Net++ TECHNOLOGY

IT KLINIKA RELOADED

THE INSIDER

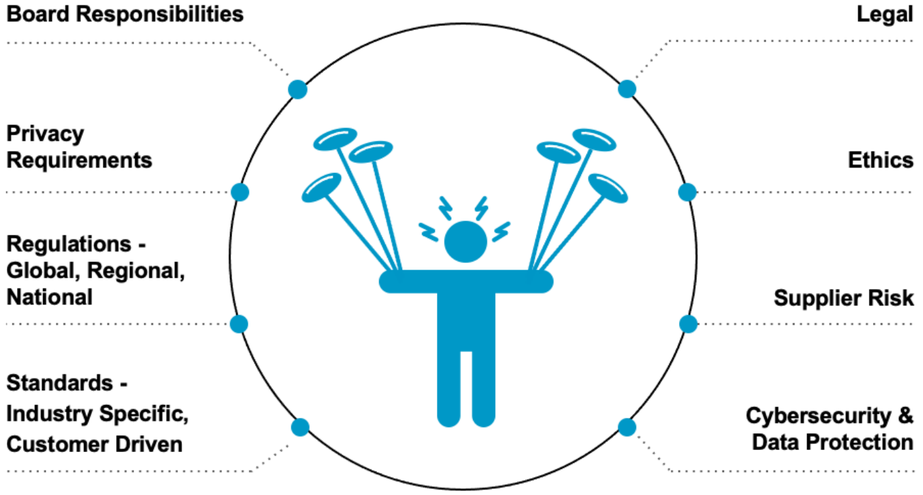
Kako detektovati i zaustaviti curenje poverljivih informacija? Kako sprečiti kađu podataka?

Vladimir Vučinić

DLP

Managing Data Protection and Compliance is Complex

You have too many plates to spin…



Cybersecurity has to deliver because the stakes are high

- Business Disruption
- Lost Revenue
- Reputational Damage & Lower Trust
- Fines, Penalties & Prosecution

NetOne TECHNOLOGY

DLP

The stakes are high

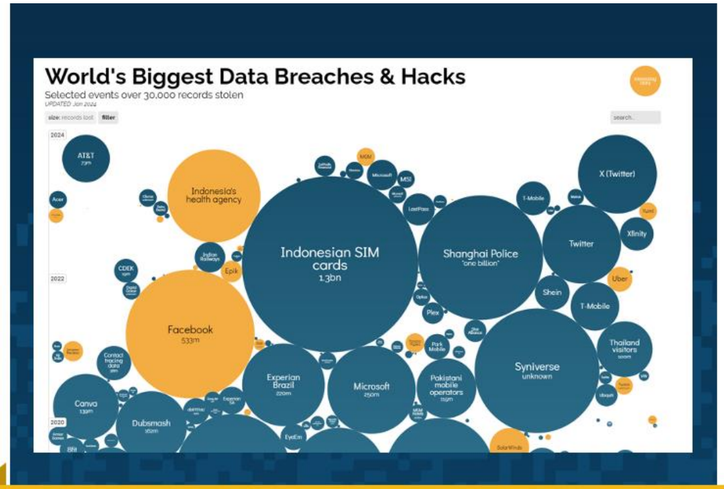
Privacy Regulations (e.g. GDPR) -> Fines

Insider Risk

Credential Theft

Vulnerabilities

Attackers



COSTS

- Non-compliance fines
- Collective Legal Actions
- Reputation Damage
- Business Operation Impact

NetOO TECHNOLOGY

DLP

Data Protection Challenges and Disruptive Drivers

ZERO TRUST
Defend increasingly blurred network perimeter and expanded attack surfaces

SECURE DIGITAL TRANSFORMATION
Accelerated transition from legacy on-prem to hybrid cloud

WORK FROM ANYWHERE
Remote work is becoming new norm during COVID

COMPLIANCE & PRIVACY
Regulators cracking down on checkbox compliance and putting pressure on security budgets

INTELLECTUAL PROPERTY PROTECTION
Deliberate data theft by employees is easier in work-from-home environment

NetOO TECHNOLOGY

DLP

Generative AI – A new treat to sensitive data

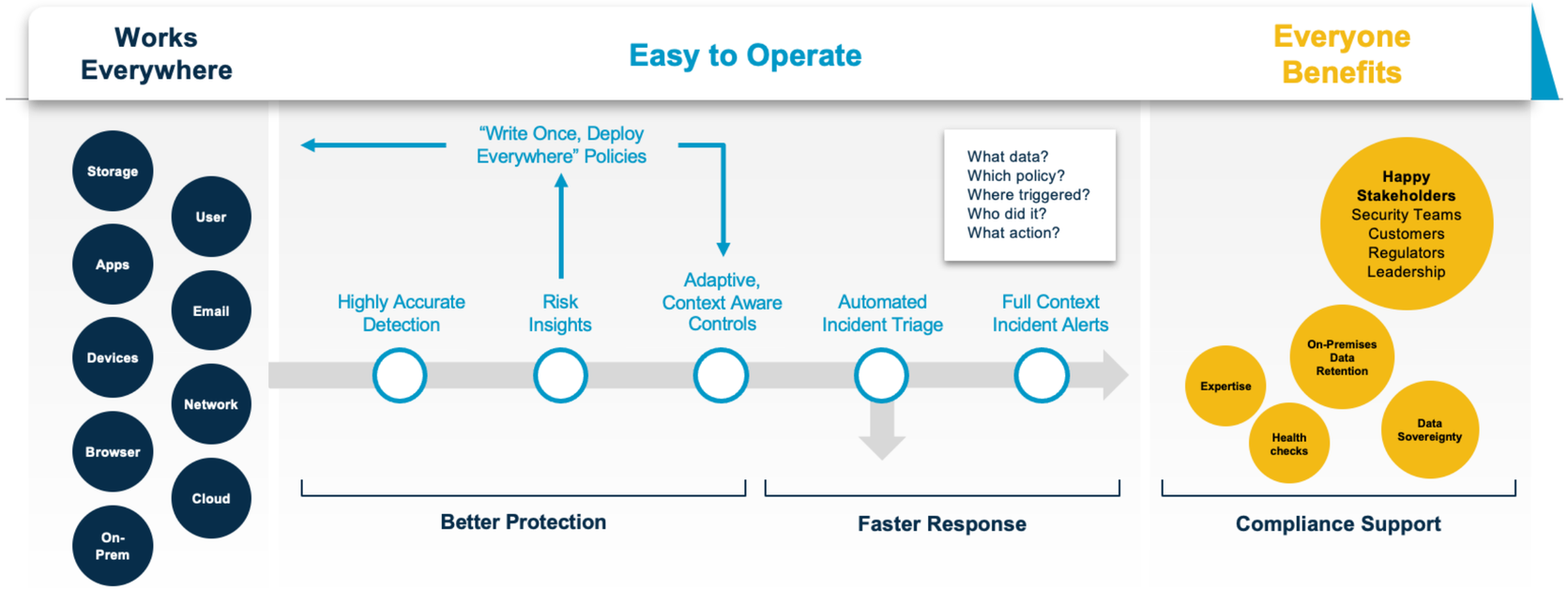
Sensitive Data

- Automation Efficiencies
- Personalization Benefits
- Optimization Benefits
- Innovation Opportunities
- Security Concerns
- Privacy Concerns
- Legal Concerns
- Integration Concerns

DLP

Protection with a Unified, Accurate System

World-class protection, the simpler way

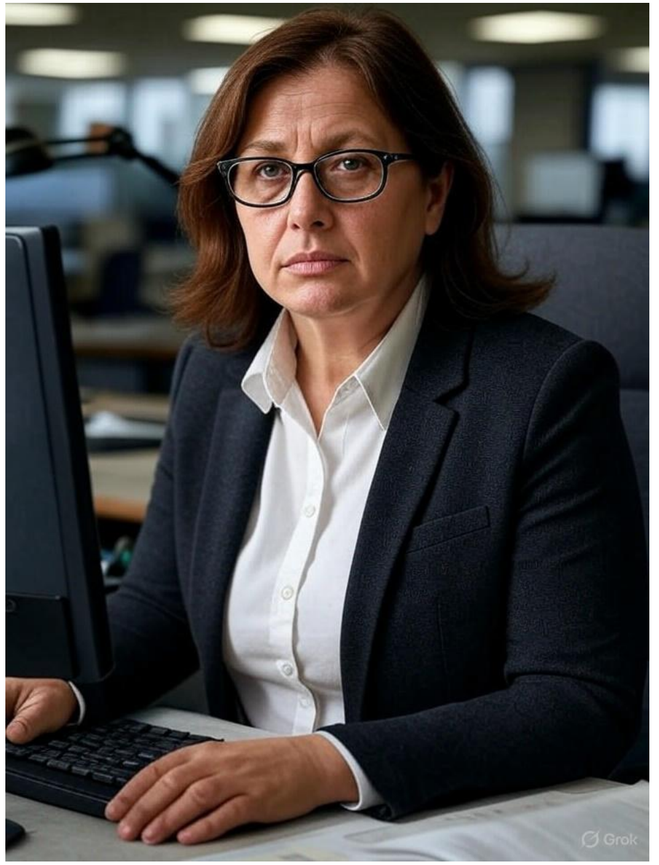


NetOne TECHNOLOGY

SLAVICA

- tipičan zaposleni
- prošla cybersecurity obuku (ali...)
- posla preko glave
- veruje da IT ne radi ništa po ceo dan
- veruje da IT samo smeta i izmišlja nešto
- vredna, radna, ali nije baš da voli računare

jedan radni dan

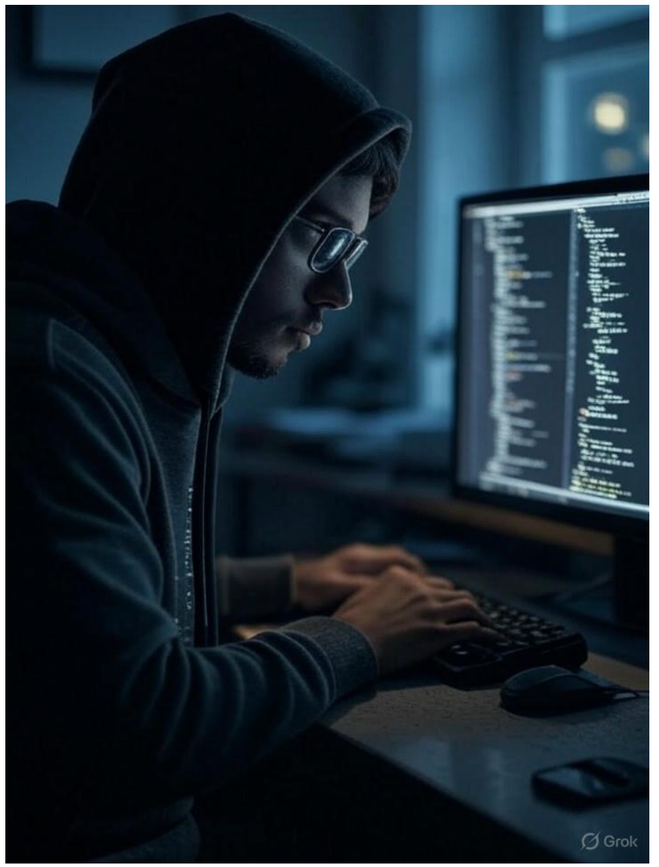


NetPlus TECHNOLOGY

DR4GOVICH

- tipičan hacker
- posla koliko želi (i sa neke egzotične lokacije)
- veruje da IT ne radi ništa po ceo dan
- veruje da može da upadne u svaki sistem
- sa lakoćom izvlači podatke iz firmi
- prodaje tuđe podatke kako bi živeo luksuznim životom

jedan dan



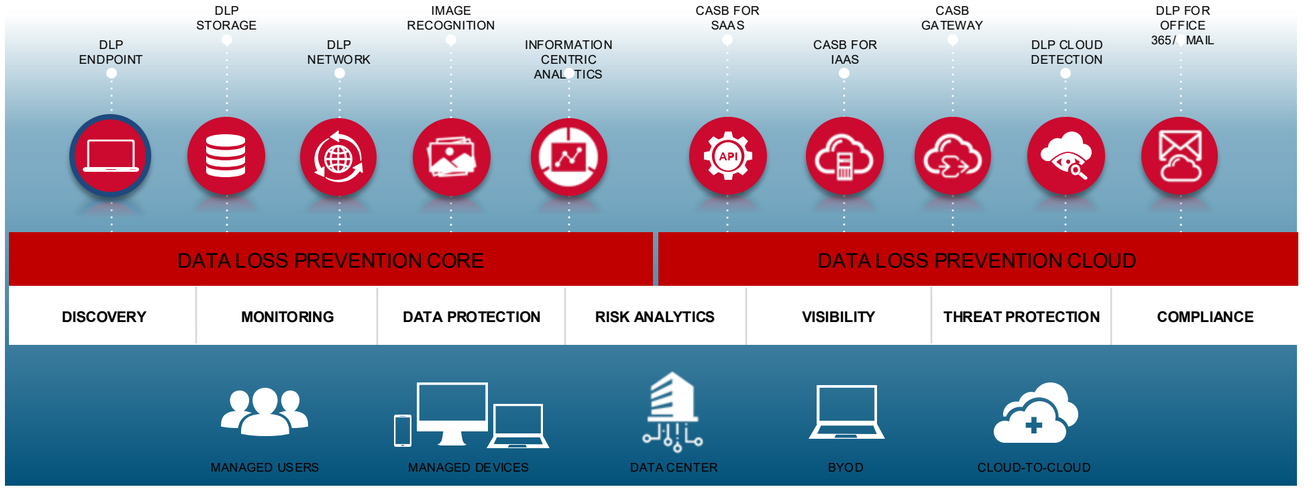
NetPP TECHNOLOGY

KAKO TO STVARNO IZGLEDA (DEMO)?

- prikaz DLP core rešenja, konzole
- prikaz polisa i upravljanja sa detekcijom
- response rule – šta nam je raspolaganju
- incidenti i analiza (DLP konzola)
- Slavica radi sa više poverljivih dokumenata
- kopiranje dokumentata sa poverljivim podacima

DLP

Symantec Data Loss Prevention Solutions

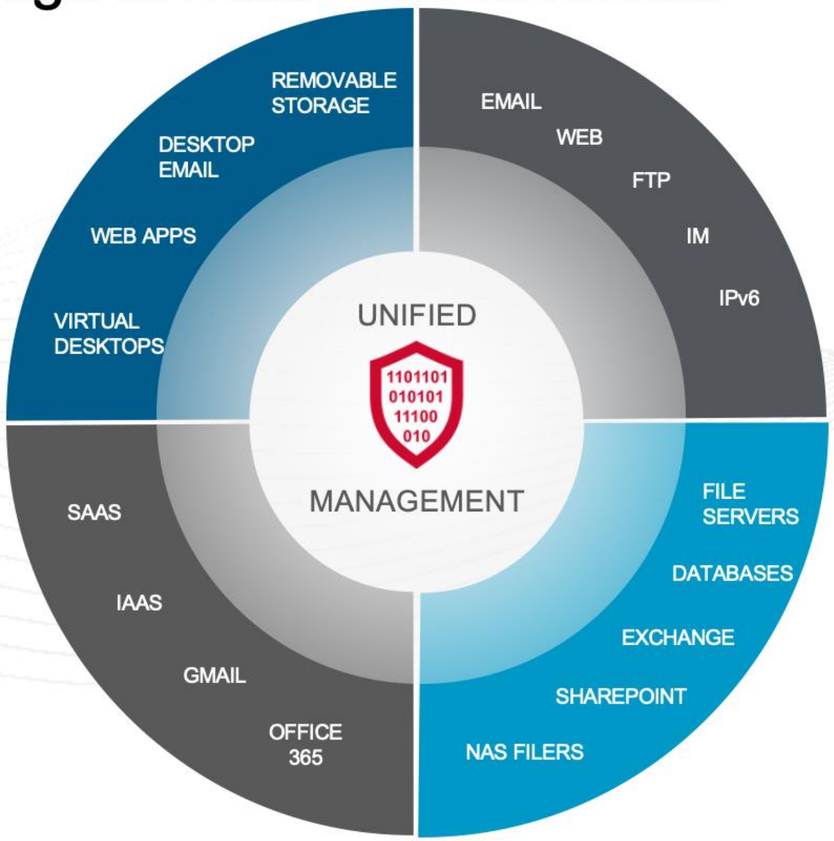


Symantec™ by Broadcom

NetOO TECHNOLOGY

DLP

Broadest Coverage of Data Loss Channels



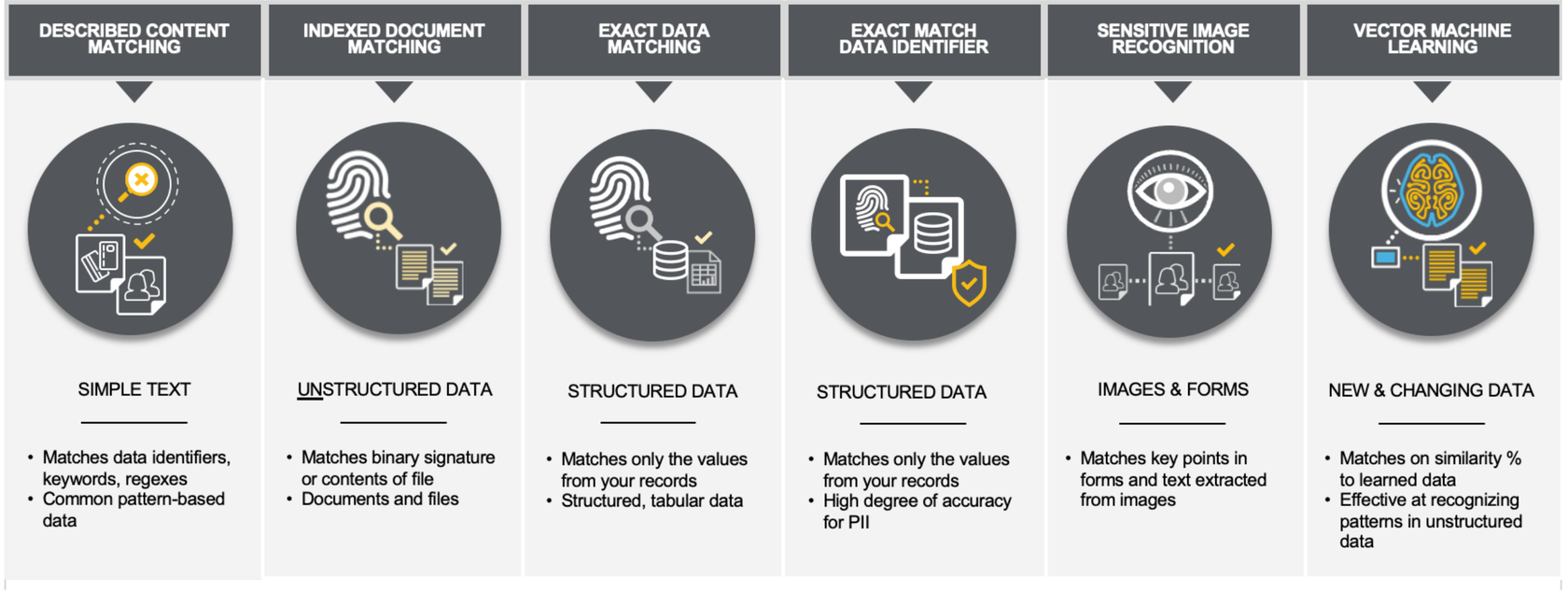
Symantec™ by Broadcom

NetOne TECHNOLOGY

DLP

Multi-Layered Detection Catches What Others Miss

High levels of accuracy and control with minimal false positives

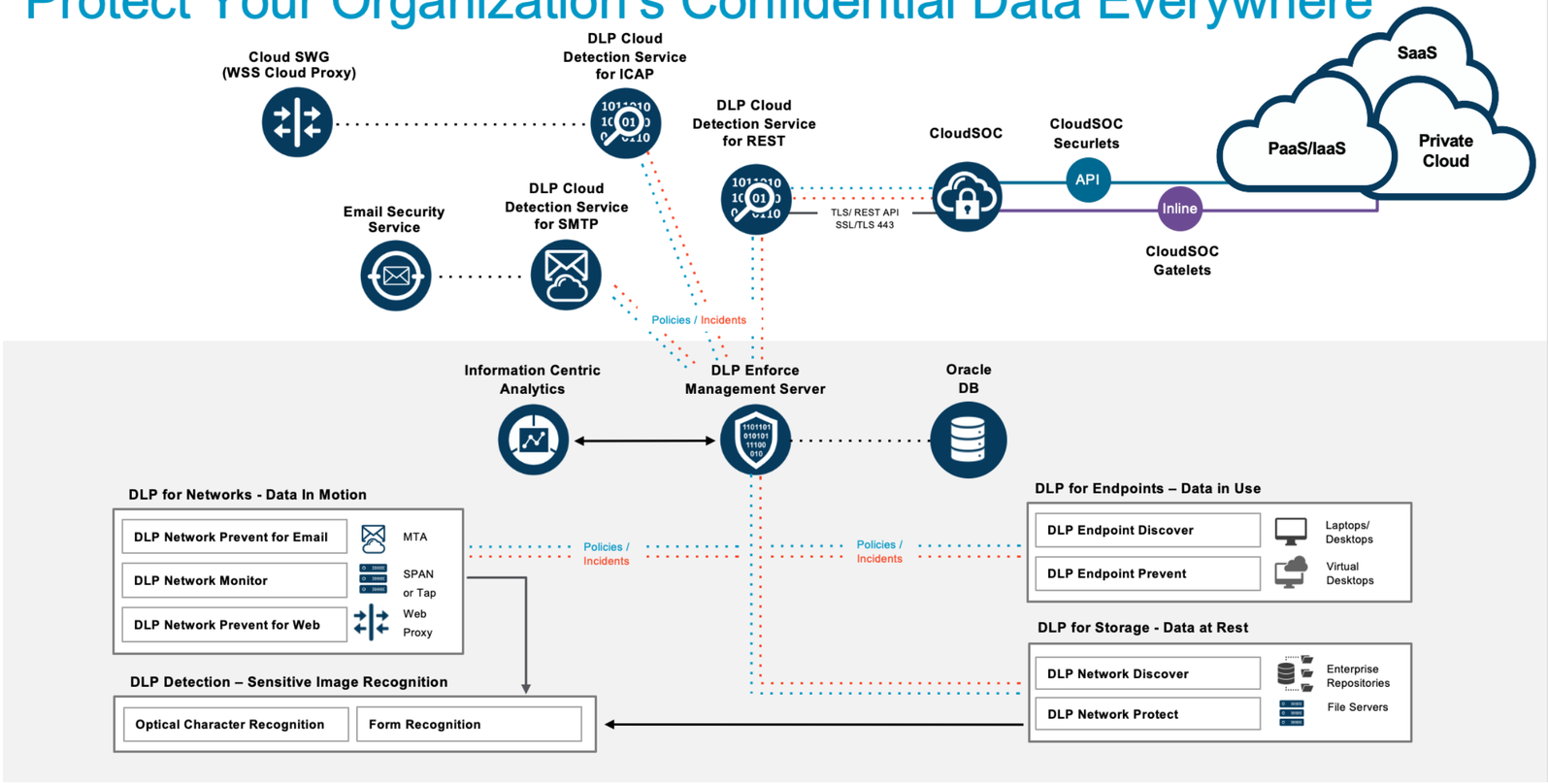


Symantec™ by Broadcom

NetOO TECHNOLOGY

DLP CORE & CLOUD

Protect Your Organization's Confidential Data Everywhere



Symantec™ by Broadcom

NetOne TECHNOLOGY

DLP

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.

Symantec™ by Broadcom

NetOO TECHNOLOGY

DLP

User Risk-Based Detection: DLP + Information Centric Analytics (ICA)

What is it?

- **Risk-Based Detection** lets you include a user risk score as part of a DLP policy.
- User Risk Score **Detection Rule**
  lets you detect content based on user risk score and can be combined w/ any other rule.
- User Risk **Response Rule condition**
  lets trigger a response action based on user risk score.

Benefits

- **Leverages ICA user-risk scores**, calculated from multiple sources
  Risk score: 1 to 100 (w/ 100 being highest risk)
- Provides ability to **apply stricter policies to high-risk users**
- Helps **maintain flow of business**, while preventing high-risk activities

Symantec™ by Broadcom

NetOne TECHNOLOGY

DLP

Getting the Right **Incident Response**

Right Metrics

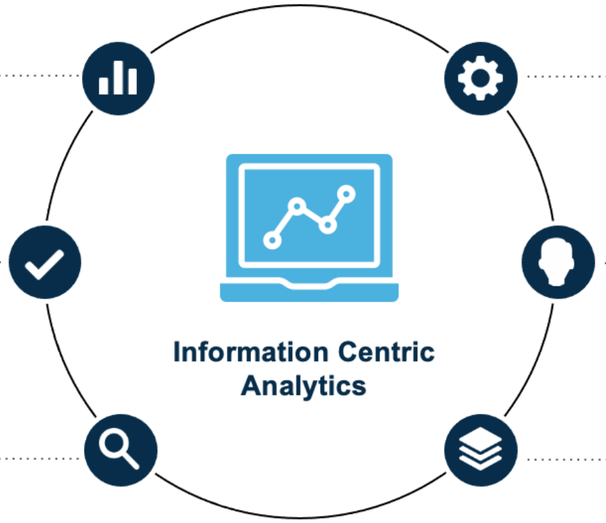
Prove Results to Execs and Auditors

Right Action

1-Click Response

Right Information

5-Second Test



Right Automation

Resolution, Enforcement, Notification

Right Person

Route Incidents to Right Responder

Right Order

High Severity of Incidents First

90% of DLP is Incident Response

Symantec™ by Broadcom

NetOne TECHNOLOGY

DLP

Operational Simplicity Leads To **Better Outcomes**

Solve the skills shortage problem

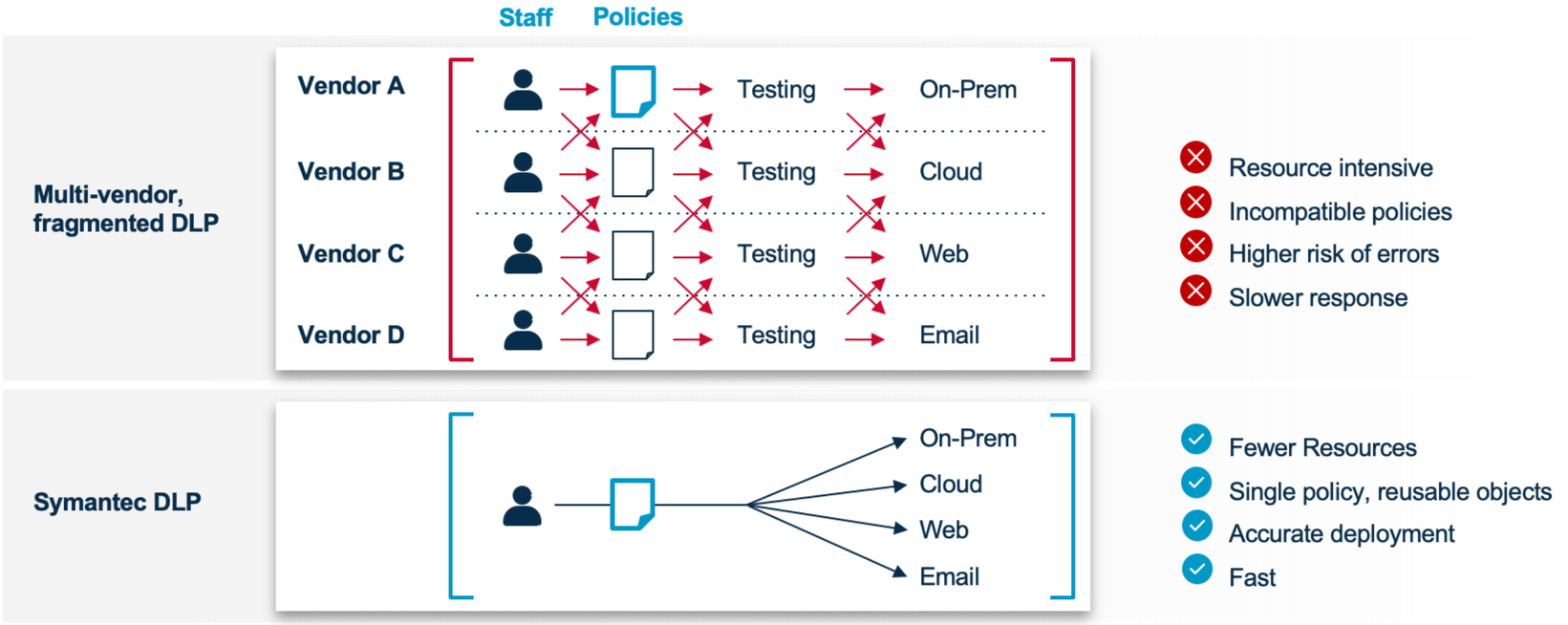
	Piecemeal	Higher Quality Outcomes →	Integrated
Detection	Potentially broad, but fragmented		**Broad** - detection everywhere
Incident Response	False alerts or missed detections		**Full context**, shared intelligence
Policy	Multiple policies lead to delays & lower quality		**Unified policy**, simpler to manage
Skills	Staff must specialize		**Less need** for specialist teams
Compliance Reporting	Conflicting data sets		Data all in **one place**

Symantec™ by Broadcom

NetOne TECHNOLOGY

DLP

Stop Policy Complexity From Damaging **Your DLP Outcomes**

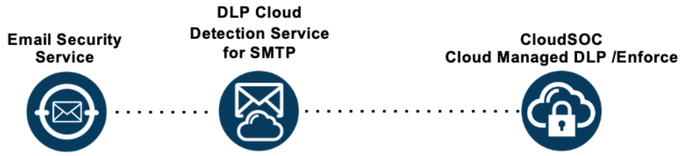


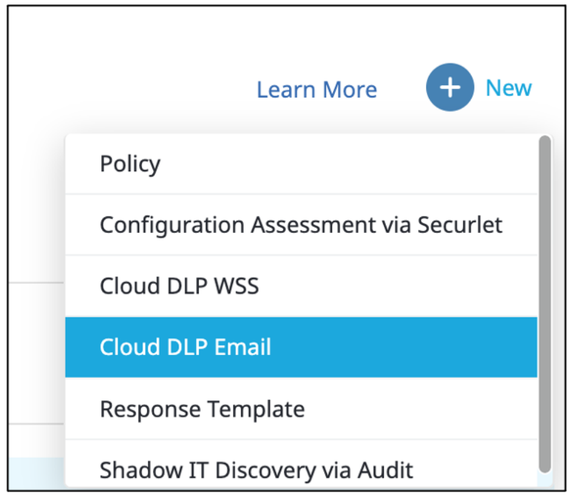
Symantec™ by Broadcom

NetOne TECHNOLOGY

DLP INTEGRACIJA

Email Security.cloud

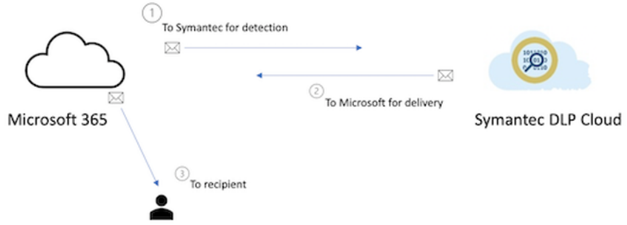




- Monitor DLP Profiles to identify sensitive data in emails
- Provide remediation or trigger encryption via Policy Based Encryption in Email Security.cloud
- Multiple Deployment options

Forward Mode (DLP, Threat Protection, Encryption)

Reflective Mode (DLP Only)



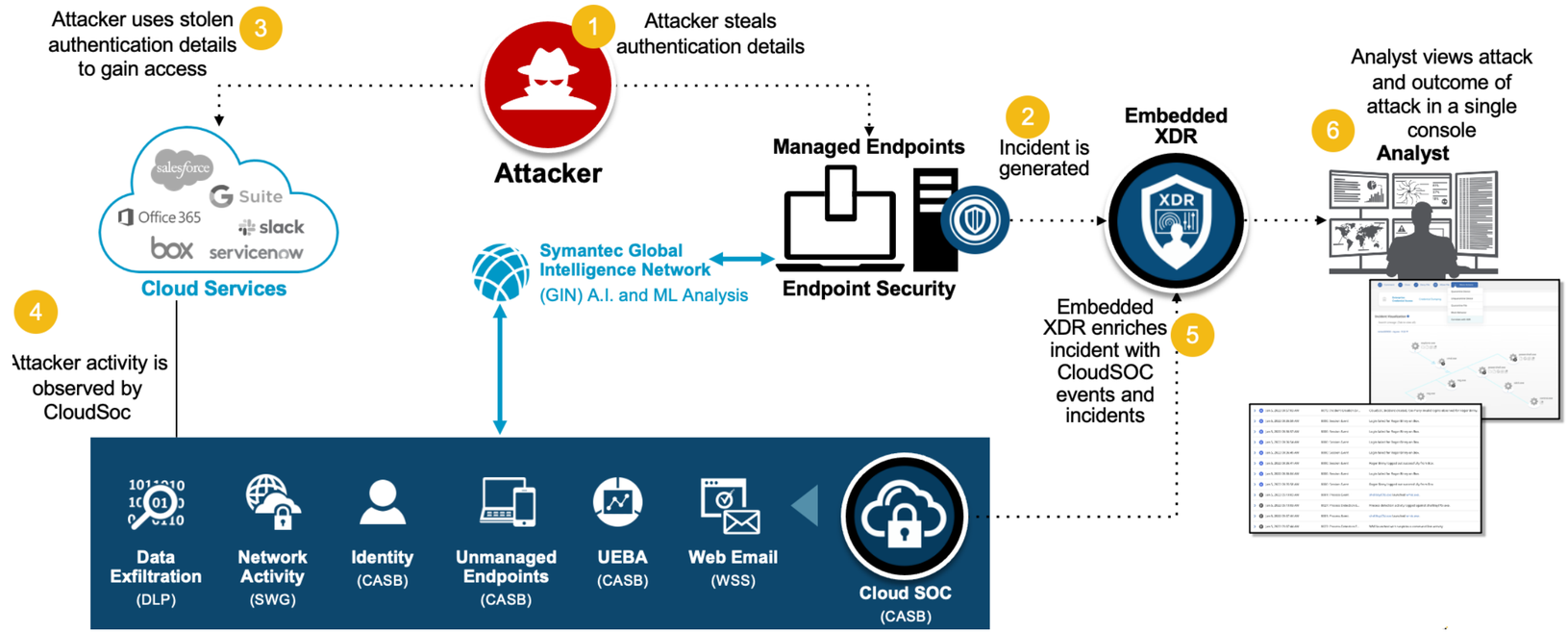
Symantec by Broadcom

NetPlus TECHNOLOGY

DLP INTEGRACIJA

XDR: Endpoint protection and CloudSOC integration

Correlates suspicious user behavior on endpoints and cloud services



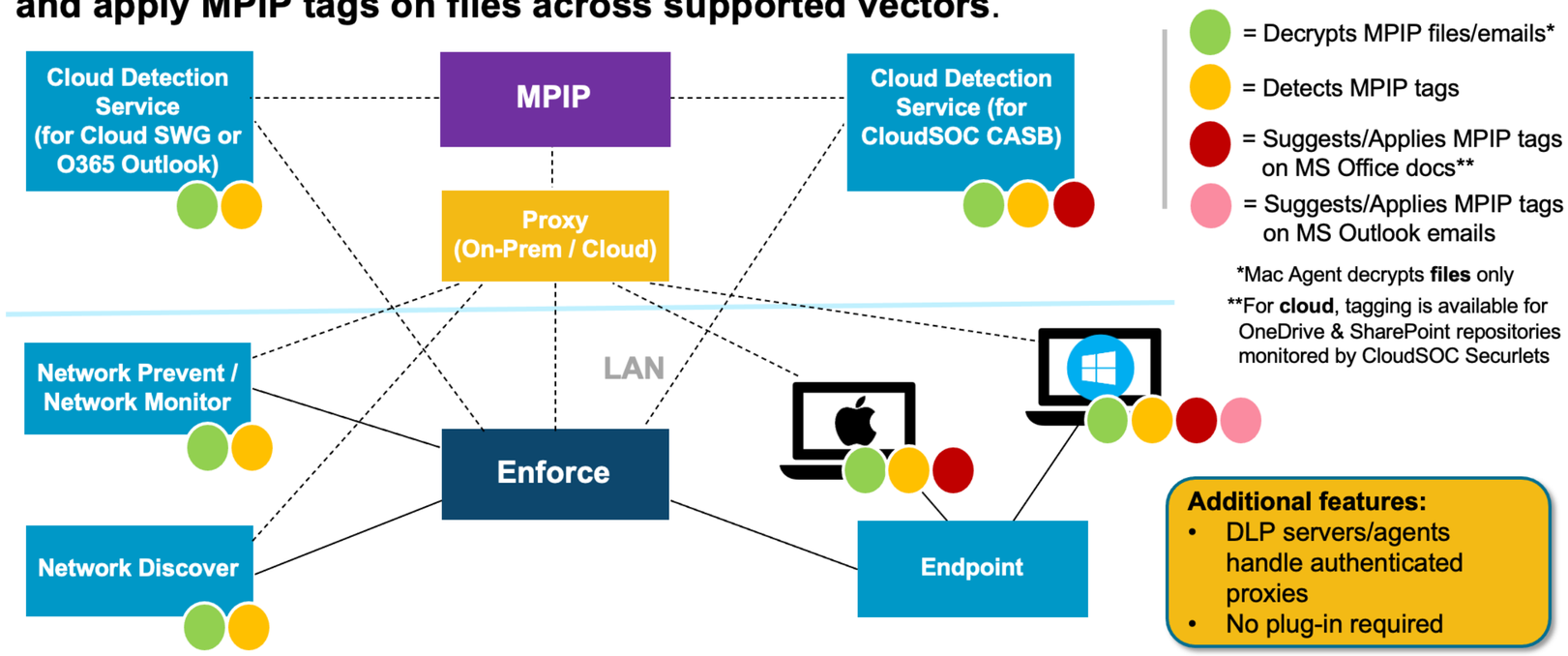
Symantec by Broadcom

NetPlus TECHNOLOGY

DLP INTEGRACIJA

DLP and MS Purview (MPIP) integration

DLP can decrypt MPIP-protected files and read MPIP tags across all vectors, and apply MPIP tags on files across supported vectors.



= Decrypts MPIP files/emails*

= Detects MPIP tags

= Suggests/Applies MPIP tags on MS Office docs**

= Suggests/Applies MPIP tags on MS Outlook emails

*Mac Agent decrypts **files** only

For **cloud, tagging is available for OneDrive & SharePoint repositories monitored by CloudSOC Securlets

Additional features:

- DLP servers/agents handle authenticated proxies
- No plug-in required

Symantec by Broadcom

NetOne TECHNOLOGY

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

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

Symantec™ by Broadcom

NetOne TECHNOLOGY

PITANJA?

NetPlus TECHNOLOGY

HVALA NA PAŽNJI

+381 11 36999 967

www.netpp.rs

Otokara Keršovanija 11/39, Beograd