Net++ TECHNOLOGY

NE VERUJ NIKOME 2023

DLP u Zero Trust okviru

Presentations are tools that can be used as lectures, speeches, reports, and more it is mostly presented.

Davor Perat

GOVORIĆE DANAS

VLADIMIR VUČINIĆ

Net++ technology

DUBRAVKO HLEDE

MBCOM Technologies

DIMITRIJE VELIČANIN

Net++ technology

DAVOR PERAT

MBCOM Technologies

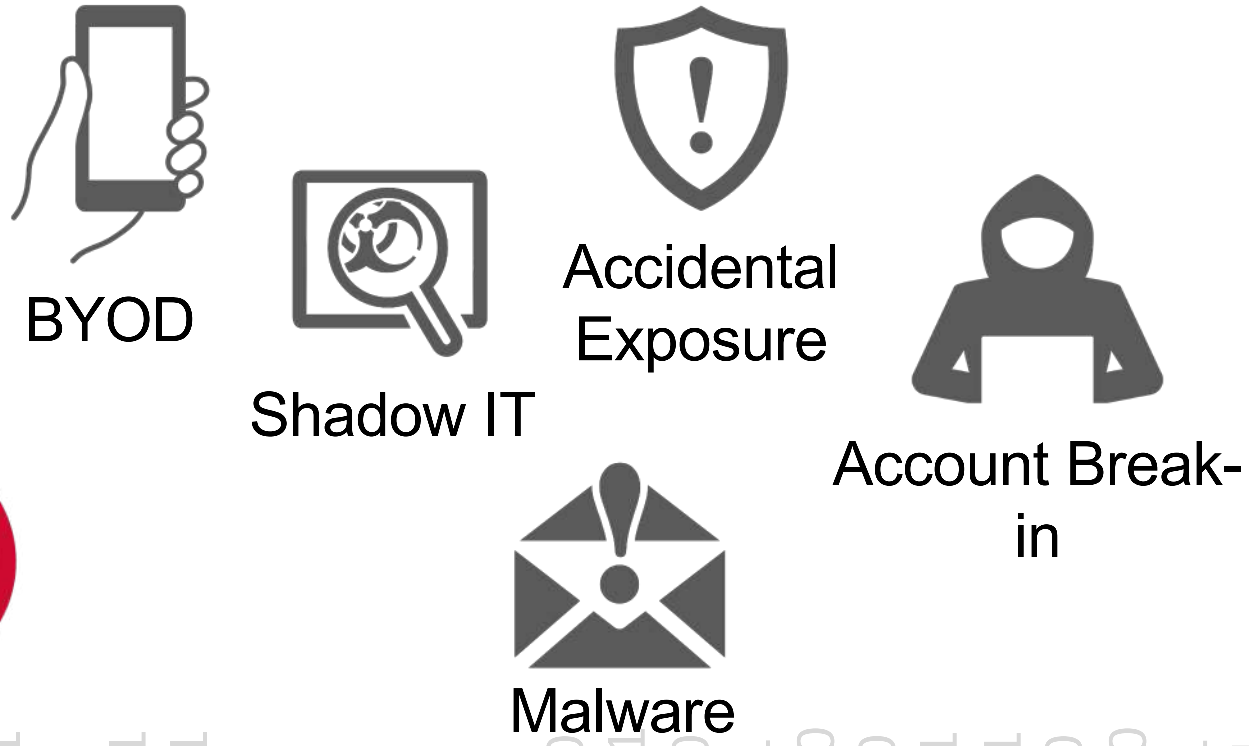
SRĐAN VRANIĆ

Co.Next

Data Loss & Cloud App Challenges

1. **Protect Data Everywhere (On-premises & cloud)**

2. **Secure Cloud Data by Securing the Cloud**



BYOD

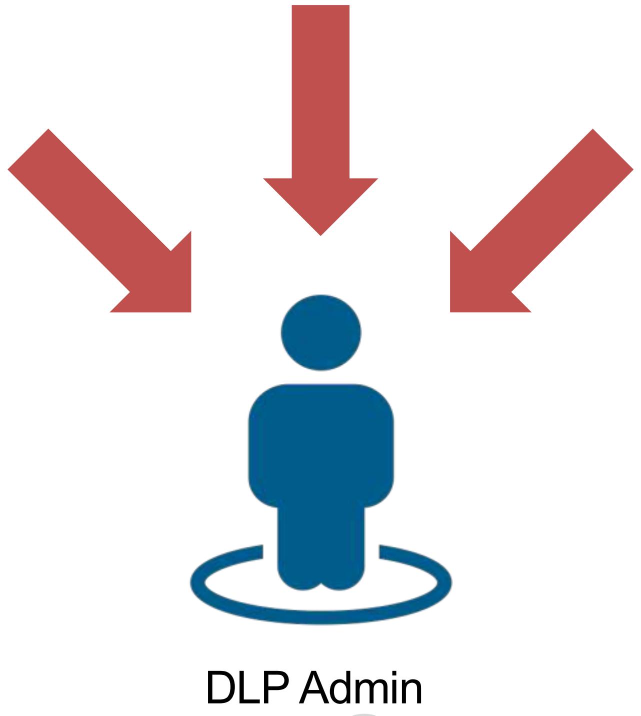
Shadow IT

Accidental Exposure

Account Break-in

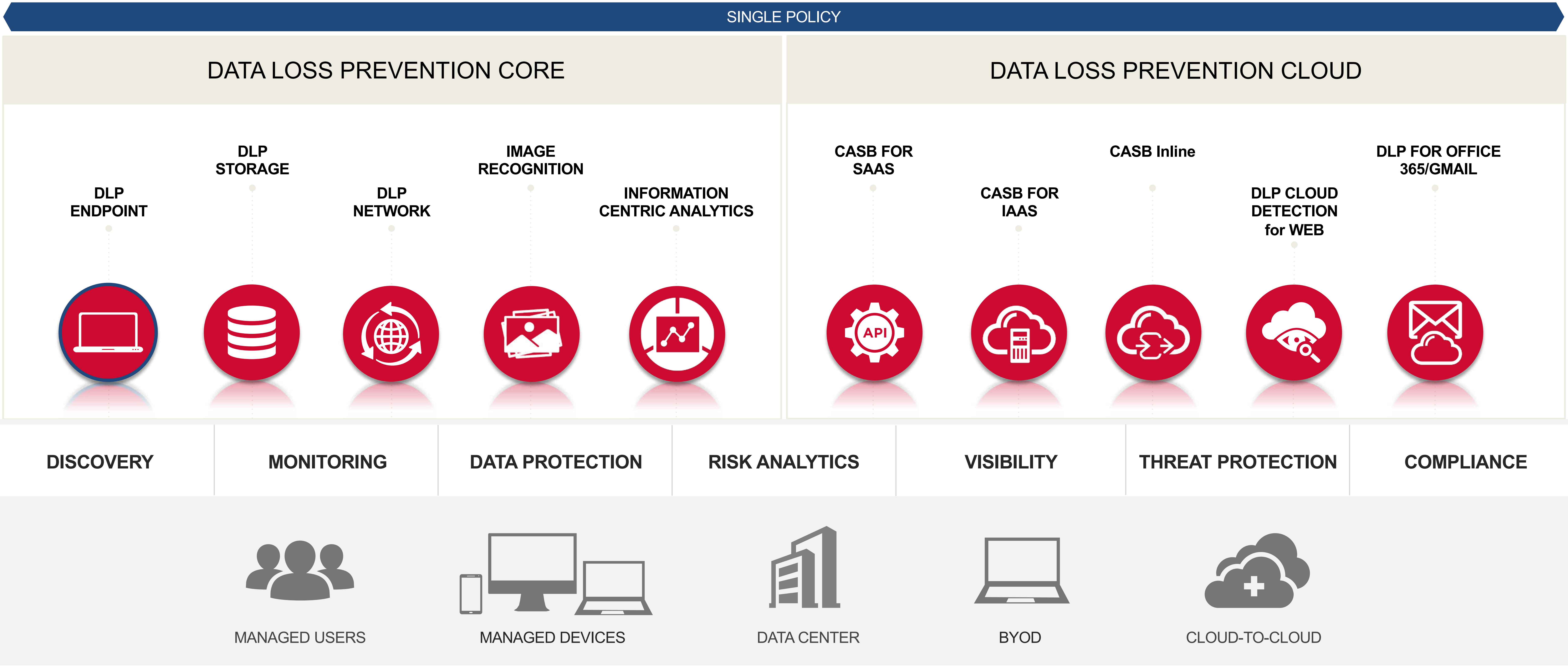
Malware

3. **Reduce Operational Demands on DLP Admins**



DLP Admin

Symantec Data Loss Prevention Solutions



SINGLE POLICY

DATA LOSS PREVENTION CORE

- DLP ENDPOINT
- DLP STORAGE
- DLP NETWORK
- IMAGE RECOGNITION
- INFORMATION CENTRIC ANALYTICS

DATA LOSS PREVENTION CLOUD

- CASB FOR SAAS
- CASB FOR IAAS
- CASB Inline
- DLP CLOUD DETECTION for WEB
- DLP FOR OFFICE 365/GMAIL

DISCOVERY | MONITORING | DATA PROTECTION | RISK ANALYTICS | VISIBILITY | THREAT PROTECTION | COMPLIANCE

MANAGED USERS

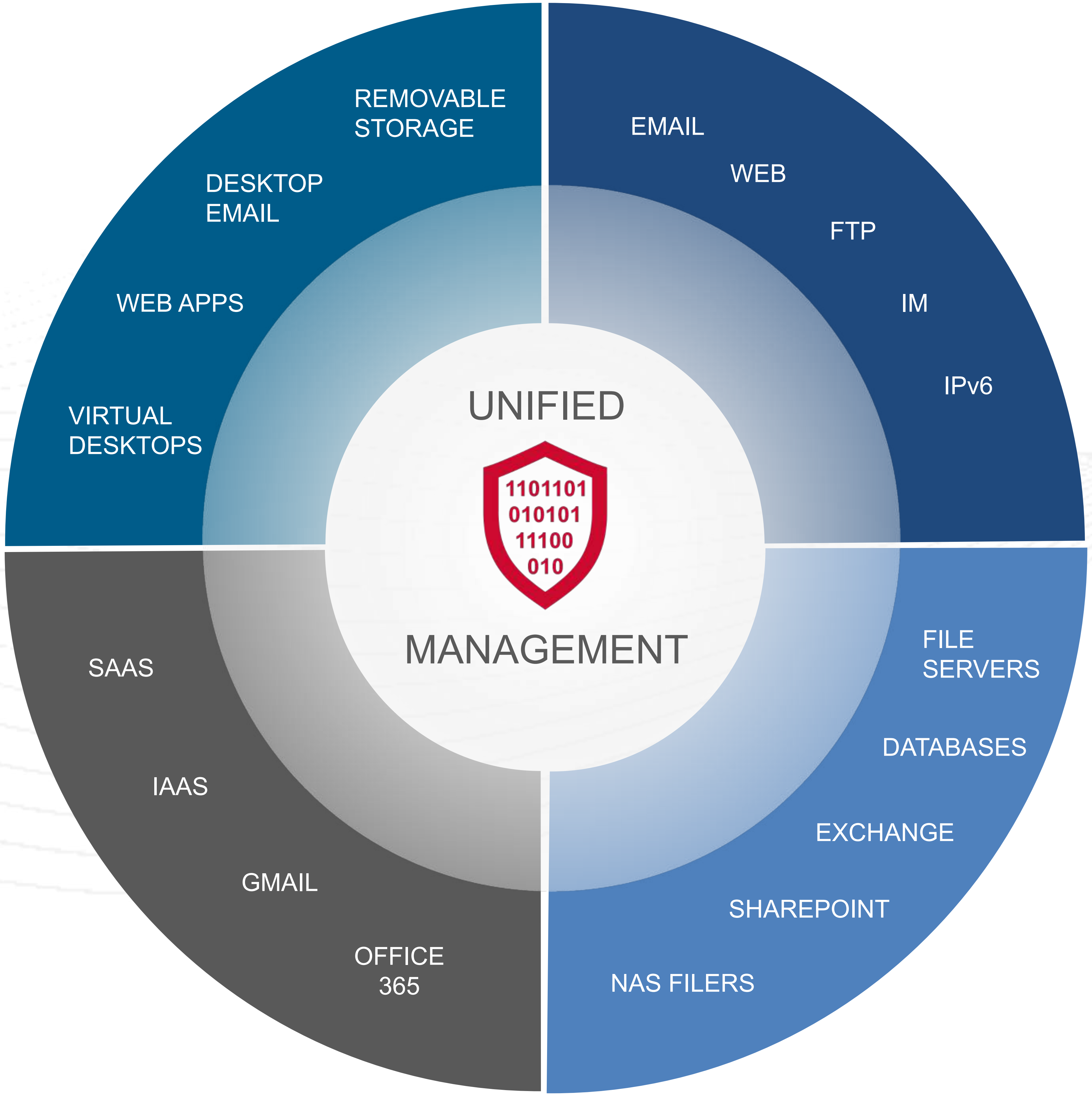
MANAGED DEVICES

DATA CENTER

BYOD

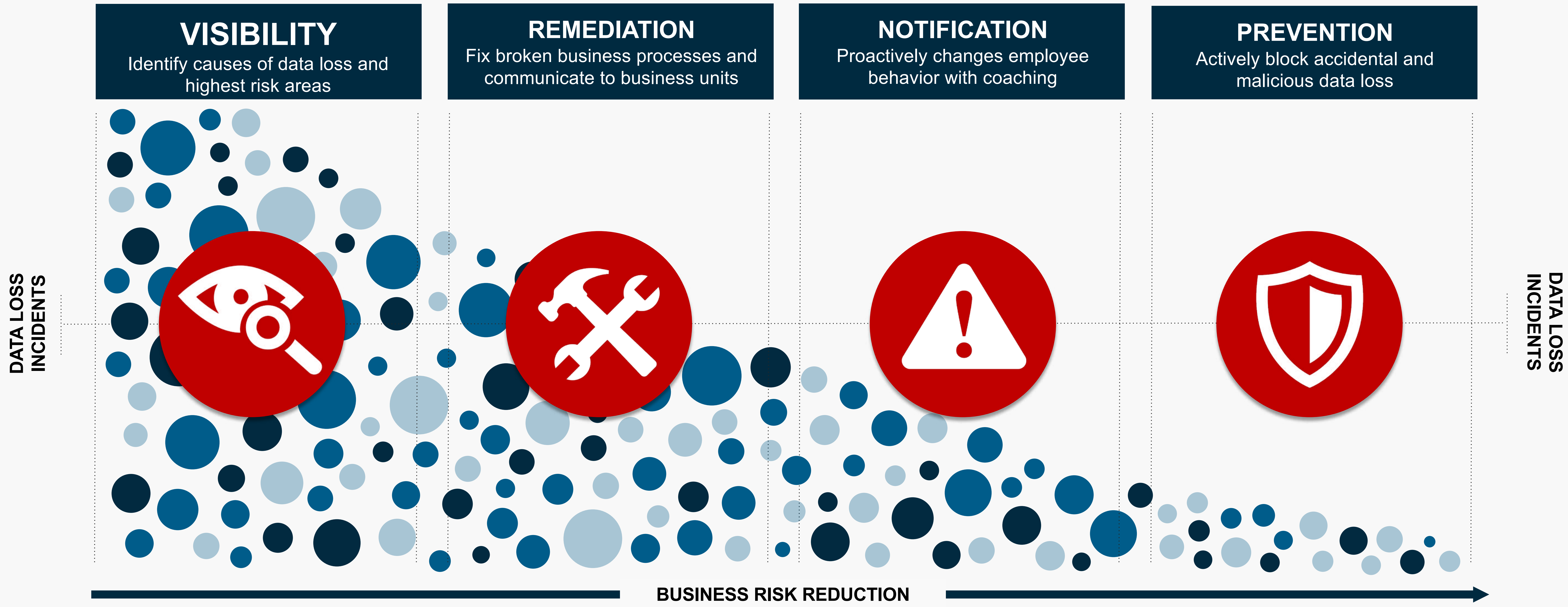
CLOUD-TO-CLOUD

Broadest Coverage of Data Loss Channels



Our Unique Approach

A proven four-phase methodology for business risk reduction



VISIBILITY
Identify causes of data loss and highest risk areas

REMEDIATION
Fix broken business processes and communicate to business units

NOTIFICATION
Proactively changes employee behavior with coaching

PREVENTION
Actively block accidental and malicious data loss

Multi-Layered Detection Catches What Others Miss

Provides high levels of accuracy and control with minimal false positives

DESCRIBED CONTENT MATCHING

SIMPLE TEXT

- Matches data identifiers, keywords, regexes
- Common pattern-based data

INDEXED DOCUMENT MATCHING

UNSTRUCTURED DATA

- Matches binary signature or contents of file
- Documents and files

EXACT DATA MATCHING

STRUCTURED DATA

- Matches only the values from your records
- Structured, tabular data

EXACT MATCH DATA IDENTIFIER

STRUCTURED DATA

- Matches only the values from your records
- High degree of accuracy for PII

SENSITIVE IMAGE RECOGNITION

IMAGES & FORMS

- Matches key points in forms and text extracted from images

VECTOR MACHINE LEARNING

NEW & CHANGING DATA

- Matches on similarity % to learned data
- Effective at recognizing patterns in unstructured data

90% of DLP is Incident Response

Reducing the time means getting it right

Right Metrics |

Prove Results to Execs and Auditors

Right Automation |

Resolution, Enforcement, Notification

Right Action |

1-Click Response

Right Person |

Route Incidents to Right Responder

Protect your data everywhere

Right Information |

5-Second Test

Right Order |

High Severity of Incidents First

Data Loss Prevention Core

Discovery, Monitoring, Protection & Risk Analytics for Your Hybrid Cloud Environment

DLP
ENDPOINT

DLP
STORAGE

DLP
NETWORK

IMAGE
RECOGNITION

INFORMATION
CENTRIC ANALYTICS

Protect Sensitive Data On-premises

On-premises protection across Endpoint, Network and Storage

PROTECTING THE ENDPOINT

Scans local hard drives and protects sensitive files and applications that users are storing on their laptops and desktops.

PROTECTS SENSITIVE DATA AT REST

DLP for storage finds confidential data by scanning network file shares, offers robust file protection capabilities and secures all of the exposed files

PROTECTS DATA IN MOTION

Monitors email and web traffic on your corporate network and protects sensitive data from being leaked to the Web.

Risk Analytics – ICA

Accelerated DLP Incident Management

Expedite triage by automatically filtering through the noise to prioritize the highest risk incidents for investigation

Advanced Analytics

Analysis of large, complex data sets to create clear visibility into those behaviours that demand immediate investigation and prioritization

Connecting the Dots

Integrated behavioral analytics capable of analyzing alerts and telemetry from diverse security sources, including DLP, CASB, WSS – connecting the dots between violations, users, accounts and assets.

Data Loss Prevention Cloud

CASB for SaaS
Discover and control Shadow IT in your organization with deep visibility across thousands of apps, and evaluate whether the apps & data meet all compliance requirements – GDPR, HIPAA. Govern access to critical data, protecting data at rest.

CASB for IaaS
Ensure visibility and compliance across your IaaS environments – AWS, Azure & GCP. Discover and continuously monitor the cloud environment for resource misconfigurations with CSPM.

CASB Inline
Govern Access to Critical Data, securing Data-in-Motion, protect against threats and malware and continuously monitor risk with UEBA capabilities

DLP for Web
Govern and control exposure of Critical Data via the web

DLP for Email
Govern and control exposure of Critical Data via when sent over Email when using i.e. O365 or Google Workspace (Gmail)

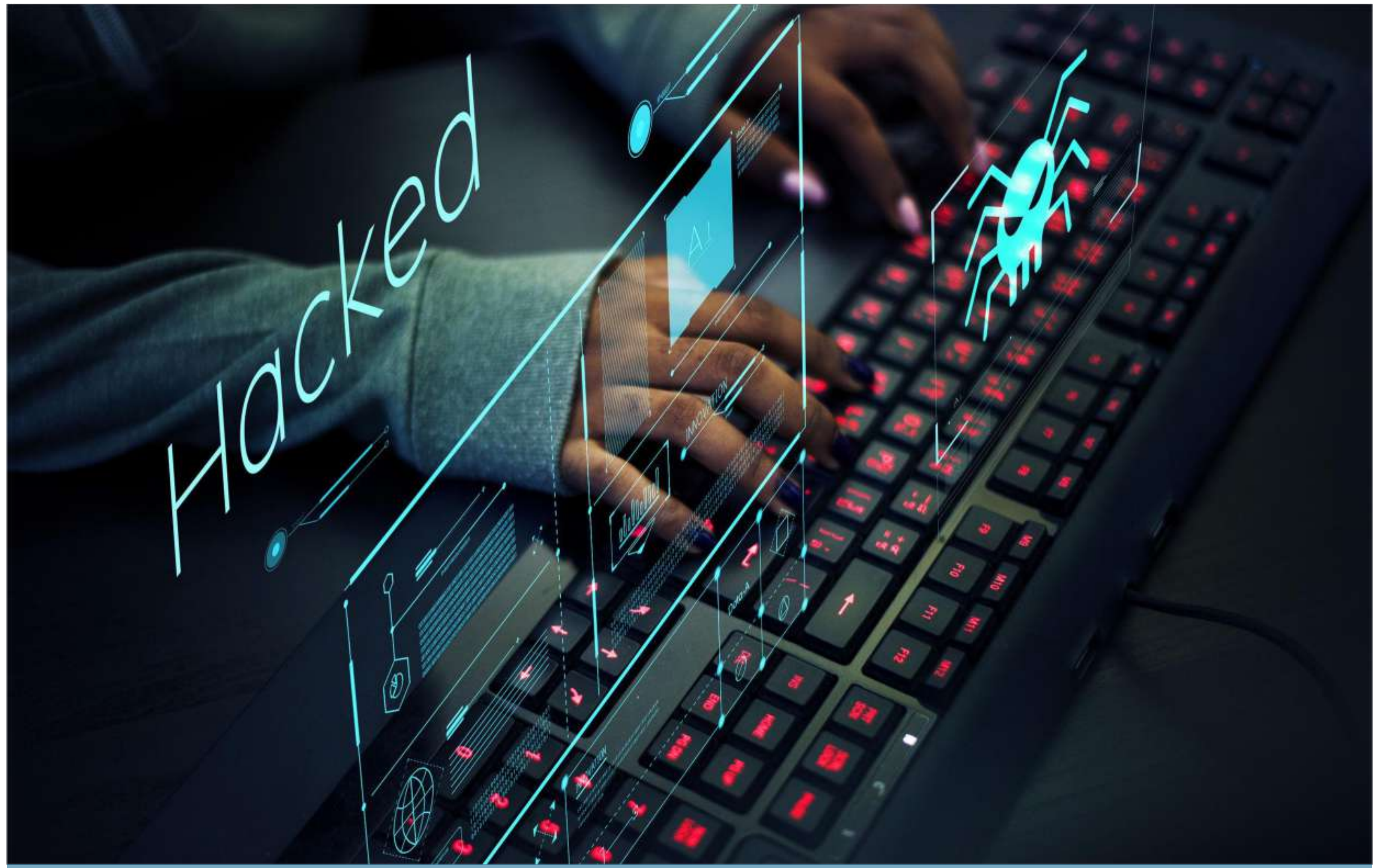
ADD-ON: Advanced Threat Protection

Safeguard your organization in the cloud with industry-leading threat protection. Secure your cloud accounts and transactions against malware with file reputation intelligence, A/V scanning, and sandboxing technologies.

ADD-ON: CloudSOC Mirror Gateway

Secure cloud access from unmanaged devices. Extend CASB controls to unmanaged devices or BYOD, giving them the same secure access to cloud apps as managed devices, with no need for an agent an

Discover and Mitigate Risk of Shadow IT



Challenge

Shadow IT spreads data across dozens of cloud services and applications, making it very hard to identify services, assess risks and control sensitive data.

Uncover Shadow IT

from proxy/firewall and assign a Business Readiness Rating^{TM} to thousands of apps and services.

Identify and track risky apps

Continuously monitors cloud app usage and highlights any risks and compliance issues these may pose.

Control Usage

Take action with automated policies to adopt, block, or substitute those cloud apps.

Cloud Security Posture Management

Comprehensive visibility and compliance in the cloud

RESOURCE DISCOVERY / VISIBILITY

Discover all cloud resources and view their security postures in a centralized console

CONFIGURATION ASSESSMENT

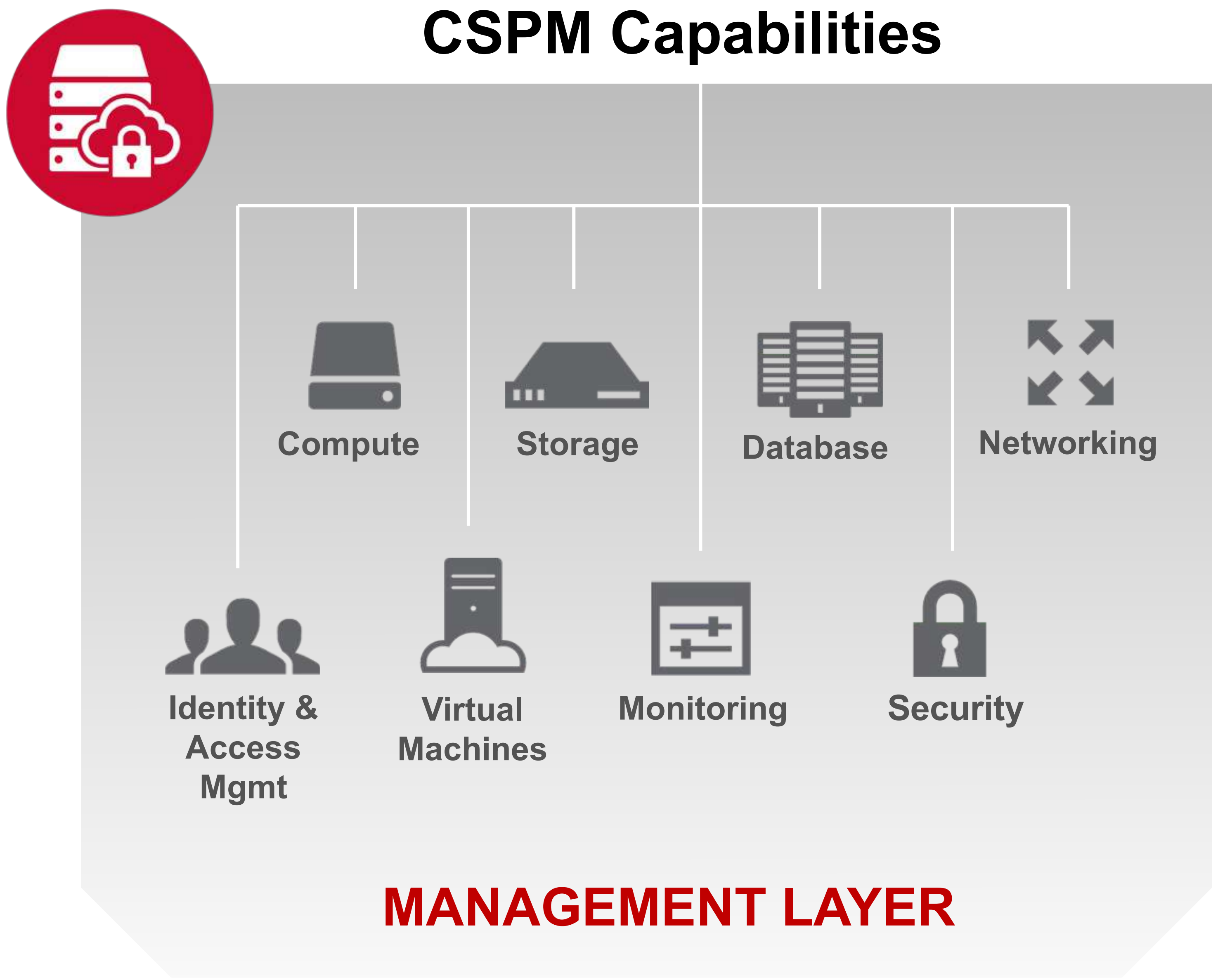
Monitor security settings and infrastructure changes and alert on policy violations – based on CIS benchmarks

REGULATORY COMPLIANCE

Benchmark security policies and settings against industry best practices and regulations such as HIPAA, PCI, SOC2

AUTO - REMEDIATION

Quickly remediate misconfigurations and apply security policies to improve security posture and maintain compliance

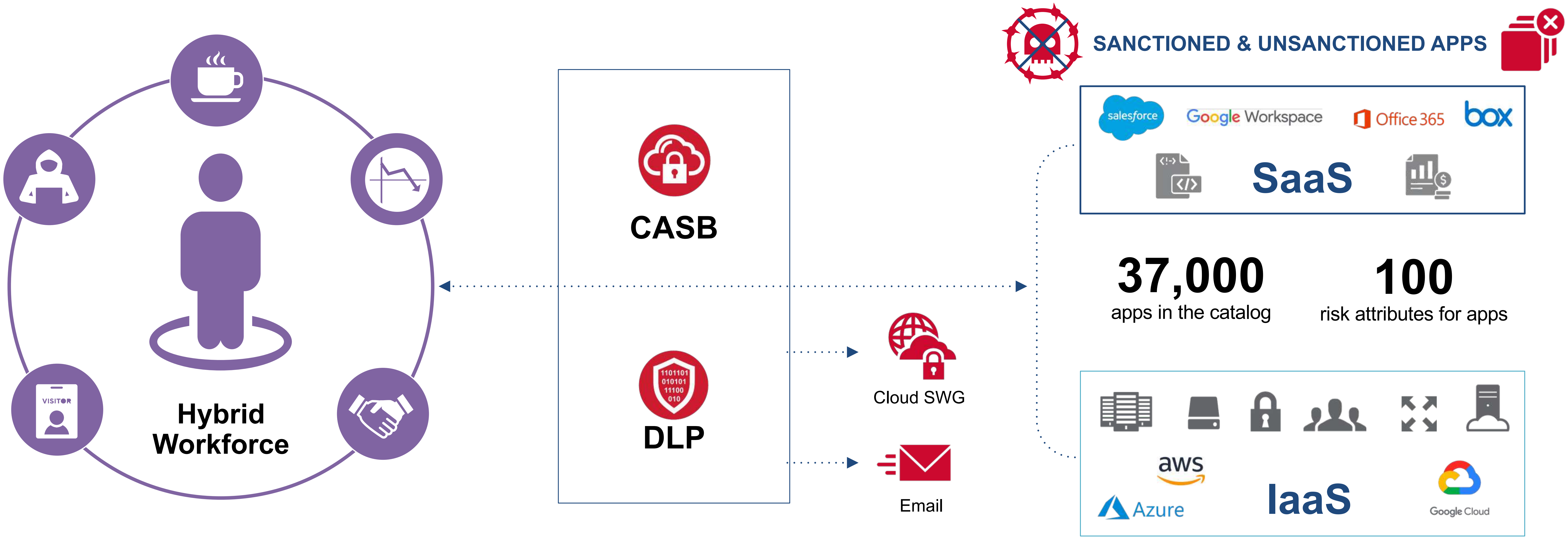


COMPLIANCE

- ✓ NIST
- ✓ PCI
- ✓ HIPAA

DLP in the Cloud

Delivering a comprehensive, secure and seamless user experience



SANCTIONED & UNSANCTIONED APPS

SaaS

37,000 apps in the catalog

100 risk attributes for apps

IaaS

CASB

DLP

Cloud SWG

Email

Hybrid Workforce

Gain granular visibility & control in the cloud and uncover Shadow IT

Monitor and protect sensitive data at rest and in motion in apps

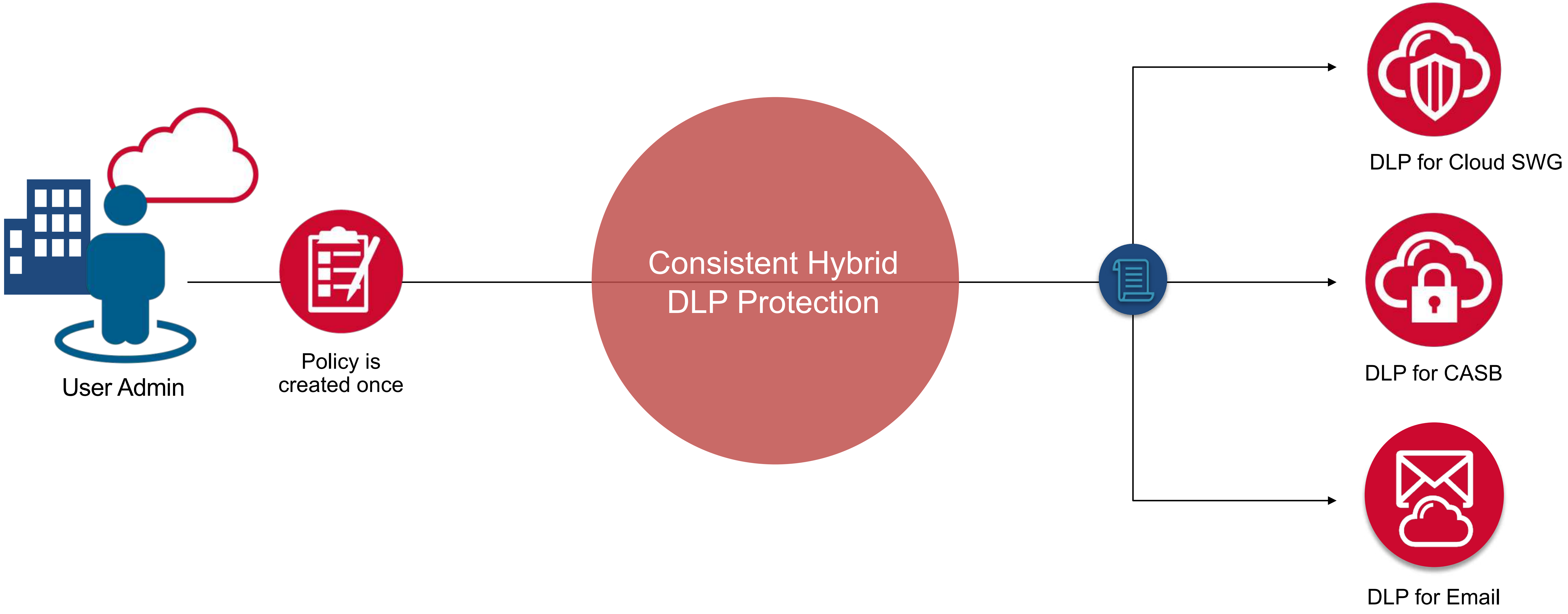
Identify risky behavior and defend against a host of cloud threats and malware.

Compliance Assurance in SaaS & IaaS

Continuously monitor risk and respond to security events quickly.

Protecting Data Everywhere

Integrated policies applied consistently to all channels.



User Admin

Policy is
created once

Consistent Hybrid
DLP Protection

DLP for Cloud SWG

DLP for CASB

DLP for Email

Rich Detection Capabilities

User Analytics

Remediation

Protect Your Files and Data in the Cloud

Understand your data and exposure in the cloud

- Visibility into user context, what’s shared and classification labels
- Quantify over-sharing exposure, external- and compliance risks
- Protect your apps via our Securlets (API based) and Gatelets (inline) deployments

Detect and protect your data no matter where it’s stored

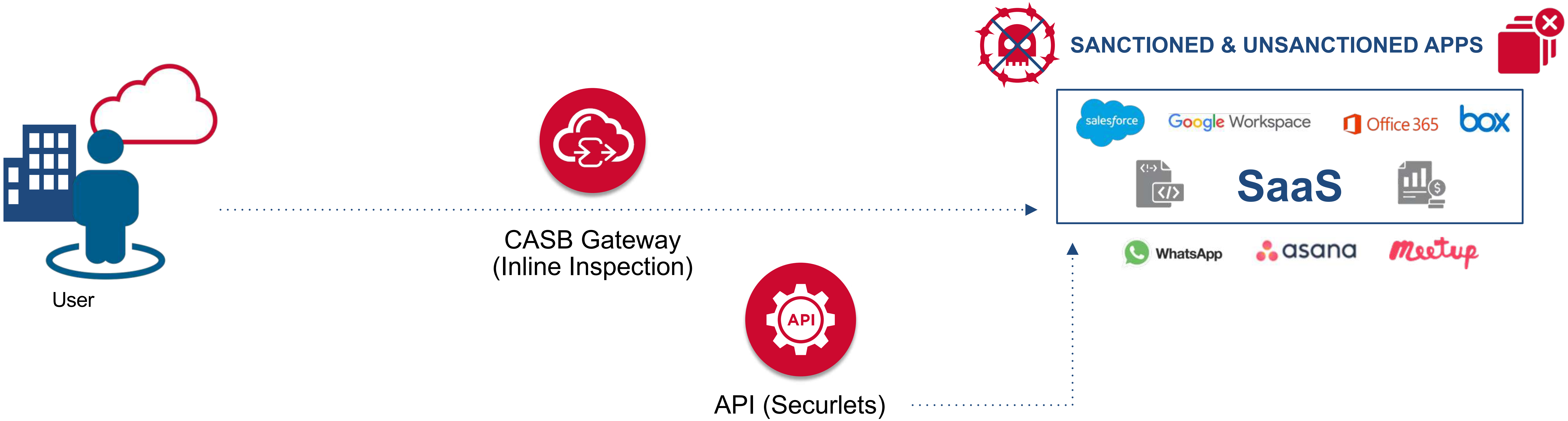
- Extend on-prem DLP to the cloud, web and email
- Govern data in the cloud with granular DLP policies via Cloud Managed DLP or Enforce
- Detect sensitive data using best in class detection technologies such as OCR, etc
- Automatically protect against data loss using Microsoft Information Protection encrypted files

Monitor, investigate and remediate violations

- Create policies to detect sensitive content and trigger response actions to protect it
- Use User risk scores in DLP policies (Adaptive Risk-based Policies) to apply the appropriate response actions
- Investigate DLP incidents and correlate with users’ activities through native UEBA
- Quarantine files, remove permissions and notify users

Monitoring Cloud Usage and Activities

API and Inline inspection



Inline Inspection (Gatelets)

- Inline gateway-based Security
- Real-time policy enforcement
- Visibility/control for sanctioned & unsanctioned cloud accounts

API Based (Securlets)

- API-based Security
- Fast & easy to implement
- Visibility/control for sanctioned cloud apps
- Visibility into exposed files
- Fine-grained remediation (i.e., un-share files with PII)

Detections Across Cloud Apps

Threat delivery and persistence

- Invalid login attempts
- Malicious URLs
- Virus violation
- Anomalously repetitious delete

Indicators of a compromised session

- Anomalously new device, browser or IP block
- Anomalous activity levels across devices, browsers, IP blocks
- Suspicious location changes
- Suspicious logins
- Invalid logins/invalid logins across users

Malicious use of an end user account

- Anomalously large shared data/anomalously large number of shares
- Anomalously large download data/anomalously repetitious downloads
- Anomalously large deleted data/anomalously large number of deletes
- Anomalously large transfers for the time of day
- Ransomware activity

Malicious use of a privileged user

- Anomalously large number of user actions
- Anomalous variety of activities

DLP for Web

Protecting your data with Cloud SWG

Decrypting traffic to provide DLP content inspection

Protecting your data being leaked to web destinations

Cloud SWG blocks user action based on DLP policy

Uniform policy and incident management through DLP

DLP for Email - Office 365 and Gmail

Preventing data loss and targeted attacks across email

Email is
a top vector
for data loss

How do we protect your data over email?

Inspect email content against DLP policies.

Block/Quarantine email to prevent a confidential data leak

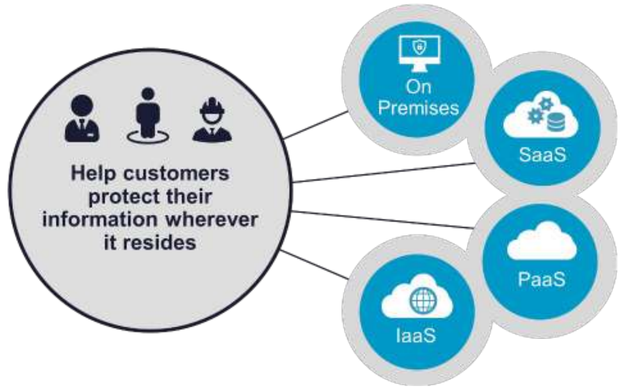
Uniform policy and incident management through DLP

Why Symantec For Information Security?

Performance At Scale:
Leading levels of data detection, rich incident context and broad integrations from a single policy

ACCURATE DETECTION

Symantec DLP offers superior protection across many channels



Help customers protect their information wherever it resides

Single DLP Policy Across All Channels

RICH CONTEXT

User Risk and rich incident context allows adaptive data protection

Adaptive Protection, Faster Remediation

REDUCED BURDEN

Simplified workflows around the needs of the DLP Admin and Incident Response teams

Total Cost of Ownership

NE VERUJ NIKOME 2023

HVALA NA PAŽNJI

Email: office@netpp.rs

Telefon: +381 11 3699 967