

Thiếu hụt nguồn nhân lực, vị trí công việc và kỹ năng cũng như liên tục đào tạo
Tự động hóa, điều phối và phối hợp hoạt động

Trellix


THANK
YOU
MAAKE
TERMA KASIH
RAIBH MAITH AGAT
MULTUMESC
GRAZIE
MERCI
MOCHCHAKKERAM
GRAZIE
CHOKRANE
MATUR NUWUN
MATONDO
CHOKRANE
UA TSAUG RAU KOJ
DANK JE
RAIBH MAITH AGAT
SPASIBO
MAAKE
OBRIGADO
SPASIBO
WELALIN
JUSPAXAR
OBRIGADO
MATONDO
MERCI
ARIGATO
MOCHCHAKKERAM
OBRIGADO
SPASIBO
KIITOS
MOCHCHAKKERAM
SALAMAT
KIA ORA
MULTUMESC
CHOKRANE
SALAMAT
CAM ON BAN
MERCI
RAIBH MAITH AGAT
OBRIGADO
MOCHCHAKKERAM
ASANTE
UA TSAUG RAU KOJ
MOCHCHAKKERAM
KIITOS
OBRIGADO
DANK JE
VINAKA
NIRRINGRAZZJAK
MAMANA
MULTUMESC
KIITOS
DANKON
NIRRINGRAZZJAK
MOCHCHAKKERAM

thank you!

Trellix