
Intelligentní ochrana osobních údajů (a citlivých dat) v procesu digitální transformace a přechodu do cloudu.

Vladimír Špička
FORCEPOINT



Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain

Outline

Challenges of Data Security Today

Our Data Protection Point of View

Intelligent Data Security



—

The world is changing but there
are 2 constants:

People & Data

They pose the greatest risk

I am your
greatest
asset.

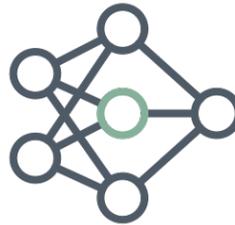
I am your
greatest risk.



Challenges of traditional approaches to data security



Lack of visibility to data – everywhere



Complex & rigid policies



Lack of context & understanding of user intent

Organizations are forced to rethink their data protection strategy

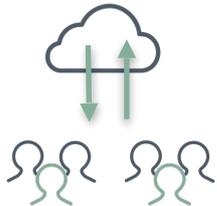
The attack surface is constantly growing



Data resides in places you don't own or manage



Data proliferation with the increasing use of SaaS apps



Users heavily rely on SaaS apps to effectively collaborate with partners

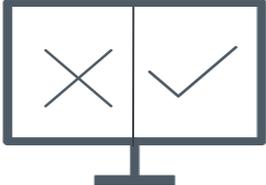


Hybrid environments add a new layer of complexity

Today's data protection options are limited

**Traditional
DLP**

*Block it or
Allow it*



Current policies are far too rigid to be effective.

**Traditional
Analytics**

*Forensic
Analysis*



Learning why something happened **yesterday** does not stop the problem.



An effective solution should cut through the noise of alerts, highlight early warning signals to **prevent** the loss of important data.

Identifying the right business outcomes



Control and manage data shared, stored and accessed on cloud applications



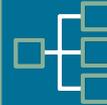
Correlate user behavior to the value of the data being accessed



Gain deeper insights to user intent



Dynamically enforce policy controls while enabling employee productivity



Manage and enforce policies across all channels via a single console

Achieving the desired business outcomes



Determine the data that is important and locate it



Proactively and dynamically protect that data



Eliminate the complexity of achieving compliance

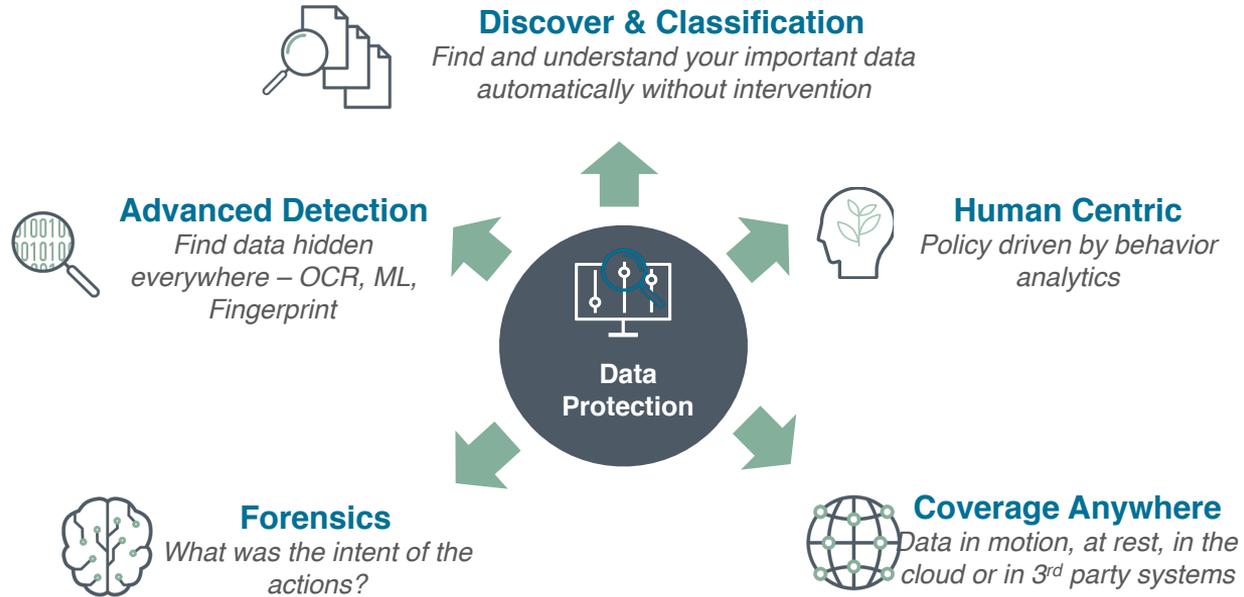


Control and manage data everywhere it resides

Forcepoint's Data Protection Approach

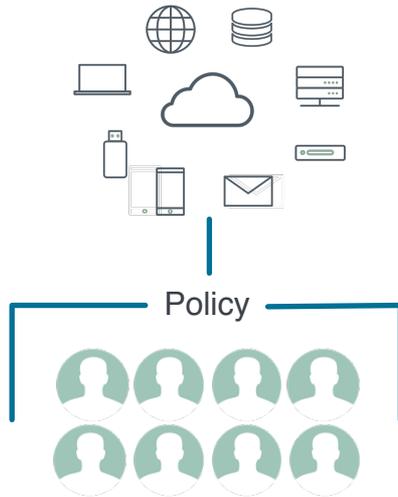
Data protection can be the cornerstone approach to Security

- ▶ Focus on critical data & human risk
- ▶ Broad partnerships to fit into any environment



Human-Centric Cybersecurity

Traditional Security



One-to-many enforcement of static, generic policies, producing high false positive rates.

Intelligent Data Security



One-to-one enforcement of different policies based on the risk, enabling automation.



Protecting your most valuable assets at the human point: The intersection of users and data

Intelligent Data Security

Individualized data protection

Replace broad rules applied to groups with one-to-one, risk-adaptive security that won't slow down your people.



Automate policy enforcement

Surface behavioral anomalies and adjust individualized data security controls, preventing data loss in near-real time.



Decrease false positives

Enforce policies where and when you need it, decreasing alerts and inquiries into IT/Security.



Instant cloud control

Rapid detection, visibility, and control of cloud access across your organization.

Risk-Adaptive Protection

Risk-adaptive protection dynamically applies monitoring and enforcement controls to protect data based on the calculated behavioral **risk level of users** and **value of data** accessed.

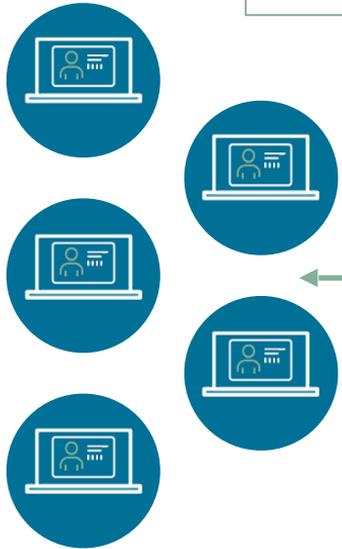
This allows security organizations to better understand risky behavior and automate policies, dramatically reducing the quantity of alerts requiring investigation.

How Risk-Adaptive Protection Works

- 1 Each user has a unique and dynamic Risk Level
- 2 Risk levels are driven up and down based on changes in behavior
- 3 Risk Levels drive different outcomes
- 4 Security adapts to Risk Levels as they fluctuate

Dynamic Data Protection Delivers Automated Enforcement

Forcepoint DLP



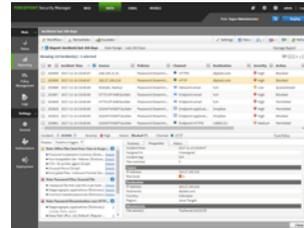
Endpoint monitoring,
Collection and enforcement



Endpoint
Server

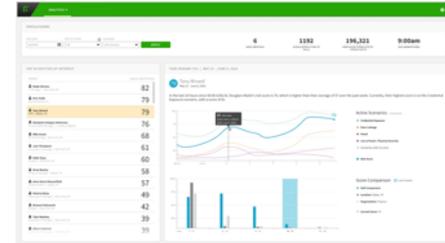


Set dynamic
enforcement
action plan



View DLP
incidents
with end-user
risk level

Dynamic Data Protection



Automatically
analyze DLP
data for identity
risk calculation



Investigate
high-risk entity
activity

Better Understanding of Intent



What if your employee tries to print a customer's credit card data? DLP blocks it, but then he...



tries to send it to a personal email address. DLP blocks it, but then he...



tries to copy the data to USB. DLP blocks it, but then he...



tries to upload it to Dropbox. CASB blocks it, but then he...



tries to upload it to Google Drive. CASB blocks it, but then he...



tries to FTP it outside the organization. DLP blocks it.

Is this employee a risk? How would you know?

Better Understanding of Intent

Let's try that again, but with Forcepoint's Dynamic Data Protection....



Tries to print customer's credit card data. DLP blocks it, but then...



Tries to copy it to USB. DLP blocks it, but then...



Tries to upload it to Google Drive. CASB blocks it, but then...



Tries to send it to a personal email address. DLP blocks it, but then...



Tries to send it to upload it to Dropbox. CASB blocks it, but then...



Tries to FTP it outside the organization. DLP blocks it.



Better Understanding of Intent

Options for the security team



1 Initiate an investigation



2 Adjust policies and implement protective measures



Doing more than just auditing alerts



Problem

- ▶ DLP implementers are concerned with being viewed as a strain on user productivity in the event their policies result in too many false positives.



The Security Requirements

- ▶ Having the ability to forensically audit their alerts if important data leaks.



Result

- ▶ Many organizations have deployed DLP in audit only mode. The security team can mine alerts to identify data exfiltration, but they don't actively block it.

Benefits of Dynamic Data Protection

Intelligent
DLP

Reduce the amount of DLP alerts that need to be triaged; transition DLP from broad to individual policies.

Increased
Productivity

Provide greater flexibility in policies, and adapt enforcement based on calculated risk.

Proactive
Security
Management

Detect and respond to high-impact events in a shorter amount of time.

Děkuji za pozornost a sledujte nás na:



@Forcepoint



Forcepoint



@ForcepontSec
@ForcepointLabs



Forcepoint LLC



Forcepoint