sealpath

SMART PROTECTION FOR SENSITIVE DATA

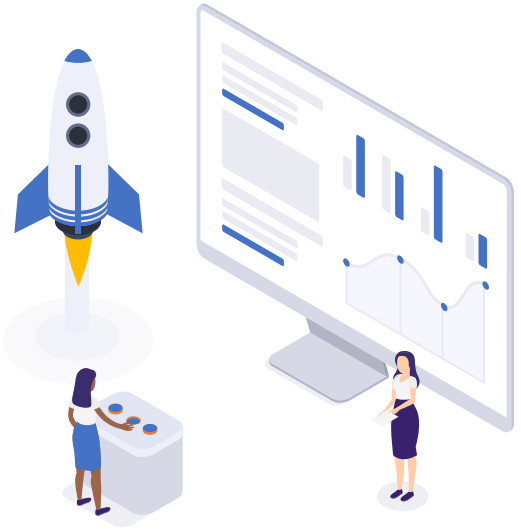
SMART PROTECTION FOR SENSITIVE DATA AND SECURE COLLABORATION

Presenter:
Sandrine Roux
Sealpath International
Channel Manager

Risks of Hybrid Working and Data Security.

Benefits of the Hybrid Work Model

- ✓ *Increased productivity*
- ✓ *Happier employees, work-life balance*
- ✓ *Cost reduction*
- ✓ *Attract more talent*



"A study by IESE Business School says that 36% of employees prefer to work from home three days a week and 32% only two days a week. Only 12% would always work remotely and 4% would never work remotely.

The Irruption of the Hybrid Workplace

Hybrid work heightens tension in applying cybersecurity controls

CSO ESPAÑA COMPUTERWORLD

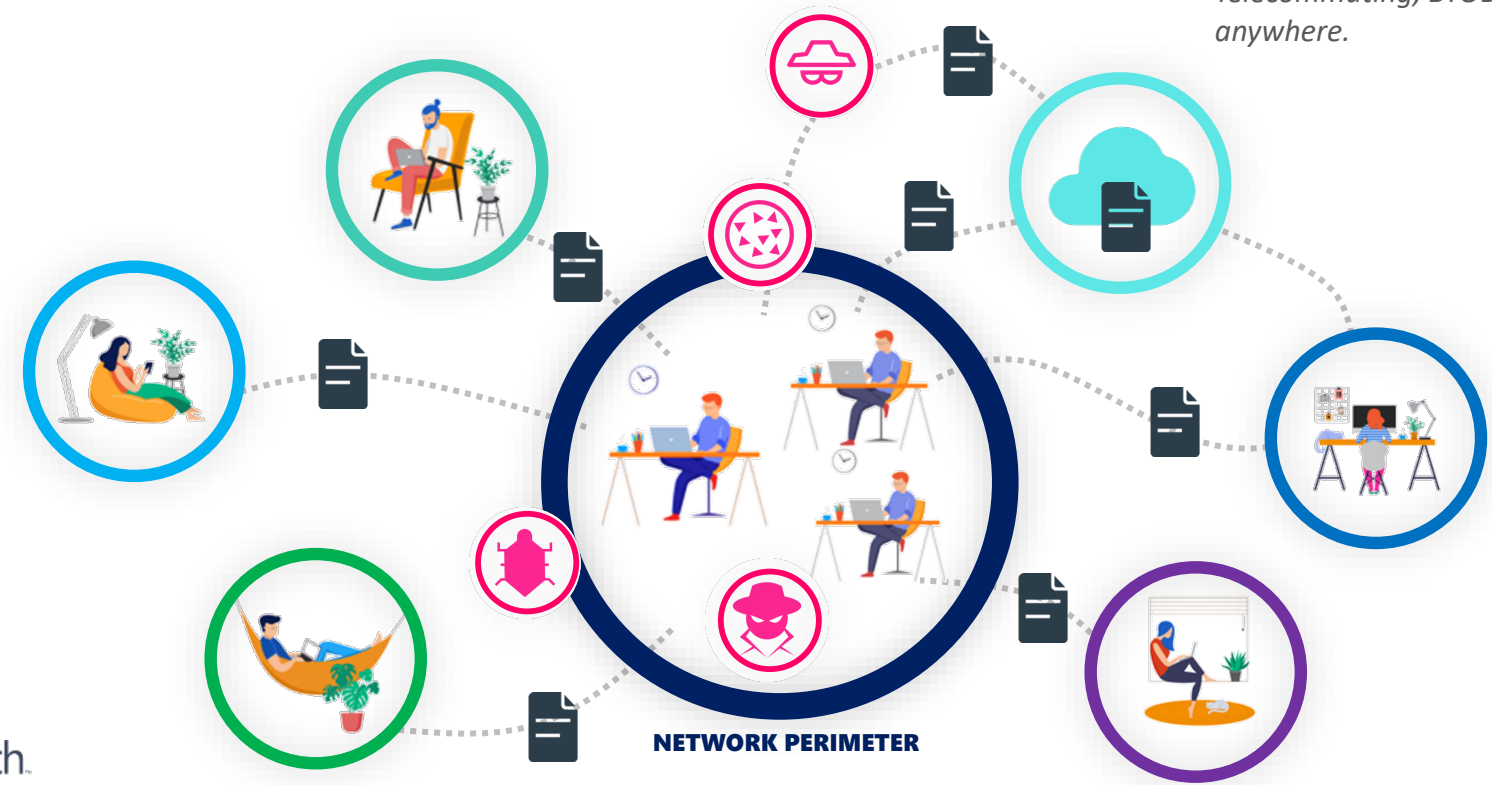
83% of IT teams believe that the rise of remote work has created a "ticking time bomb" that could lead to corporate network failures, according to an HP study.

"Organizations and staff have adapted very quickly to conducting their business in the office, at home and on the move."

¿Internal = Trusted and External = Not Trusted?

The company perimeter has disappeared

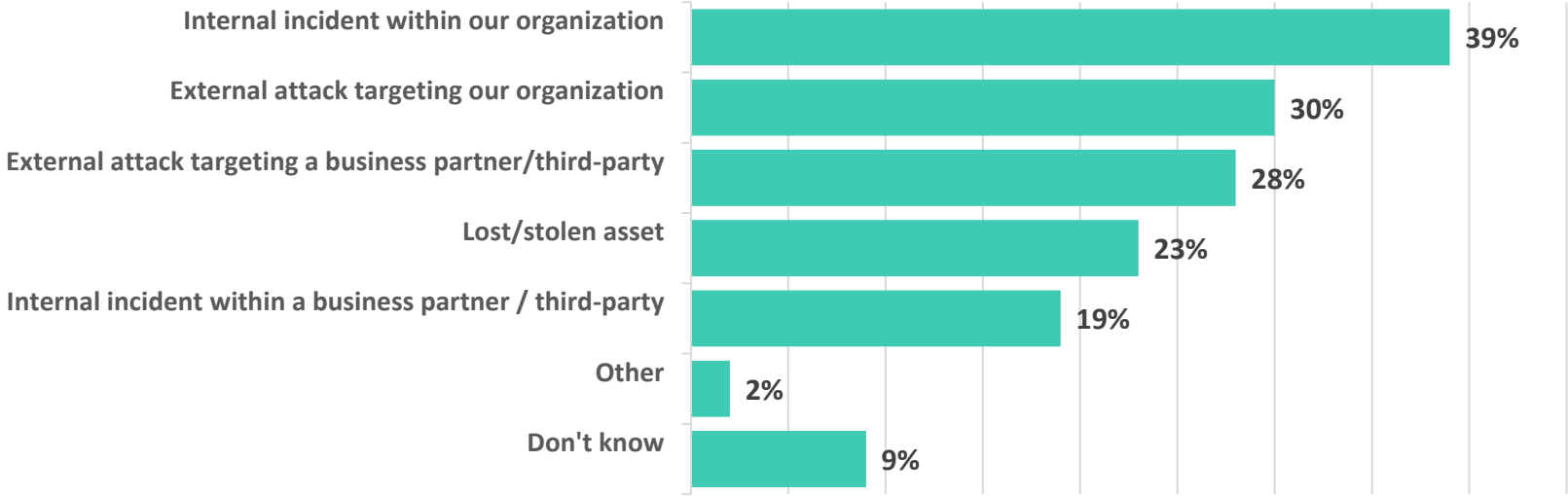
Cloud collaboration boosting, Telecommuting, BYOD. The data anywhere.



sealpath

Data leakage can happen anywhere

What were the most common ways in which the breach(es) occurred in the past 12 months?



Source: Forrester's Global Business Technographics Security Survey

Base: 565 global network security decision-makers whose firms have had a security breach in the past 12 months

Increased Threats with Hybrid Labor

2021 - Largest increase in the cost of a leak in 7 years.
Increasing from $3.86 million in 2020 to $4.24 million in 2021.

Increased Threats with Hybrid Work

54% of 36,000 companies surveyed have had data breaches or losses in 2021.
*IBM Cyber Resilient Organization Study

Ransomware attacks cost an average of 4,62 million € and lost business represented the largest share of data breach costs, averaging $1.59 million.
*IBM Cost of a Data Breach Report 2021

48% of corporate cyber attacks come via mobile devices.
*Hiscox study cyber readiness

28% of cyber-attacks on companies occur through phishing or spoofing of employees.

sealpath

Home Network and Personal Devices

Home networks are a critical part of the enterprise network.

- ✓ *It is more difficult to manage incidents with the IT department.*
- ✓ *The home network offers fewer protections.*
- ✓ *Personal devices are more vulnerable.*
- ✓ *Access control and protection from personal devices.*

Infrastructure and Cloud Services

- ✓ *Vulnerabilities in VPN solutions or New Services.*
- ✓ *Misconfigured RDP servers with weak credentials.*
- ✓ *Stolen Access Credentials.*
- ✓ *Software misconfigurations.*
- ✓ *Increased data transfer between remote workers, servers, the cloud and employees in the office.*

sealpath

Sensitive Data

"Data will travel more than ever, across multiple media, tools and devices".

- ✓ *Secure data wherever it travels.*
- ✓ *Facilitate secure collaboration.*
- ✓ *Restrict unauthorized access and monitor in real time.*
- ✓ *Minimize the possibility of data leakage.*
- ✓ *Rapid response to alerts.*

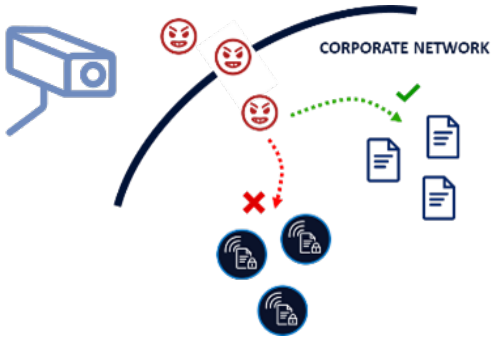
Best Practices - "Trust no one".

Choose the Zero-Trust Security model.

- ✓ *Principle of least privilege access. Only the resources needed to carry out the activity can be accessed.*
- ✓ *Network segmentation.*
- ✓ *Monitor and check everything.*

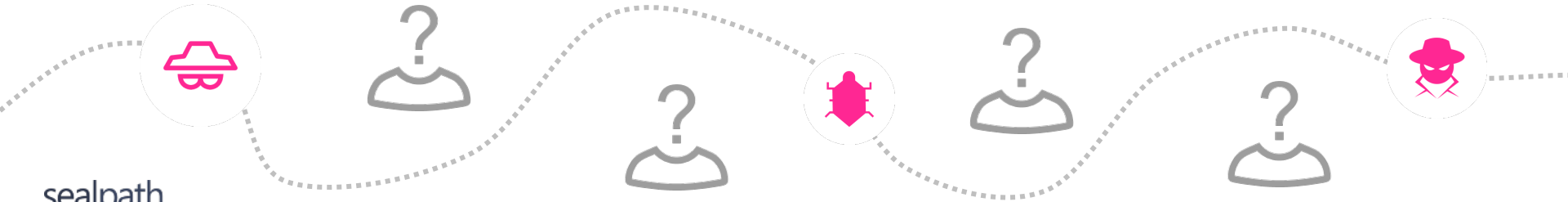
Best Practices - Analyze and Evaluate Perimeter

- ✓ *Evaluation of internal and external infrastructure security.*
- ✓ *To know the weak and strong points, in order to implement improvements.*
- ✓ *Know the real perimeter and identify security breaches.*
- ✓ *Take into account all the devices that access, protect and monitor. (Management, control and reconfiguration of assets).*



Best Practices

- ✓ *Cloud usage inventory. Risk assessments. Authorization lists.*
- ✓ *Staff training and procedures.*
- ✓ *Protect through an additional layer, the data directly.*
- ✓ *Establish zero trust security strategies and monitor compliance.*
- ✓ *Review configuration. Strong passwords and 2FA*



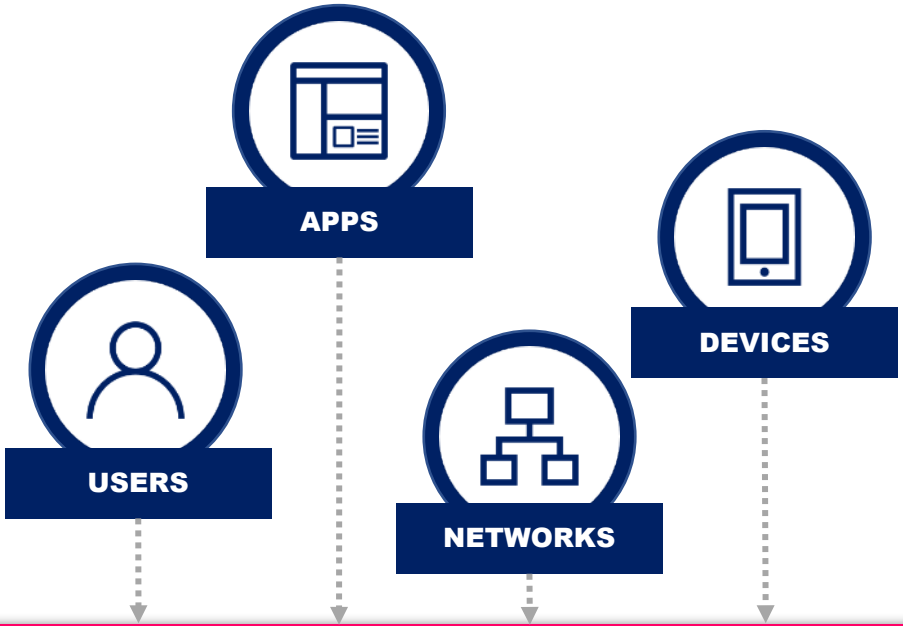
Security Solutions

- ✓ *Encryption through digital rights management (IRM).*
- ✓ *Multi-factor authentication (MFA).*
- ✓ *Network Detection and Response (DLP).*
- ✓ *Cloud Access Security Managers (CASB).*
- ✓ *Information and Event Management Systems (SIEMS).*
- ✓ *Endpoint Detection and Response (EDR) systems.*
- ✓ *Encrypted Remote Connection (VPN) or Remote Desktop (RDP).*

sealpath

The "moat and castle" model no longer works

Data security must be at the core of our data protection strategy.

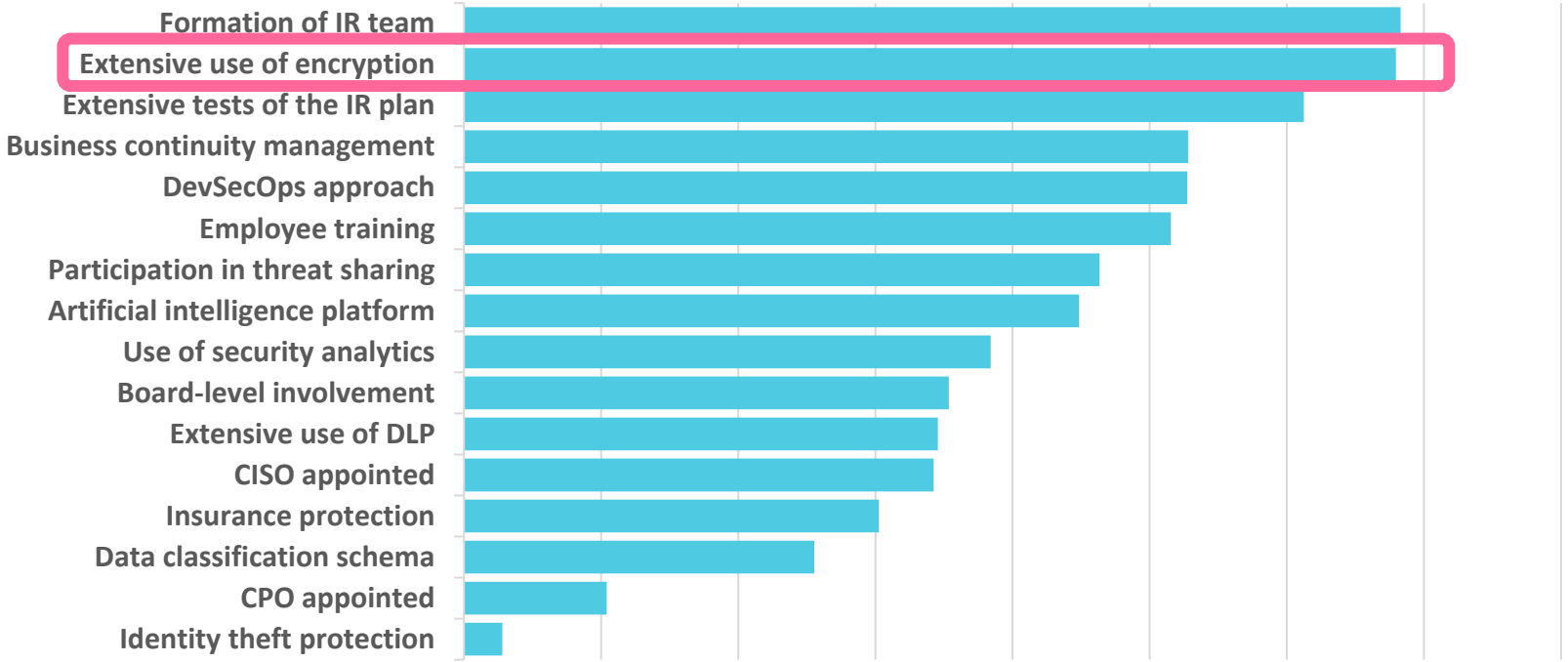


You can put up a wall, set up powerful perimeter defenses and spend a lot of resources maintaining them.

However, in the era of perimeter-less organizations, information can be anywhere and security must travel with the data.

Data encryption must be available to everyone

Factors that mitigate the cost and impact of a data leak

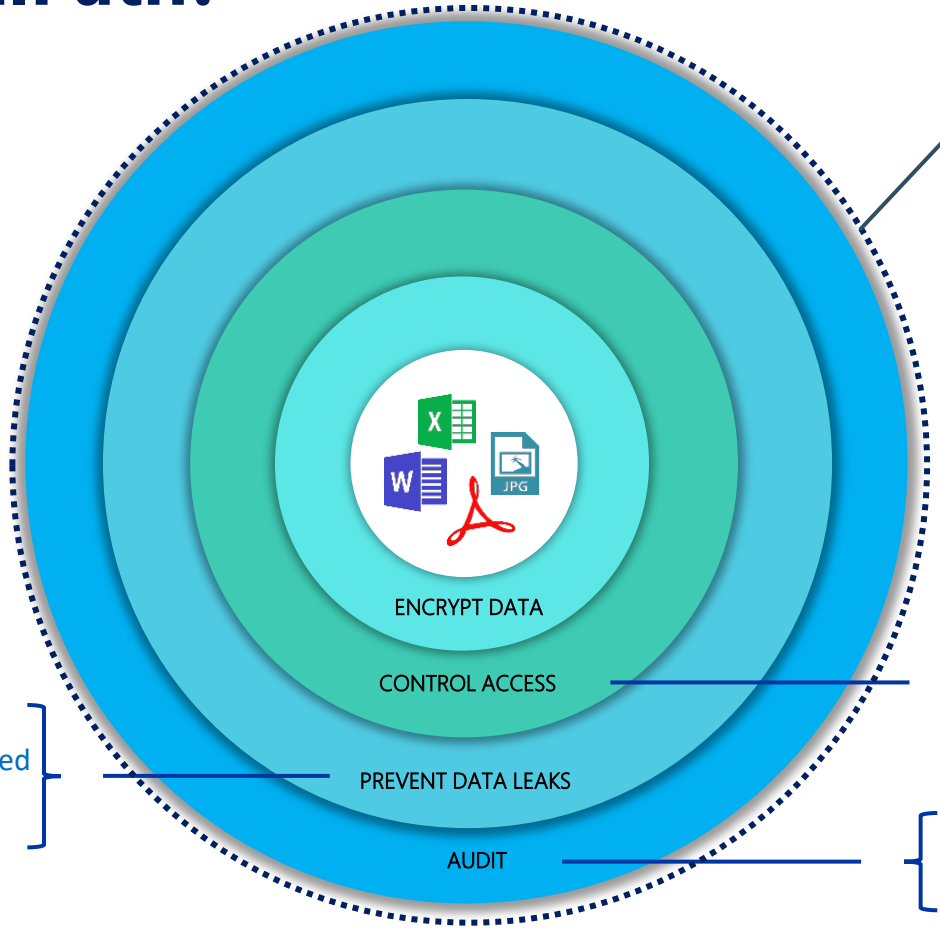


Source: IBM-Ponemon Institute. Cost of data breach report 2019

What is SealPath?

*SealPath **protects** your documents and allows you to **control** them remotely*

What is SealPath?



Integrity of communication

Who accesses, Permissions (View, Edit, Print, etc.)

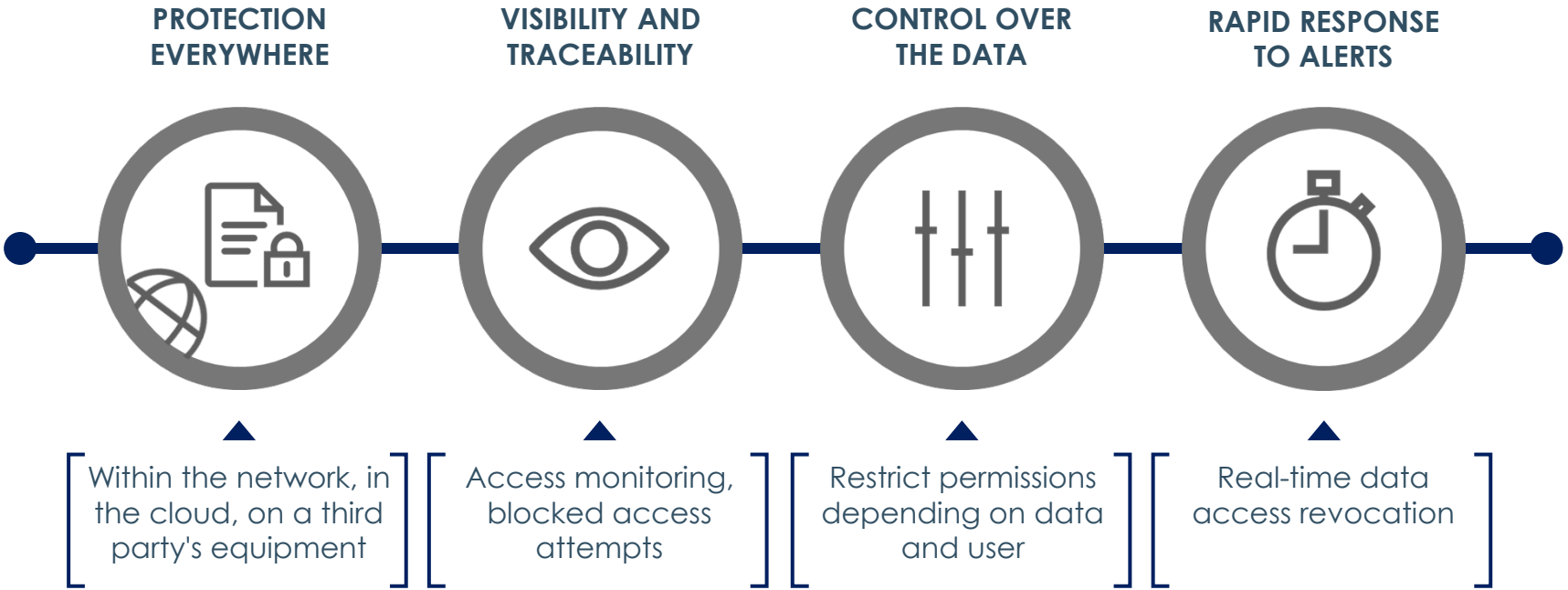
Document can be revoked remotely

Accesses, blocked access attempts, etc.

sealpath

www.sealpath.com

Advanced Security



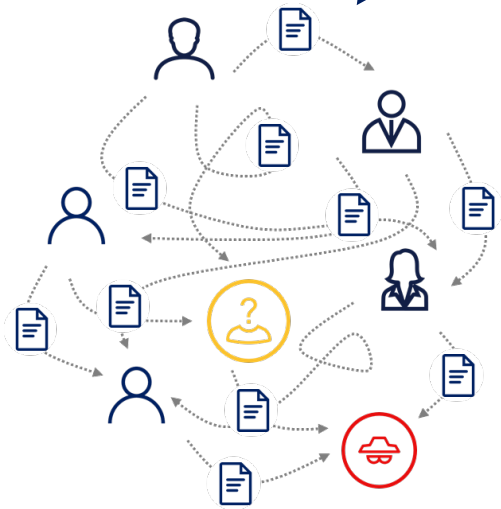
Protection based on Circles of Trust

Safe collaboration and control within the Circle of Trust

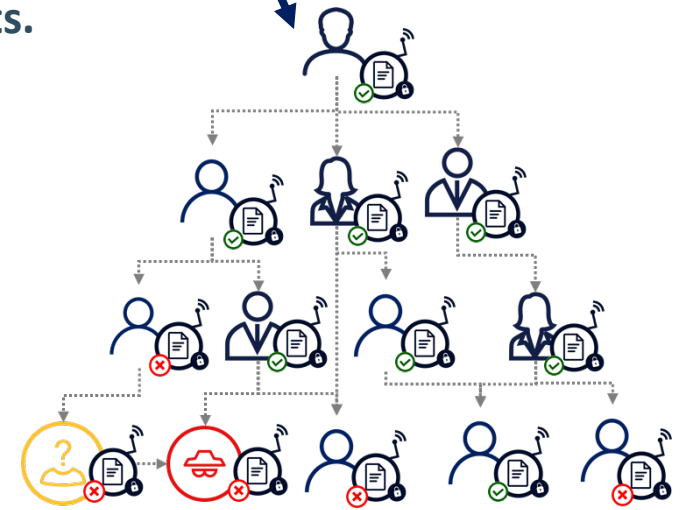
sealpath

Uncontrolled use vs controlled use

Information travels without control, but access can be limited to micro-segments.



≠



Secure Collaboration

With protection that travels with the file

SECURE TRANSFER

Anonymity is avoided.
The sender is identified.
End-to-end encryption

SECURE SHARING

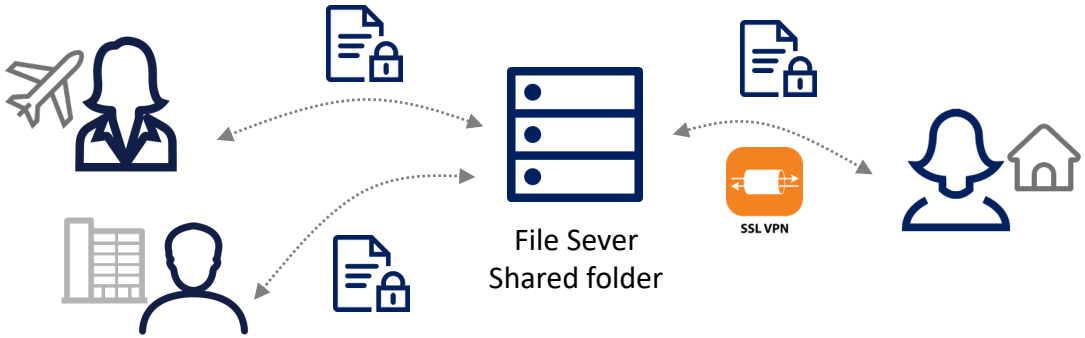
Permissions per user.
Access tracking.
Ability to revoke access

SECURE COLLABORATION

Ability to Edit
Collaboration level
controlled in real time.

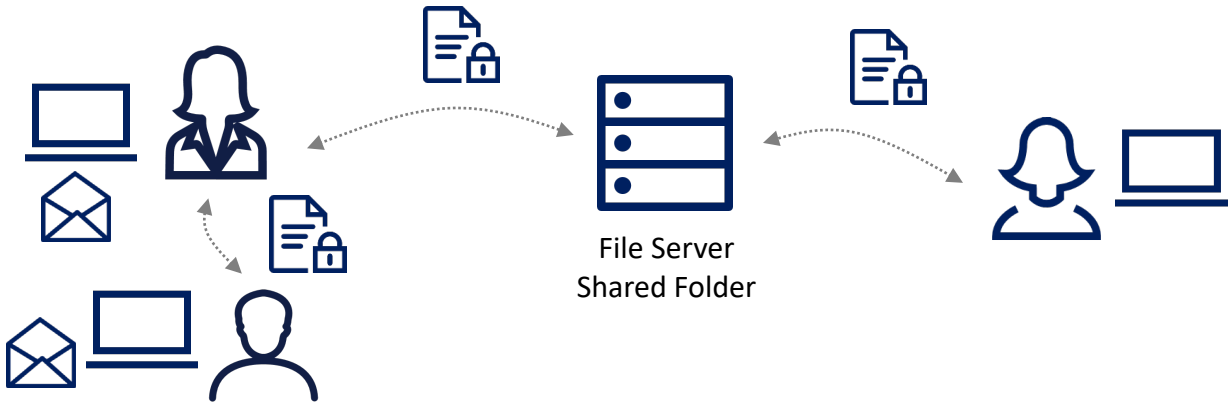
Use Case 1: HR – Sensitive Information

- ✓ Type of documentation: **Payroll, compensations, salaries, taxes,** etc**.**
- ✓ Scope: Internal HR.
- ✓ Location: File Server.



Use Case 2: Management – Sensitive Information

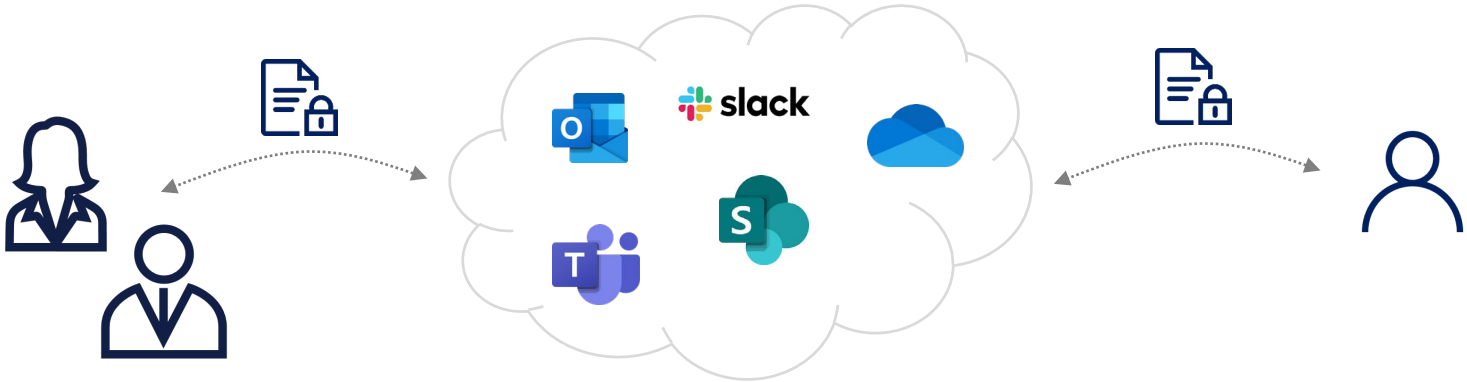
- ✓ Type of documentation: **Minutes, reports, contracts, etc. High confidentiality.**
- ✓ Scope: Internal – Top Management.
- ✓ Location: File Server + PCs + Email.



sealpath

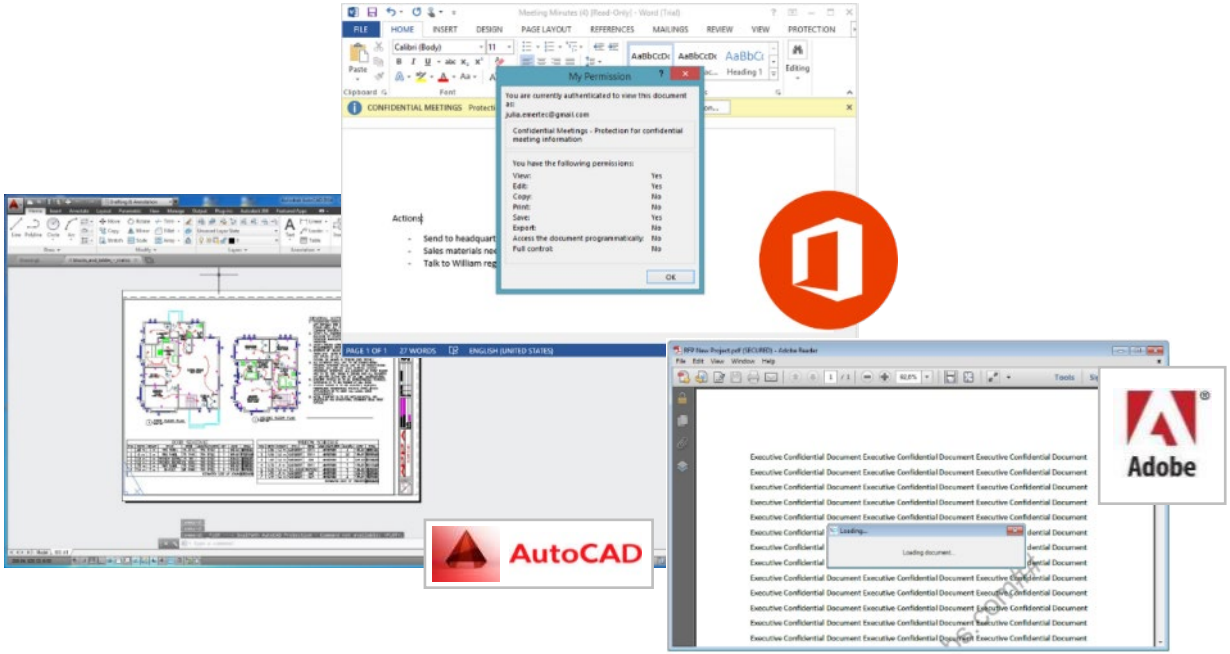
Use Case 3: Collaboration – Sensitive Information

- ✓ Type of documentation: **Product Information, Guides, Processes, Customer Details, etc.**
- ✓ Scope: Internal and External partners.
- ✓ Location: File Servers + PCs + Email + Collaboration apps + Devices.



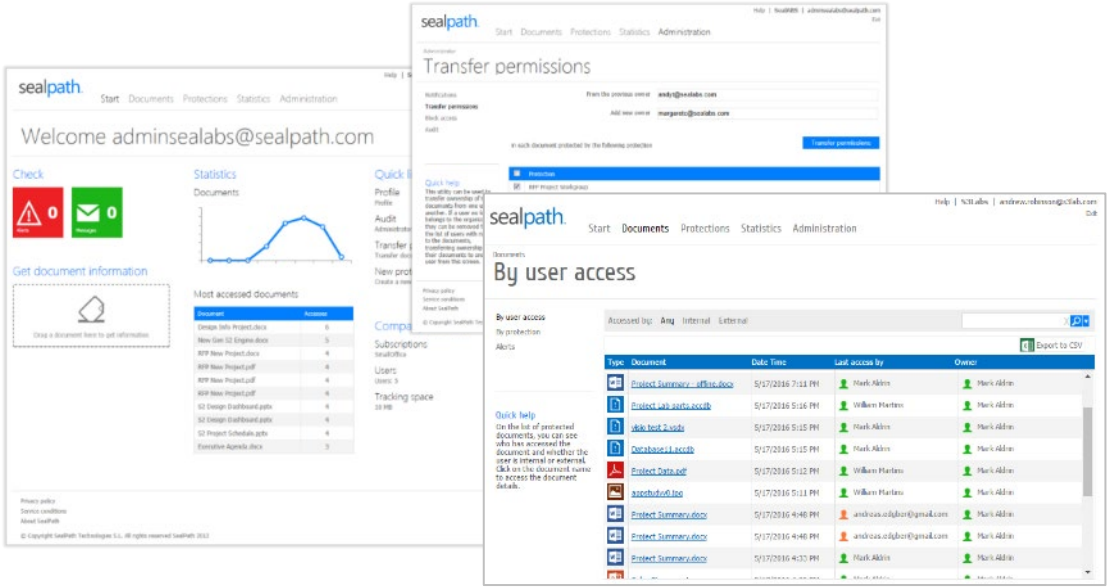
Ease of use

Use your usual tools, without any agent



Ease of management

Flexible policies, control and audit



Deployment

TWO OPTIONS

can be installed

On-Premise

Cloud/SaaS

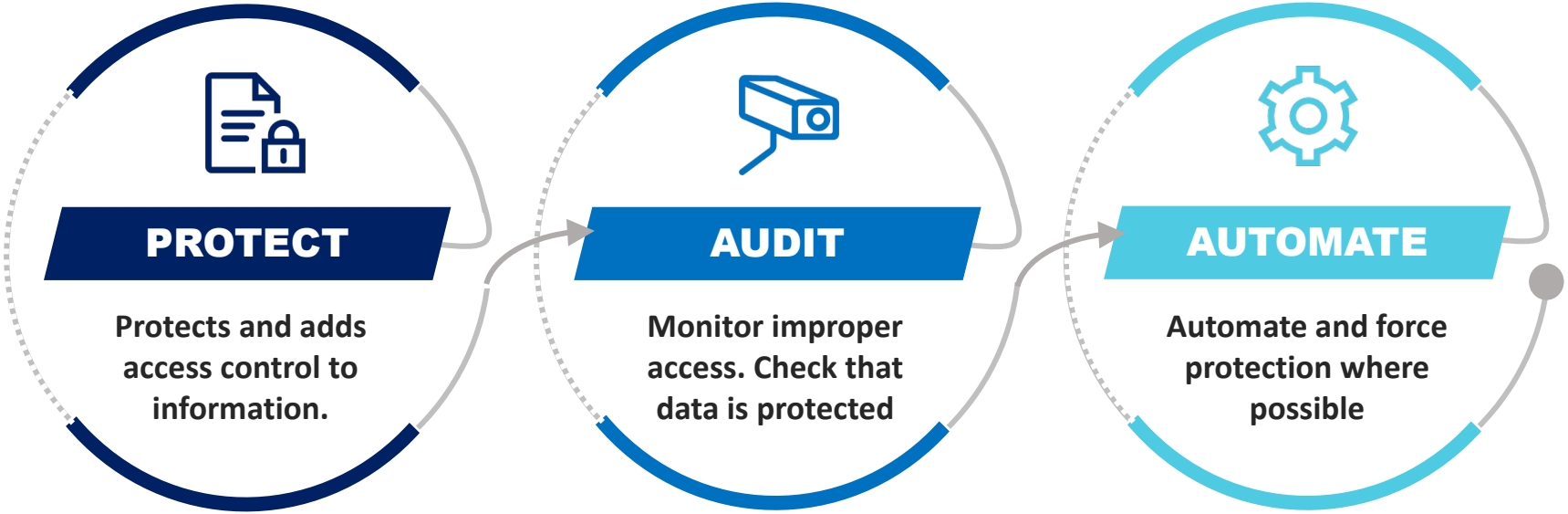
Both can be integrated with AD/LDAP
A Protection Client is installed in Desktop or File Servers

SealPath **doesn´t store documents**. Just protect them

Automation of Protection

Secure Management Cycle of the Information Life Cycle

SealPath recommendation for working with sensitive information



Extends a culture of protection within the organization.

About SealPath

+20 Countries *100% Channel-Oriented* *Strong Focus on R&D*

Some customers

SIEMENS Gamesa RENEWABLE ENERGY
ARKEMA INNOVATIVE CHEMISTRY
Claro
GENERAL DYNAMICS Land Systems
T-Systems
Dipharma Since 1949
LOEWE LOUIS VUITTON
Dietsmann Maintaining Energy
BANCO DE ESPAÑA Eurosistema
SUEZ
ONTARIO POWER GENERATION
SUPERMICRO

Alliances Integrations

FORCEPOINT
McAfee
Symantec.
Bitdefender
AUTODESK

sealpath

SMART PROTECTION FOR SENSITIVE DATA

SMART PROTECTION FOR SENSITIVE DATA AND SECURE COLLABORATION

Thank you!.

Contact: sandrine.roux@sealpath.com