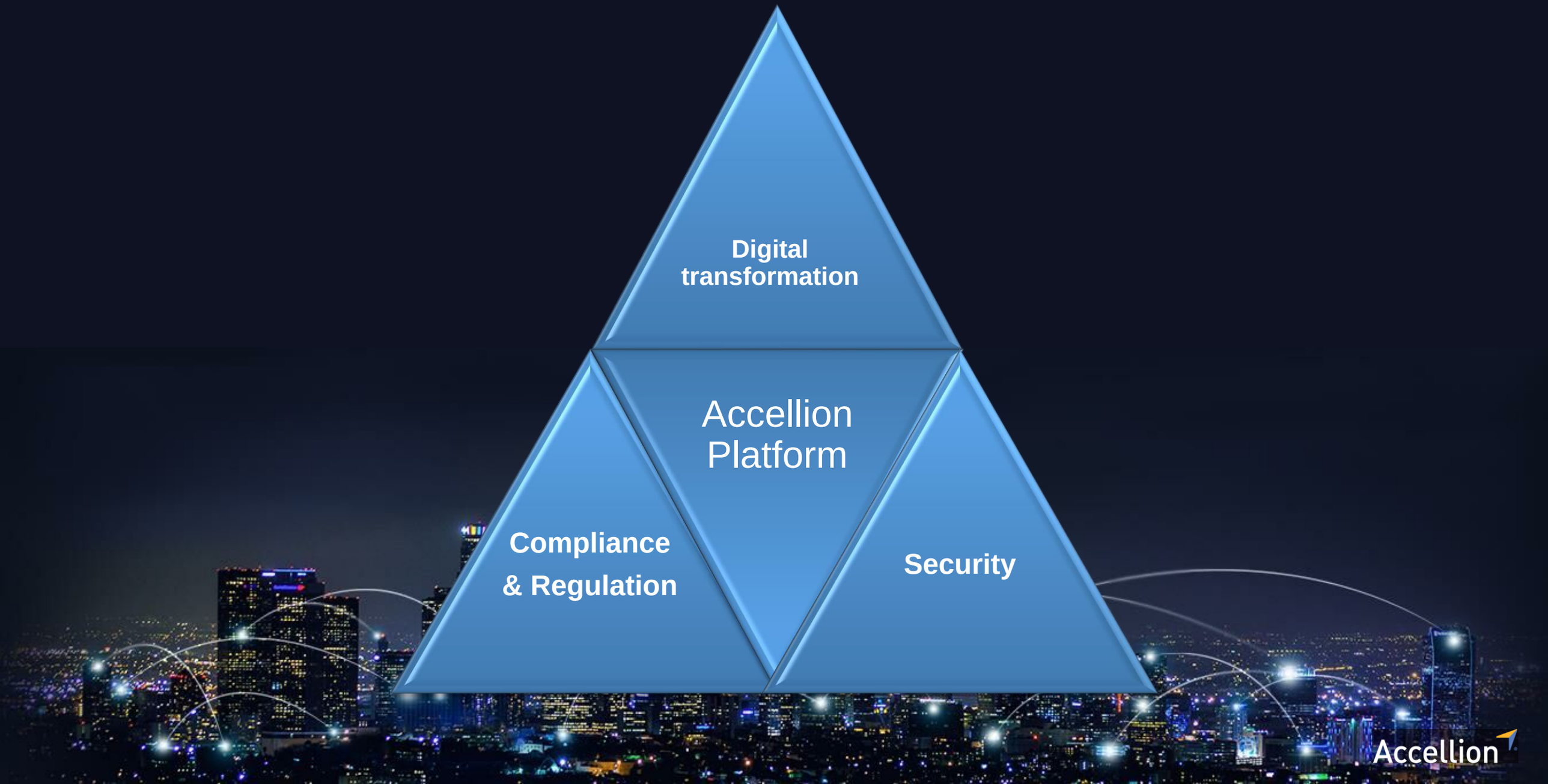
Secure content communication

Revisiting Israel requirements

The Unique Accellion approach



Accellion

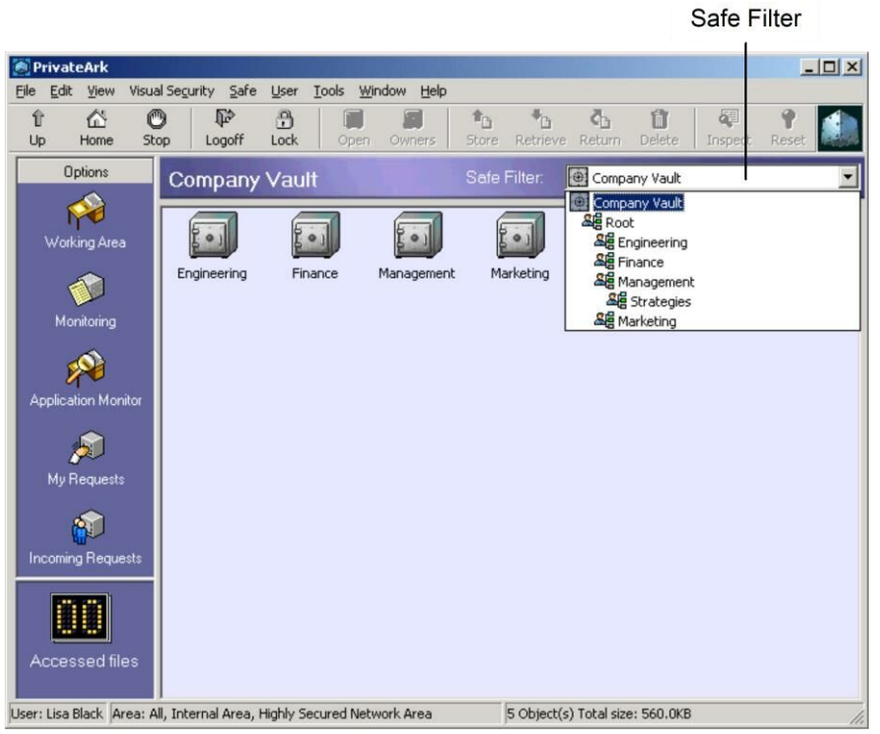
TODAY’s dependencies in CyberArk

Healthcare

Financial

Accellion

CyberArk Vault in every Enterprise in Israel !

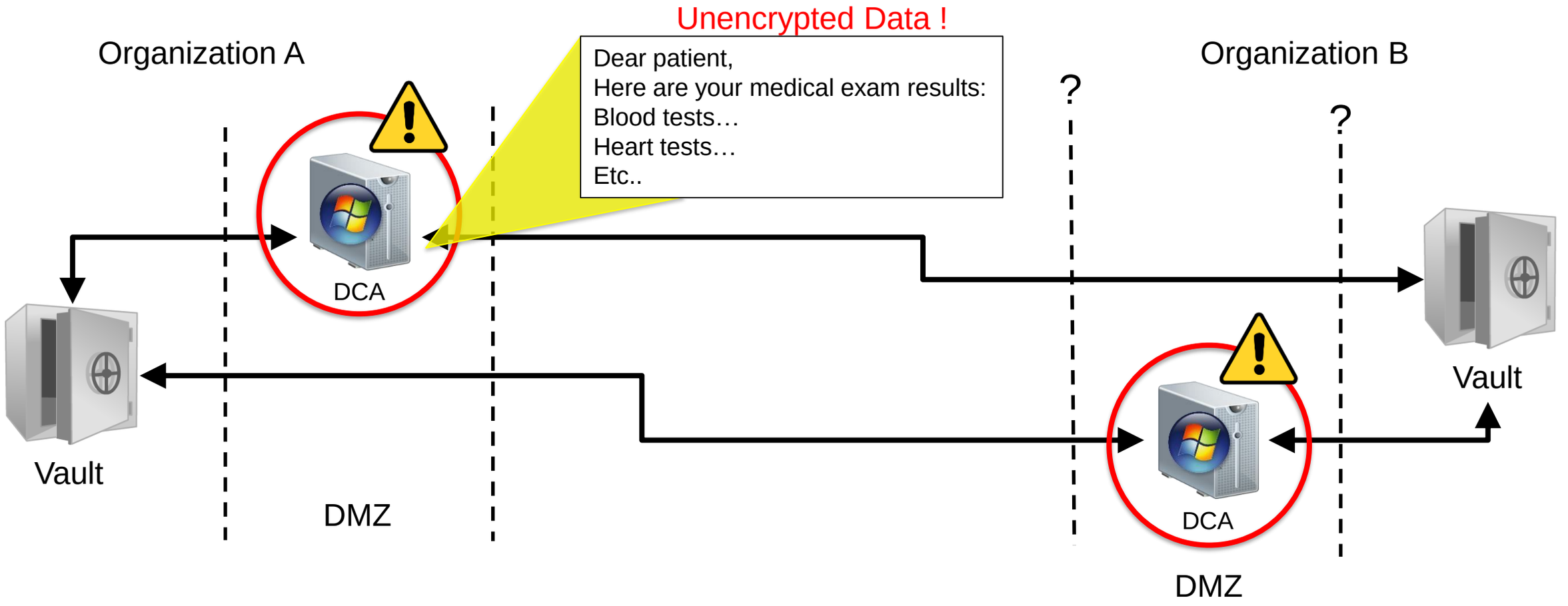


Accellion

Current situation

- CyberArk provided secure vaults and variety of interfaces.
- Based on the those interfaces system integrators developed unsecure automation processes which annulled the underlying CyberArk security infrastructure (which was state of the art at that time).
- When these processes were designed, it was satisfactory for the early 2000s, but insufficient for today
- Management of these best practices created a huge ecosystem of support and services.
- CyberArk did not enforce security measurements and it was left to the implementers.

TODAY:
DCA – The actual file transfer component: A Massive Weak Link



- ⚠ DCA is an MFT tool running on a Windows machine <u>not a vendor-hardened appliance</u>
- ⚠ The DCA sees all transmitted <u>content in the clear</u> and can change (delete, add,…) the vault's content
- ⚠ DCA installation practices often <u>skip setting security restrictions</u>

Google

cyberark dca

All Images Maps News Videos More Settings Tools

About 28,100 results (0.34 seconds)

[PDF] DCA התקנת

https://www.misim.gov.il › kasefet › webClient › PDFfiles ▾ Translate this page

.3. כרגע ., בתיקיה .C:\Program Files**CyberArk**\Utilities .קיים. קובץ .UserName_abc.cred ., .יש
.לשכפל. אותו ולשנות את השם. של. אחד מה. קבצים. ל: .4 . .UserName.cred

CyberArk Powers Flexible, Reliable Governed File Transfer ...

https://www.cyberark.com › press › cyberark-powers-flexible-reliable-gov... ▾

Sep 30, 2009 - Automated **DCA** workflows with remote FTP and SFTP servers: By supporting Distribution Collection Agent (**DCA**) workflow automation to ...

[PDF] נוהל התקנת DCA בשרת - משרד החינוך

https://sites.education.gov.il › cloud › home › Documents ▾ Translate this page

May 3, 2015 - The minimum system requirements for the **CyberArk DCA** are as follows: ... The **CyberArk DCA** requires a **CyberArk** Digital Vault, version 5.5 or ...

Downloads - Bulwarx

https://www.bulwarx.com › downloads ▾

Easily manage your local **CyberArk DCA** service. Create credentials files. Reset credentials files password. Monitor DCA settings & health. FREE from Bulwarx!

Antivirus Exclusion List : CyberARk - Reddit

https://www.reddit.com › CyberARk › comments › antivirus_exclusion_list ▾

r/CyberARk: Technical talk, news, and more about CyberArk Privileged Account ... DCA. C:\Program Files**CyberArk****DCA**. One-Click Transfer. C:\Program ...

CyberArk · GitHub

https://github.com › cyberark ▾

CyberArk, the undisputed leader in Privileged Account Security, secures secrets used by machines and users to protect traditional and cloud-native apps.

Google

cyberark dca

All | Images | Maps | News | Videos | More | Settings | Tools

About 28,100 results (0.34 seconds)

[PDF] DCA התקנת

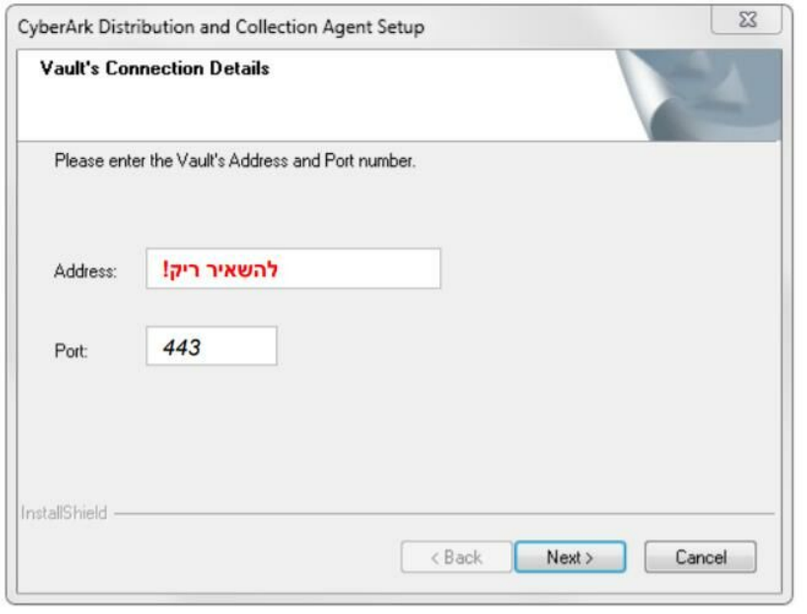
https://www.misim.gov.il › kasefet › webClient › PDFfiles ▾ Translate this page

.3 כרגע. ., בתיקיה. C:\Program Files**CyberArk**\Utilities. קיים. קובץ .UserName_abc.cred ., .יש
.לשכפל. אותו ולשנות את השם. של. אחד מה. קבצים. ל: 4. . .UserName.cred

misim.gov.il/kasefet/webClient/PDFfiles/DCA.pdf

Spotify | AWS Sign-In | EffectiveIT | How to measure cy... | 2net ...לוח - לוח שנה | ABC Lounge Music... | jeromebei — Bitbuc... | פאוורבול

5 / 8



להשאיר את השדה **Address** ריק

ובשדה **Port**:443

ולהתקדם עם Next

CyberArk Powers Flexible, Reliable Governed File

https://www.cyberark.com › press › cyberark-powers-flexible-reli

Sep 30, 2009 - Automated **DCA** workflows with remote FTP and SFTP se
Distribution Collection Agent (**DCA**) workflow automation to ...

[PDF] נוהל התקנת DCA בשרת - משרד החינוך

https://sites.education.gov.il › cloud › home › Documents ▾

May 3, 2015 - The minimum system requirements for the **CyberArk DCA**
CyberArk DCA requires a **CyberArk** Digital Vault, version 5.5 or ...

Downloads - Bulwarx

https://www.bulwarx.com › downloads ▾

Easily manage your local **CyberArk DCA** service. Create credentials file
password. Monitor DCA settings & health. FREE from Bulwarx!

Antivirus Exclusion List : CyberARk - Reddit

https://www.reddit.com › CyberARk › comments › antivirus_exclu

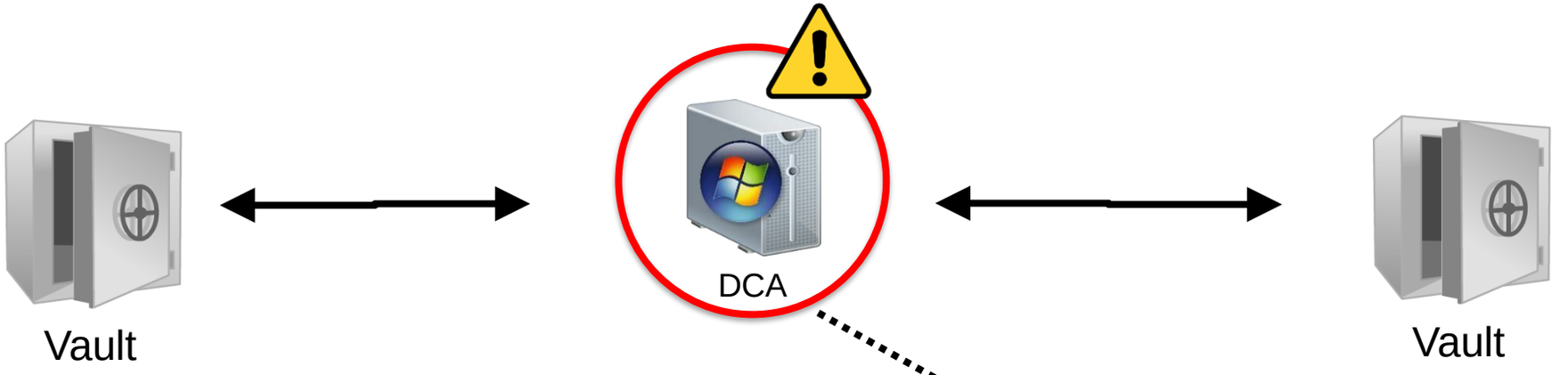
r/CyberARk: Technical talk, news, and more about CyberArk Privileged A
C:\Program Files**CyberArk****DCA**. One-Click Transfer. C:\Program ...

CyberArk · GitHub

https://github.com › cyberark ▾

CyberArk, the undisputed leader in Privileged Account Security, secures
machines and users to protect traditional and cloud-native apps.

TODAY:
DCA – The actual file transfer component: A Massive Weak Link

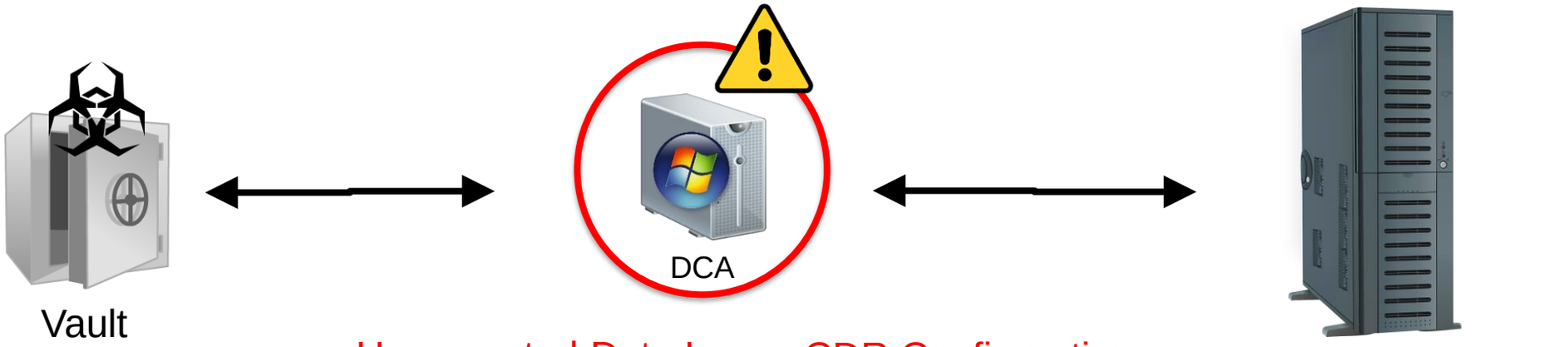


File transfer flow
Can be manipulated !

```
<local script>
    save_copy_of_file("\\HIDDEN_SRV\My Documents");
</local script>
```

My Documents

TODAY:
Same DCA – used for Sanitization (HALBANA)



Unencrypted Data !

Dear patient,
Here are your medical exam results:
Blood tests…
Heart tests…
Etc..

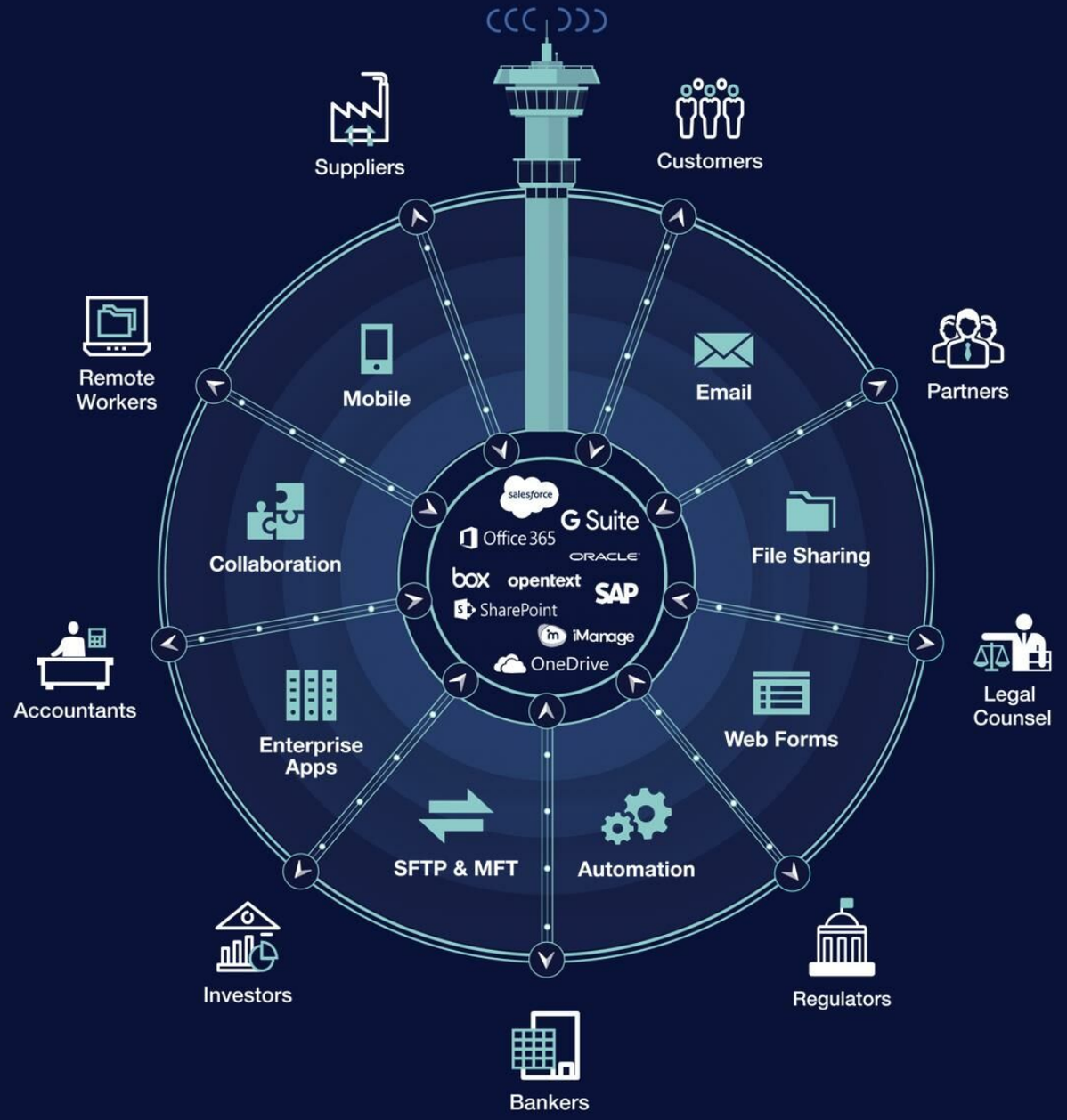
CDR Configuration
Can be manipulated !

```
<local script>
    return file_Is_Clean = always true;
</local script>
```

TODAY Problem statement

- Customers use CyberArk for file transfer mainly, ignoring security aspects
  - DCA is usually in corporate Domain → Every Sys admin can access it
- CyberArk vaults are protected, but interfaces allow unsecure transfer practices.
- Interfaces allow unsecure or less secure protocols (FTP, FTPS)
- Automation processes by system integrations annuls security:
  - Distribution and Collection Automation agent runs on any Windows machine (not hardened)
  - Files are stored for a period of time on a file system in the clear.
  - Registration and authentication of a DCA client can be compromised
- External parties may not even have any protection
  “I have a Safe” (No you don’t)

SECURE CONTENT COMMUNICATION & GOVERNANCE PLATFORM



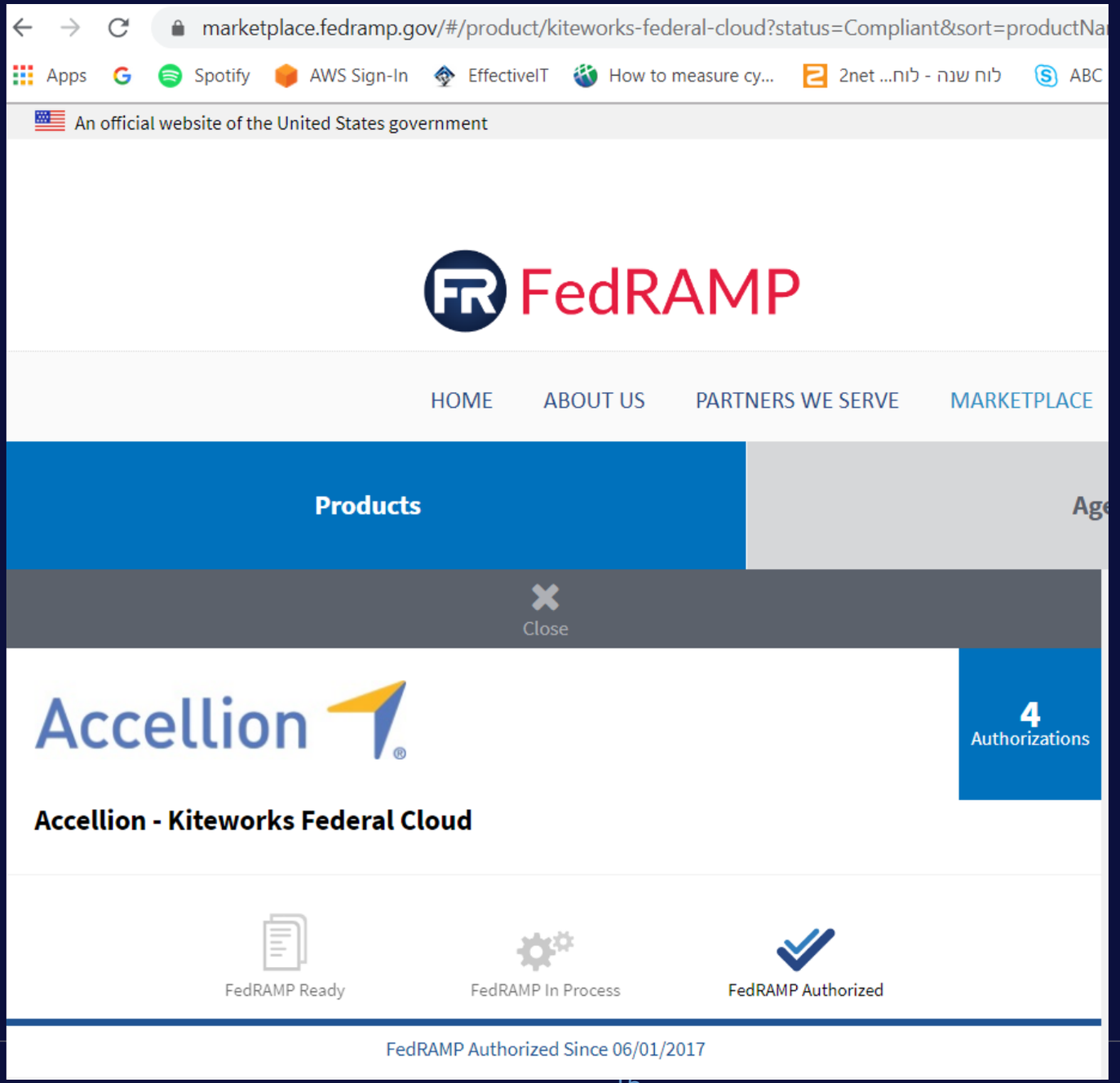
פלטפורמת Accellion

Accellion

Security

Strict security

1. Hardened appliance (virtual or physical)
2. CVSS scoring and ongoing security patches (Vendor demands)
3. Annual Penetration tests and bounty program (Vendor demands-Fedramp)
4. Direct vault to vault secured transfer (Architecture guidelines)
5. File and folder encryption at rest (Software functionality)
    1. Control over ciphers and keys
6. Secure protocols only
7. Full audit trail
    1. See and control all content exchanged with partners and third parties


marketplace.fedramp.gov/#/product/kiteworks-federal-cloud?status=Compliant&sort=productNa
Apps
Spotify
AWS Sign-In
EffectiveIT
How to measure cy...
2net ...לוח - לוח שנה
ABC
An official website of the United States government
FedRAMP
HOME
ABOUT US
PARTNERS WE SERVE
MARKETPLACE
Products
Close
Accellion
4
Authorizations
Accellion - Kiteworks Federal Cloud
FedRAMP Ready
FedRAMP In Process
FedRAMP Authorized
FedRAMP Authorized Since 06/01/2017

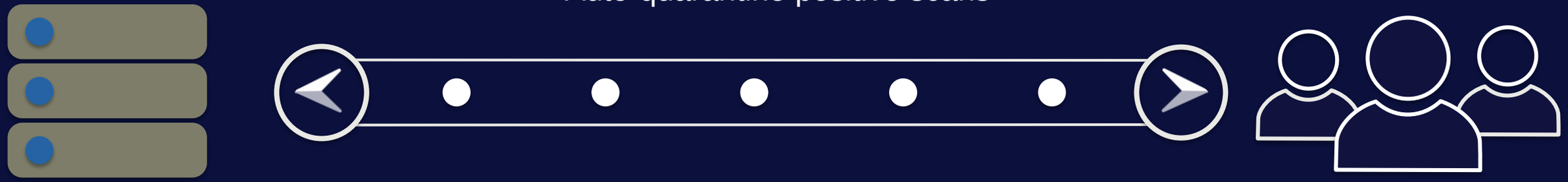
Accellion

Block External Threats with Defense in Depth

Protect against unauthorized access, infected payloads, network breaches, and ransomware

Block Malicious Content

- Embedded anti-virus scanner
- Leverage your ATP server
- Auto-quarantine positive scans



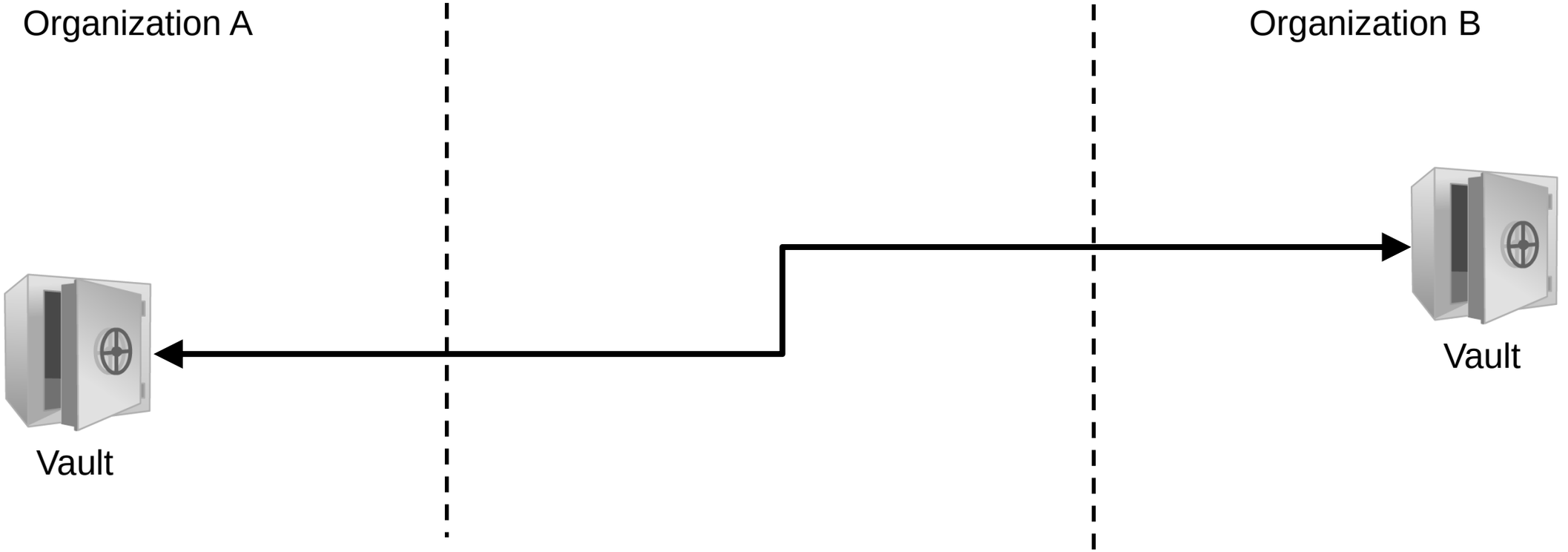
Defeat Server Attacks

- Hardened virtual appliance
- On-premise, private cloud or FedRAMP
- Bring your own keys

Prevent User Impersonation

- 2-Factor authentication
- Least privilege permissions

Secure Content Communication Architecture: Fully Hardened Path



- ☑ Each vault is a hardened appliance subject to regular audits, scanning and penetration testing and regular security updates

Security Analytics

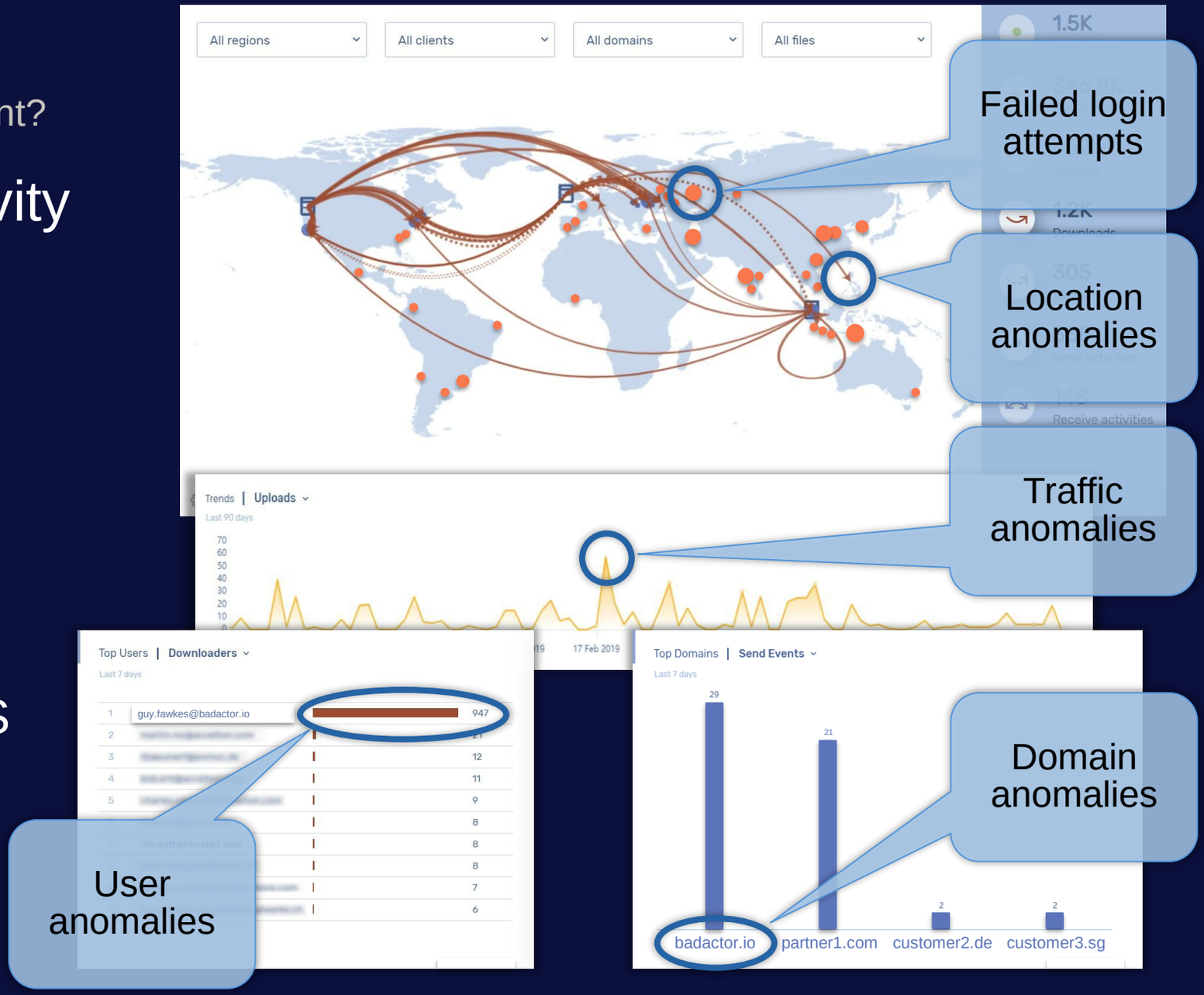
Where in the world is your sensitive content?

Visualize all third party activity

- Inbound, outbound, internal
- Real-time and historical
- Who, what, where…

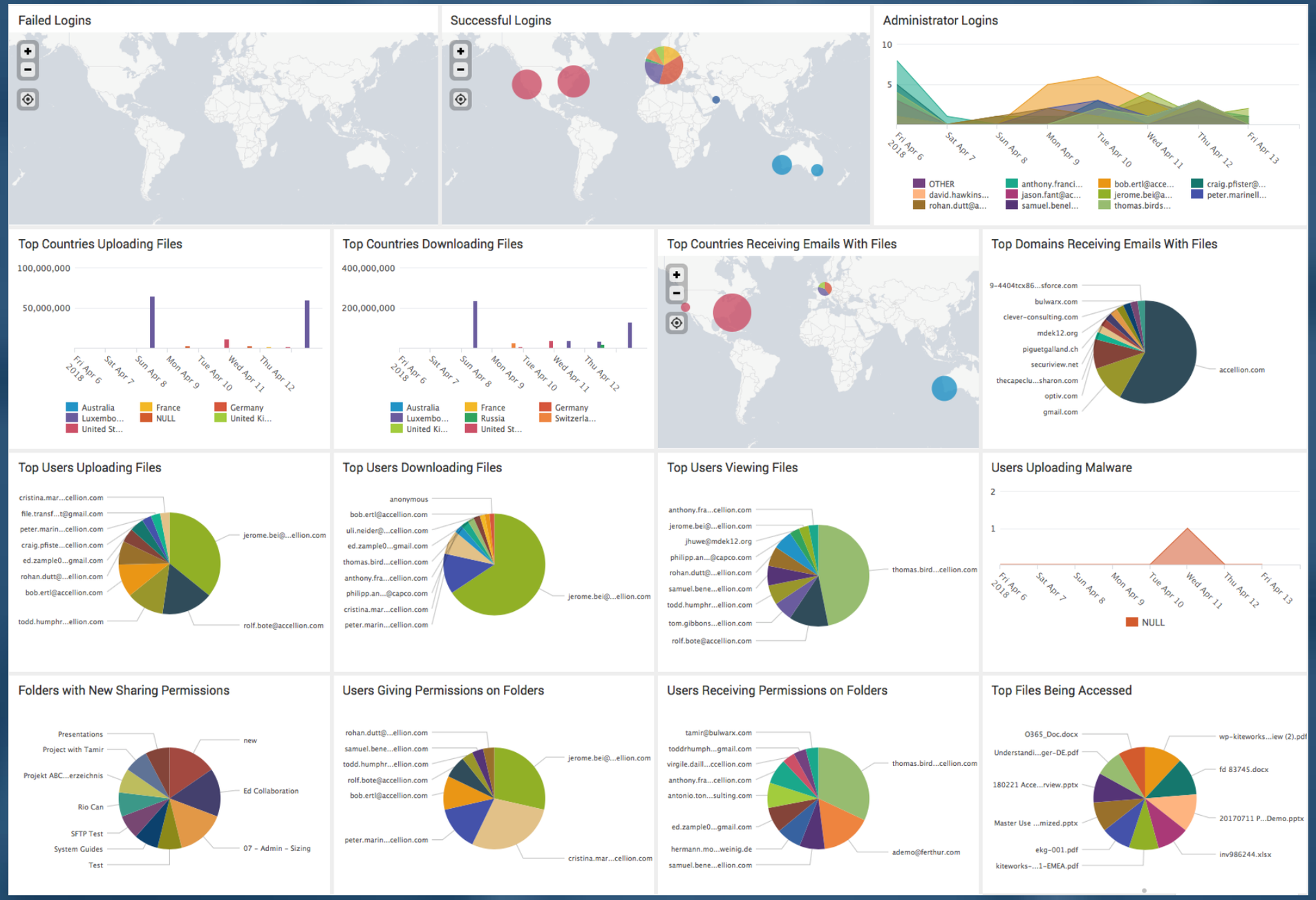
Detect leaks and breaches

- Identify behavior anomalies
- Failures: DLP, ATP, logins, IDS
- Automatically detect threats with machine learning



Accellion

SIEM Integration Example - Splunk



Compliance

Accellion

Strict compliant security with Certification !

NIST 800-53 compliant security & privacy

- Strong encryption in transit and at rest
- Encryption key ownership and rotation
- Physical security SOC 2 attestation
- 2FA for external parties and employees
- Limit access to need-to-know individuals

Audit Reporting

Demonstrate compliance to auditors – with a single click

Ensure policy settings are right

- Account expiration and off-boarding
- Passwords, access, expiration & timeout
- Logging

Check configuration & connections

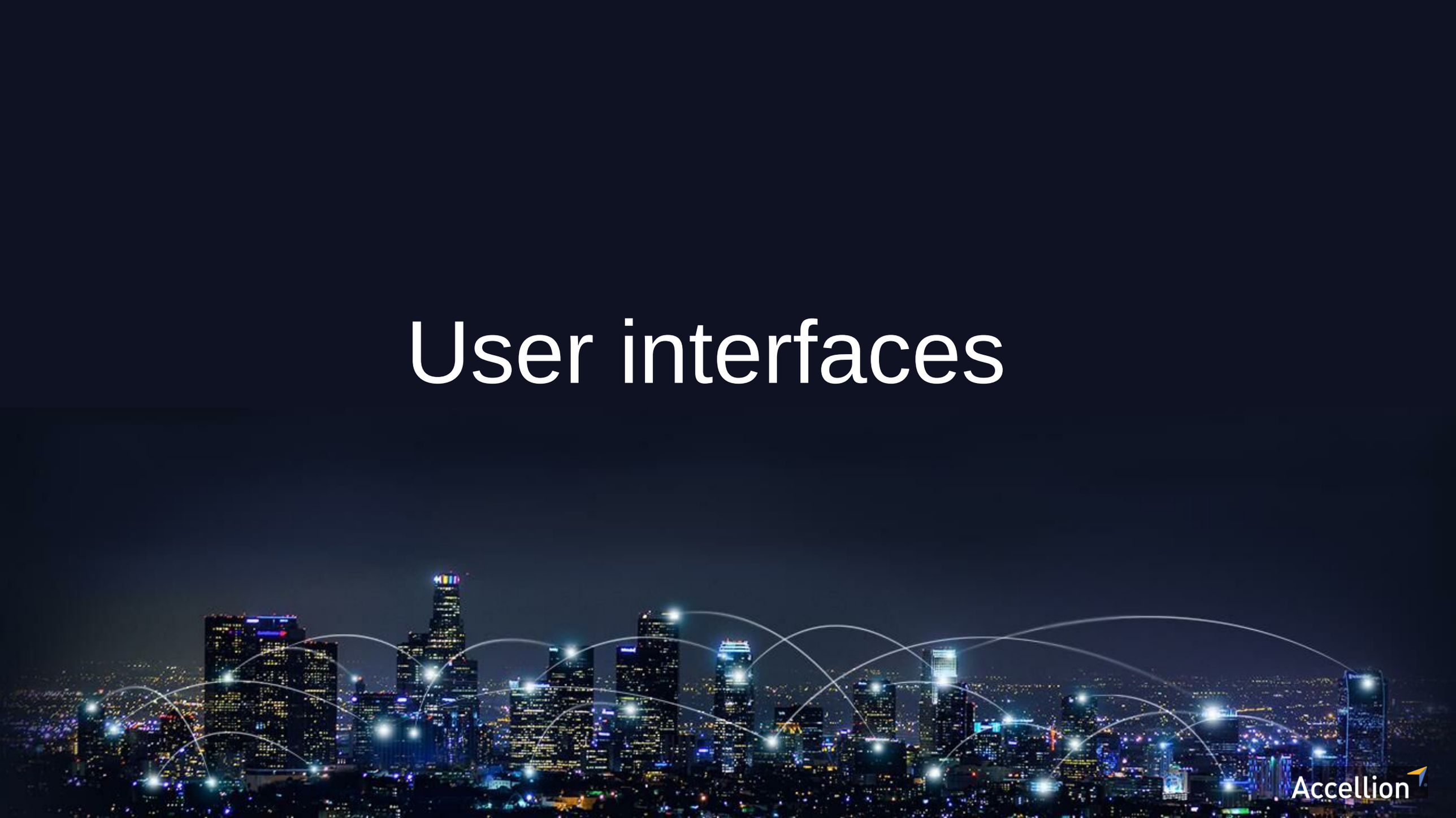
- LDAP, SSO, DLP, AV
- Replication, data sovereignty, HA

Monitor relevant operations

- Last key rotation
- Intrusion detection and critical subsystem status

Accellion

User interfaces



Accellion

SECURE CONTENT COMMUNICATION & GOVERNANCE PLATFORM

Automation interfaces

Human/manual interfaces

SFTP server

SFTP Client

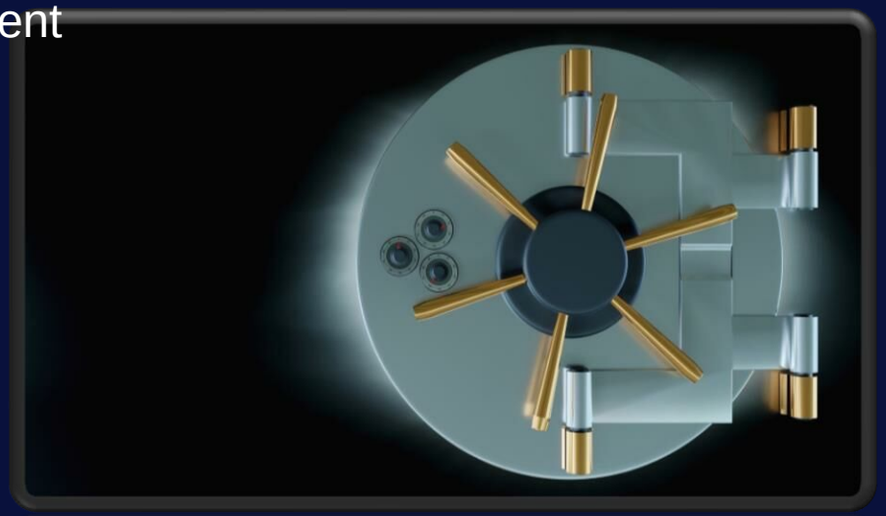
SFTP Client

SFTP

Accellion

Orchestrator

Accellion



Web portal

Outlook Add-on

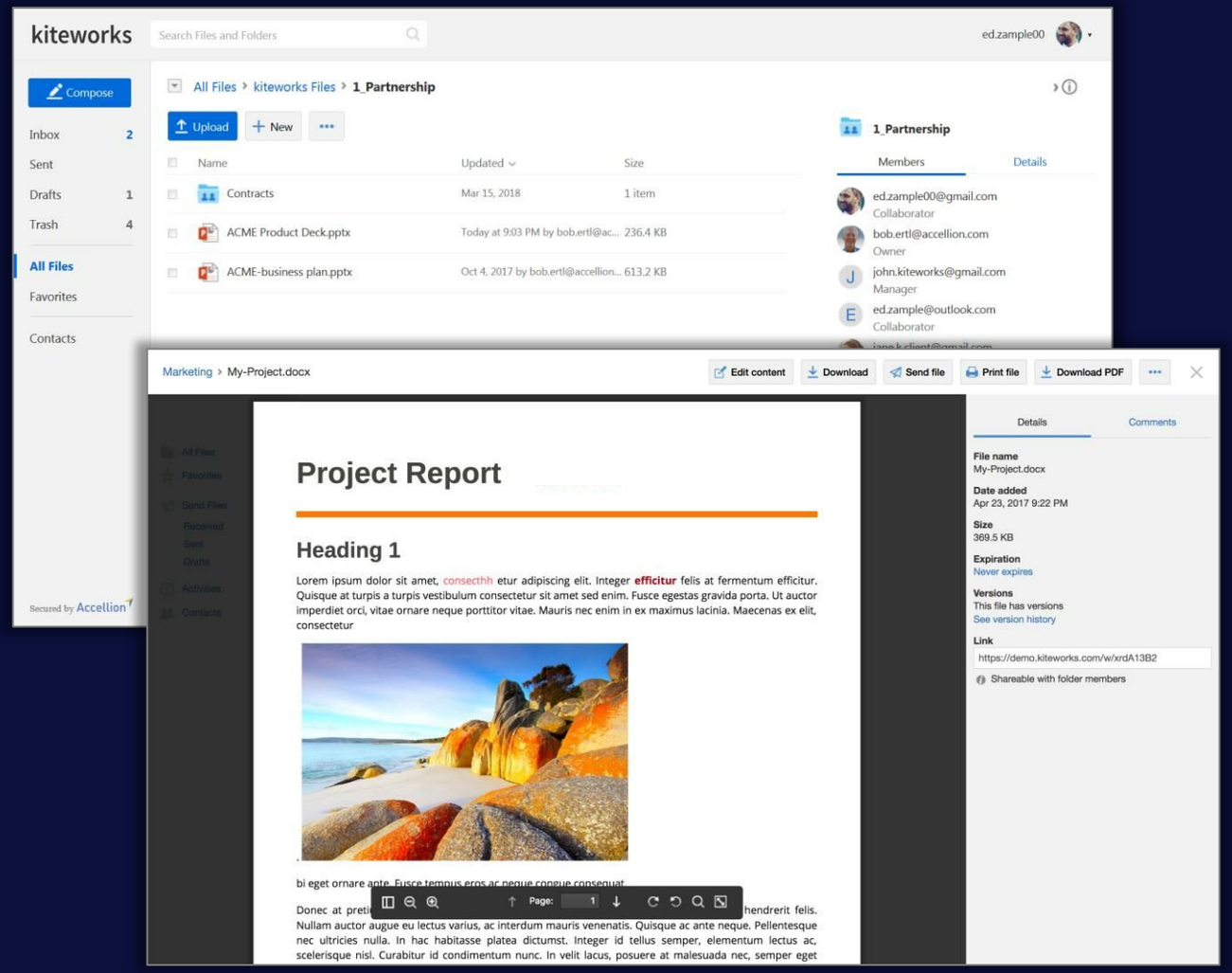
Desktop Sync. client

Office Add-ons

Mobile App

Secure File Sharing

Visibility, security and compliance for third party content communication



Protect content with least-privilege defaults

- Need-to-know, need-to-edit roles
- Watermarked, view-only for high risk parties
- Blind uploads for bids and submissions

Enterprise security, governance & compliance

- Granular, role-based policy controls
- Full audit trail, reporting and analytics
- External auth, 2FA, identity management

Ensure adoption with ease of use

- Consumer-grade user experience
- Business-led self-service folder management
- Web and mobile apps
- MS Office, G Suite, enterprise app plugins

Accellion

Enterprise Connector (OnPre + Cloud)

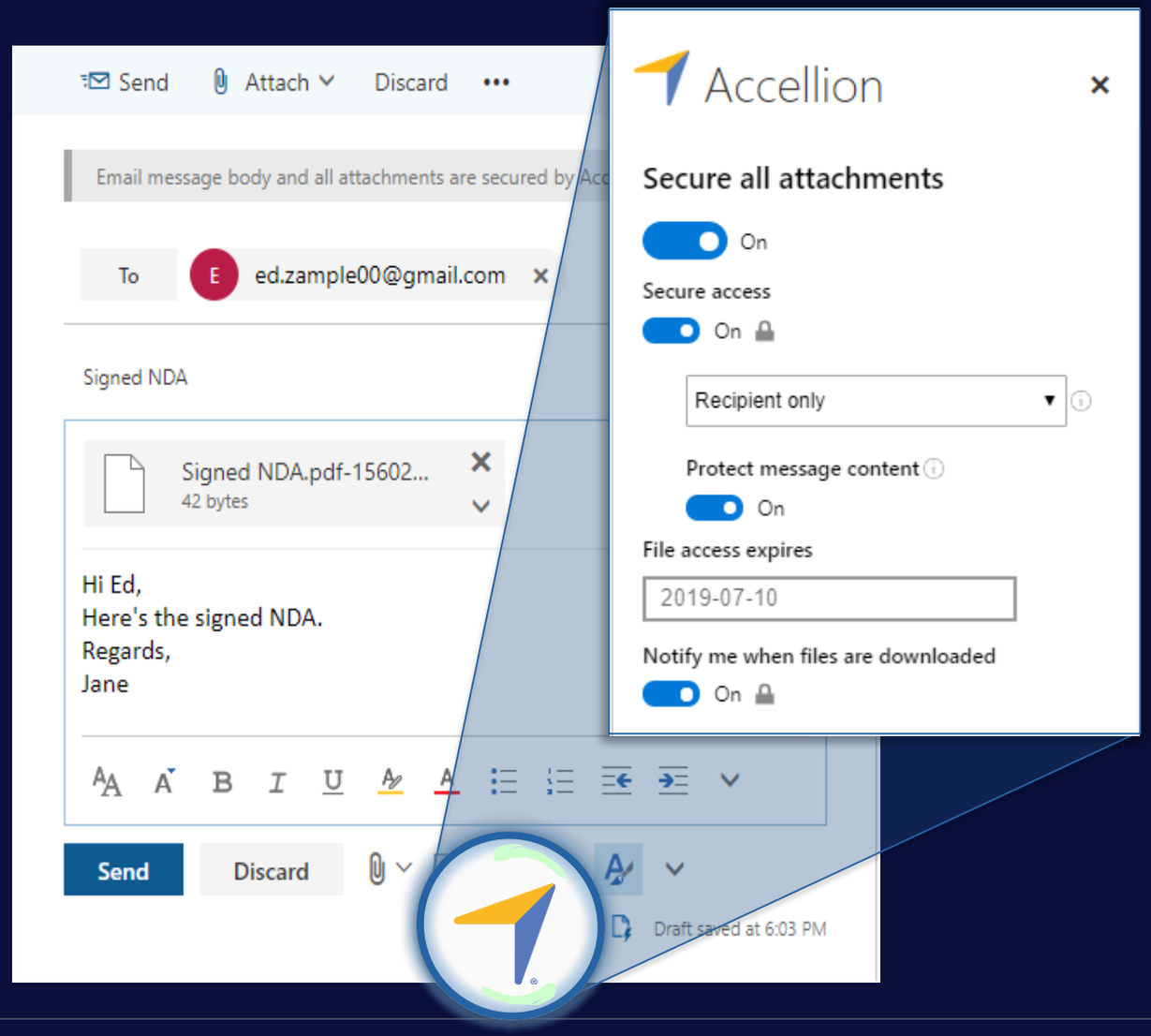
Accellion

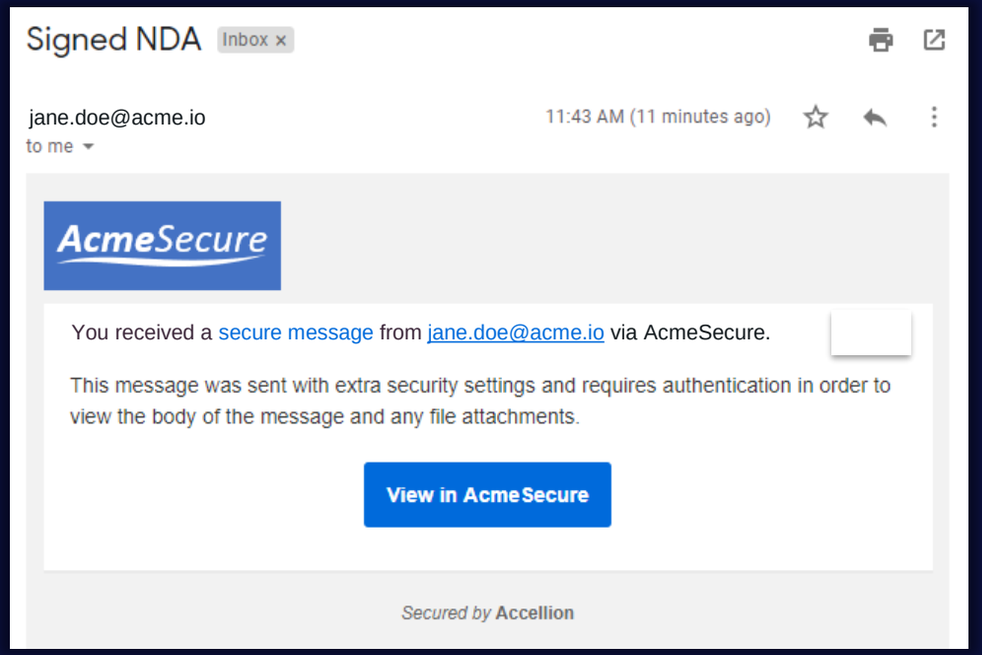
All Files

Name
kiteworks
Box
Dropbox
GoogleDrive
Google Drive
Health Care
Legal
Marketing
OneDrive for Business
Sales

Secure Email

Prevent Email Breaches & Compliance Violations



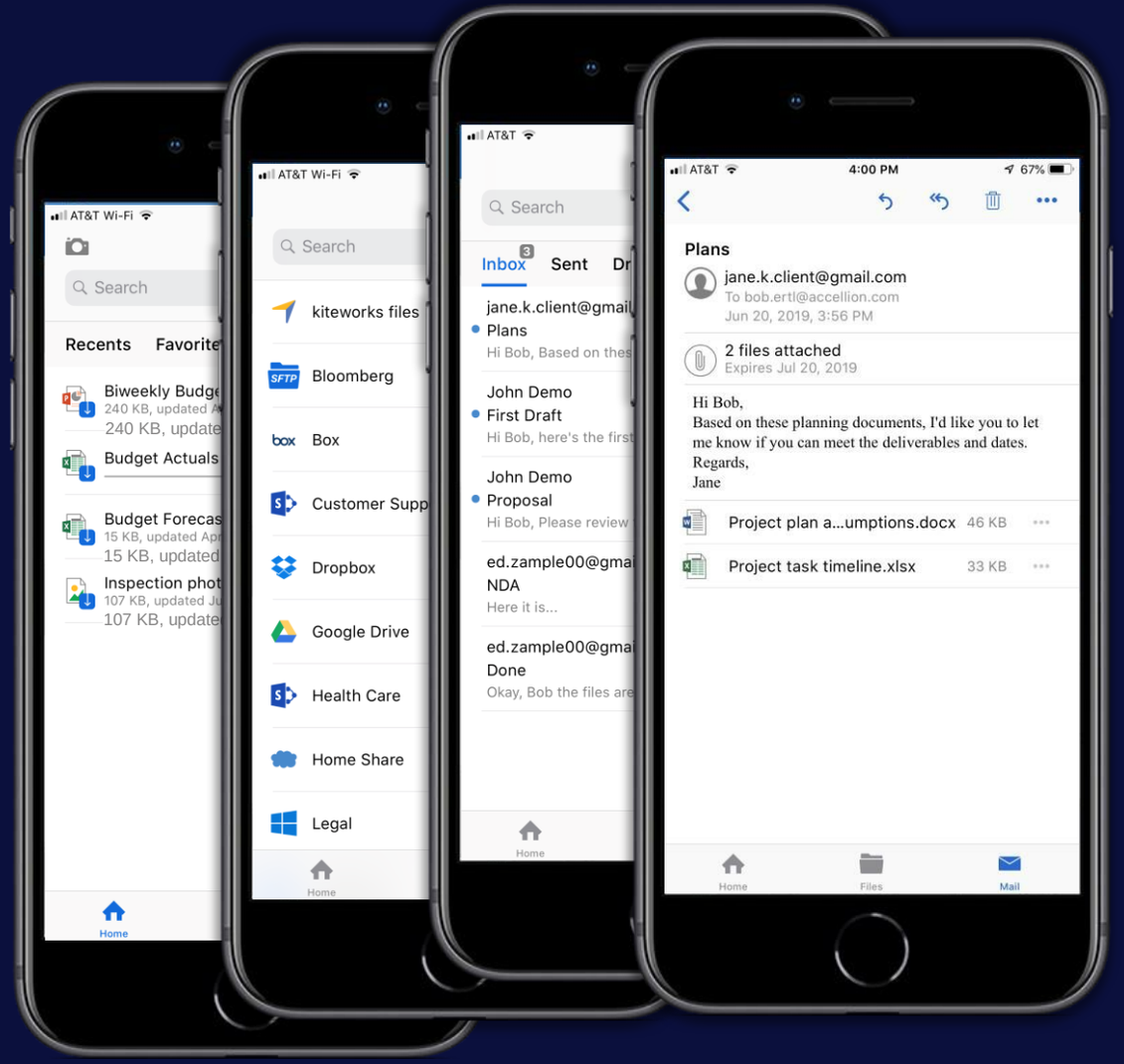


- Adopt easily in Outlook, Web, & mobile
- Encrypt all content
- Use your private storage & keys
- Third party authentication & MFA
- Centralize policy controls & audit reporting
- Detect leaks & anomalies
- Send unlimited-size files

Accellion

Secure Mobile

Ensure executives and field workers communicate securely when on the road



Secure email and shared folders

- Securely capture photos of sensitive documents, equipment, and inspections
- Access HQ content systems securely
- Familiar, fast, convenient

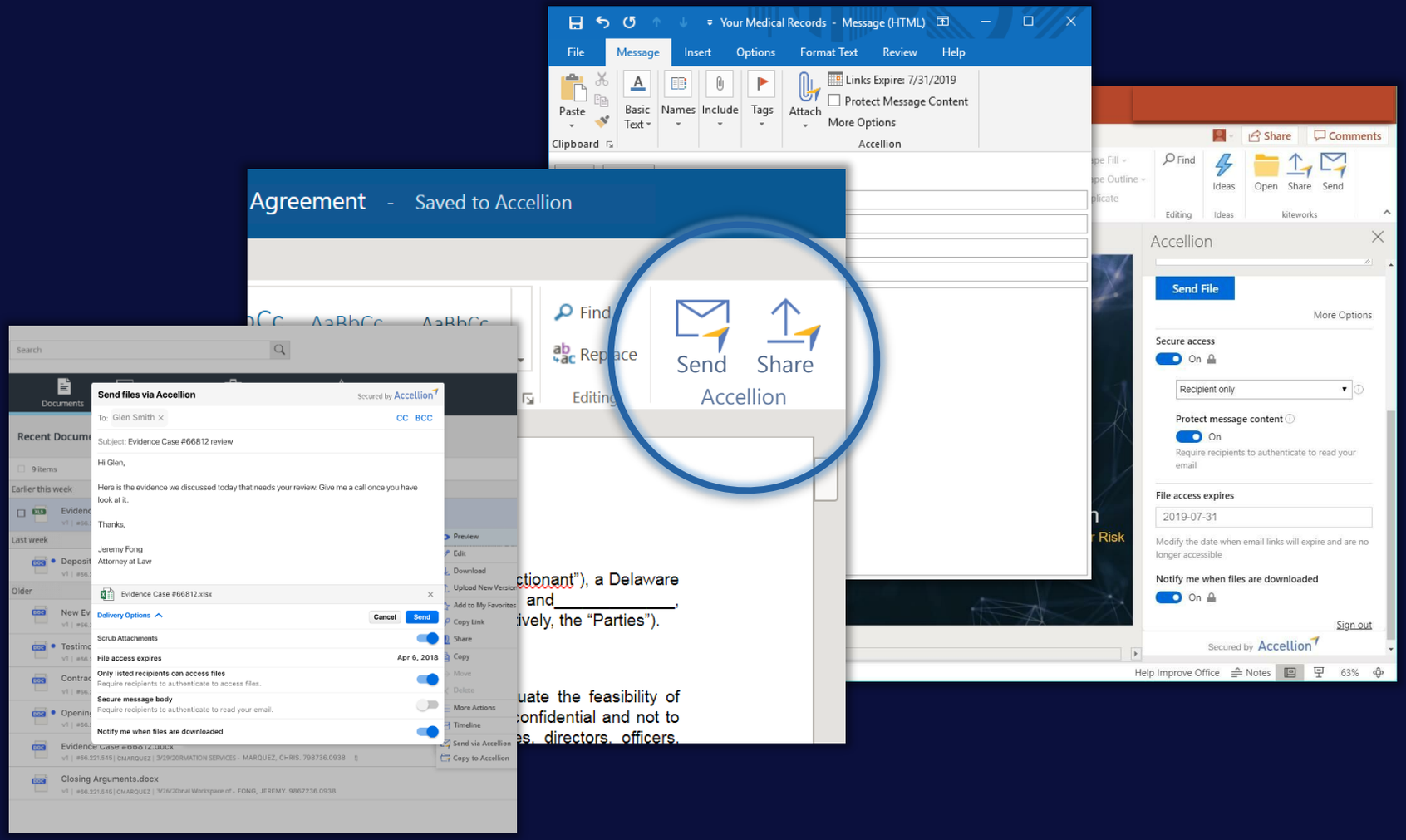
Control security, governance & compliance

- Your encryption keys
- Your secure container on their device
- Your private transmission channel
- Your storage
- Your role-based policies
- Your audit trail, logging and reporting

Accellion

Secure Office and Enterprise Plugins

Plugins everywhere employees share sensitive content with 3rd parties



Outlook

Office 365

G Suite

SharePoint

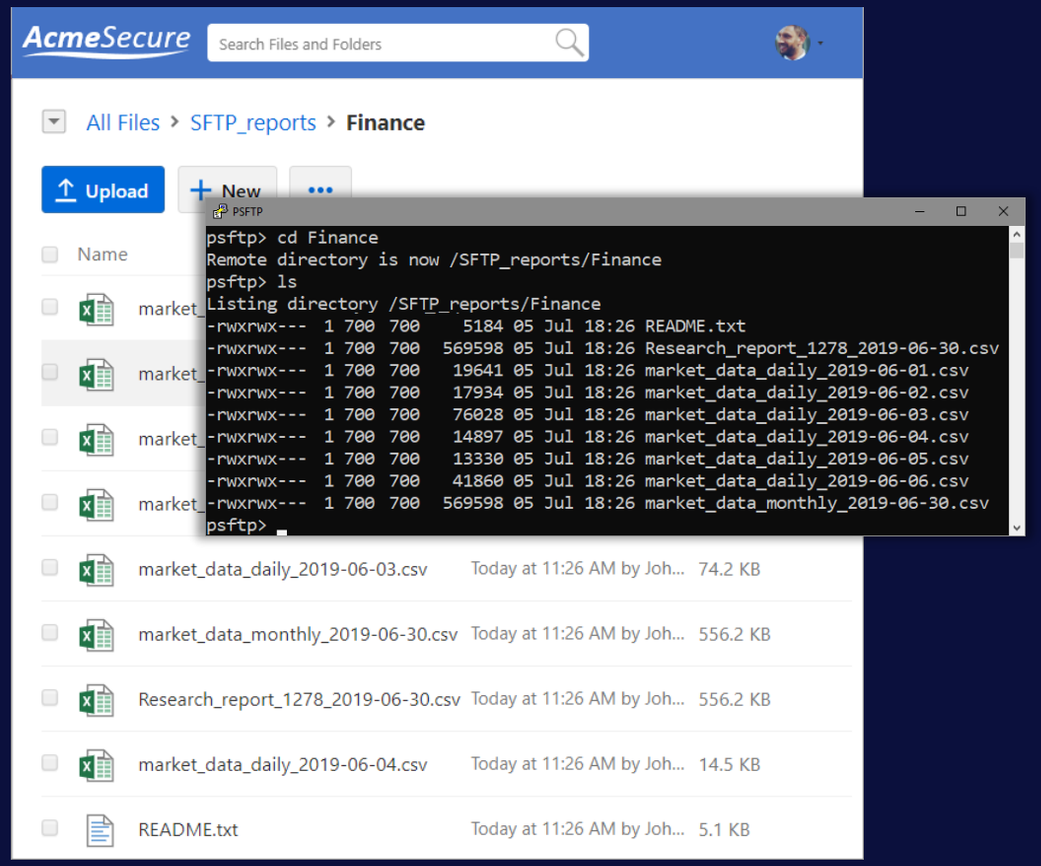
salesforce

iManage

Accellion

Governed SFTP

Reduce 3rd party cyber risk while reducing SFTP sprawl and costs



Govern access to sensitive content

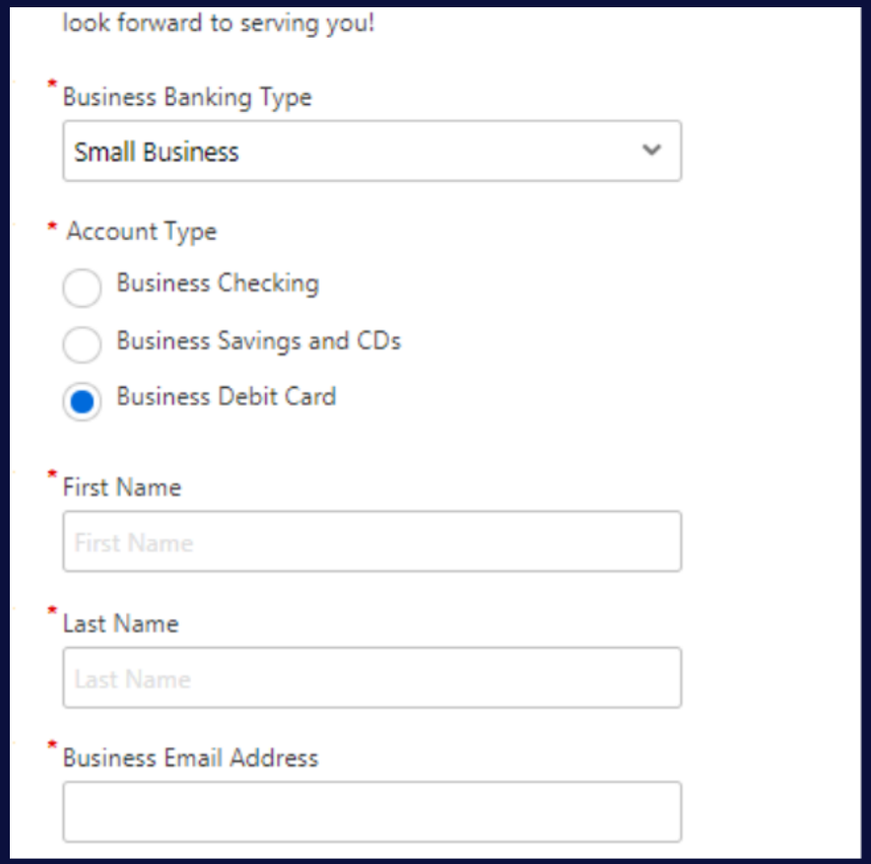
- Built in Accellion SFTP services
- Granular permissions and policies
- Centralize and simplify SFTP management
- Scale distributed cluster with high availability
- Automate routine tasks with SFTP scripts

Access legacy servers as Web folders

- Out-of-the-box SFTP connector
- Get full visibility with complete audit trail
- Share a single connection across users
- Automate secure file transfers with REST API

Secure Web Forms

Enable simple, secure submissions by customers, partners and employees



Embed secure, governed forms in Web portals

- Collect IP, PII, PHI, etc. over the Web
- Enforce security and compliance automatically
- Allow public uploads or require authentication
- Log all form submissions for full visibility

Automate workflows to ensure compliance

- Code-free automation agents
- Securely downloads attachments to a folder
- Notify users of work queued for them
- Direct post-processing scripts with form parameters

Secure Messaging – 2020 !

Automation

Streamline custom workflows and reduce costs with automation agents, scripts, and REST APIs

Accellion Orchestrator

- Leverage Accellion REST API to answer MFT use cases !

SFTP Scripting

- Leverage built-in security and governance

Email Distribution

- Ensure scan-to-email security & compliance
- Enable applications with secure email

REST API

- Create content-enabled apps and integrations
- Leverage secure content communications and administrative functions

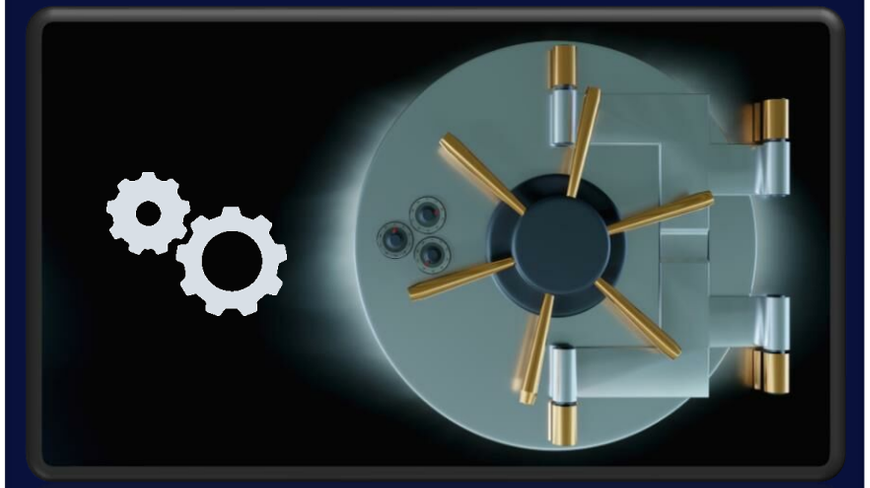
SECURE CONTENT COMMUNICATION & GOVERNANCE PLATFORM

Accellion® Orchestration

SFTP servers

Databases

CIFS/File shares



Virtual Hardened Appliance

opentext

SharePoint

OneDrive

box