



Leave No File Behind

July 2016

Disclaimer

This presentation is not an offer to sell or a solicitation of an offer to purchase securities by Zyber Secure Mobile Solutions Inc. (“Zyber”). Any such offer or solicitation, if any, will only be made by means of offering documents (e.g., prospectus, offering memorandum, subscription agreement and or similar documents) and only in jurisdictions where permitted by law. The attached material is provided for informational purposes only as of the date hereof, is not complete, and may not contain certain material information about Zyber, including important disclosures and risk factors associated with an investment in Zyber. This information does not take into account the particular investment objectives or financial circumstances of any specific person who may receive it. Before making any investment, prospective investors should thoroughly and carefully review any offering documents with their financial, legal and tax advisors to determine whether an investment is suitable for them. Securities of Zyber are a highly speculative investment and are not intended as a complete investment program. They are designed only for sophisticated persons who can bear the economic risk of the loss of their investment in Zyber and who have limited need for liquidity in their investment. There can be no assurance that Zyber will achieve its objectives. Zyber is not a reporting issuer in any jurisdiction and its securities are subject to restrictions on resale. Certain information contained herein has been provided by third-party sources and has not been independently audited or verified, by Zyber. No representation or warranty, express or implied, is made by Zyber as to the accuracy or completeness of the information contained in this document, and nothing contained in this document is, or shall be relied upon as, a promise or representation by Zyber.

Any securities described herein have not been, and will not be, registered under the U.S. Securities Act of 1933, as amended (the “U.S. Securities Act”) and may not be offered or sold in the United States except in transactions exempt from, or not subject to, registration under the US Securities Act and applicable United States state securities laws .

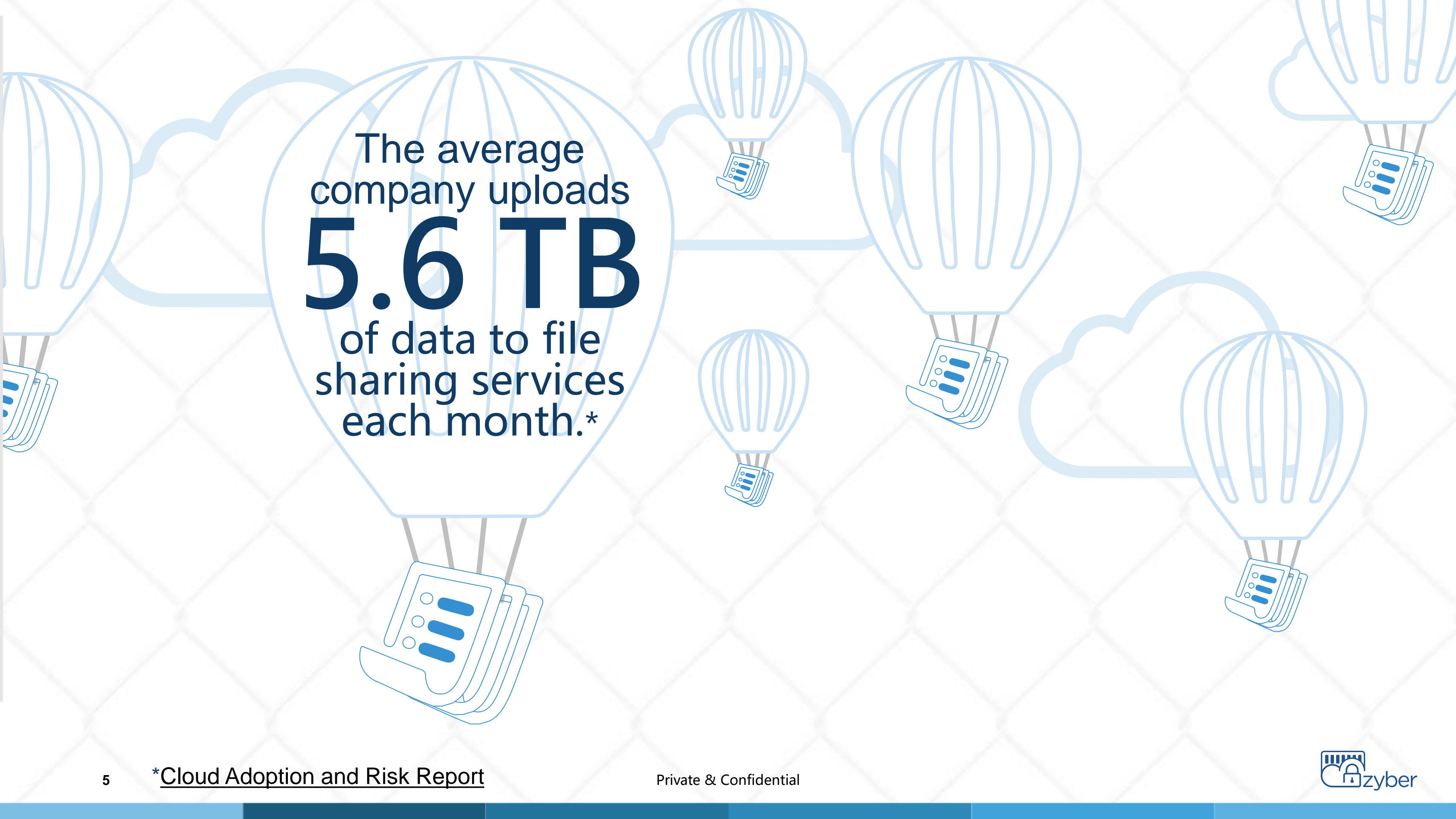
Forward Looking Statements

Certain statements contained in this presentation constitute forward-looking statements. The use of any of the words “anticipate,” “believe,” “continue,” “could,” “estimate,” “expect,” “intend,” “may,” “will,” “plans,” “project,” “should,” “target” and similar expressions are intended to identify forward-looking statements. Such statements represent Zyber’s internal projections, estimates or beliefs concerning, among other things, an outlook on revenues or other expectations, beliefs, plans, objectives, assumptions, intentions or statements about future events or performance. These statements involve known and unknown risks, uncertainties and other factors that may cause actual results or events to differ materially from those anticipated in such forward-looking statements. Zyber believes the expectations reflected in those forward-looking statements are reasonable but no assurance can be given that these expectations will prove to be correct and such forward- looking statements included in, or incorporated by reference into, this presentation should not be unduly relied upon. These statements speak only as of the date of this presentation.

Forward-looking statements included in this presentation include, but are not limited to, statements with respect to: how revenues are generated and sources of revenues; key features of the Zyber software technology and process; additional functionality to be added to the Zyber technology; the focus of capital expenditures; expansion of Zyber’s services into other countries and platforms; and future growth opportunities and strategies. Some of the risks and other factors which could cause results to differ materially from those expressed in the forward-looking statements contained in this presentation include, but are not limited to: general economic conditions in Canada and globally; technology/information security market conditions; demand for Zyber’s services; potential delays or changes in plans with respect to deployment of services or capital expenditures; possibility that government policies or laws may change; availability of sufficient financial resources to pay for the development and costs of Zyber’s services; ability to locate satisfactory industry partners; competition for, among other things, capital and skilled personnel; changes in economic and market conditions that could lead to reduced spending on encryption technology; competition in our target markets; potential capital needs; management of future growth and expansion; the development, implementation and execution of Zyber’s strategic vision; risk of third-party claims of infringement; legal and/or regulatory risks relating to Zyber’s business and strategic acquisitions; protection of proprietary information; the success of Zyber’s brand development efforts; risks associated with strategic alliances; reliance on distribution channels; product concentration; our ability to hire and retain qualified employees and key management personnel. Readers are cautioned that the foregoing lists of factors are not exhaustive. These forward-looking statements are made as of the date of this presentation and Zyber disclaims any intent or obligation to update publicly any forward-looking statements, whether as a result of new information, future events or results or otherwise, other than as required by applicable securities laws.

A person in a dark suit and patterned tie is holding a tablet. The background is a blue-tinted image of the person's hands and the tablet. Overlaid on the image is a digital network of nodes and lines, with a white cloud floating above it. The text is in white, sans-serif font, positioned on the right side of the image.

Data sharing
has become a
multi-billion dollar
nightmare
for enterprise.



The average
company uploads
5.6 TB
of data to file
sharing services
each month.*

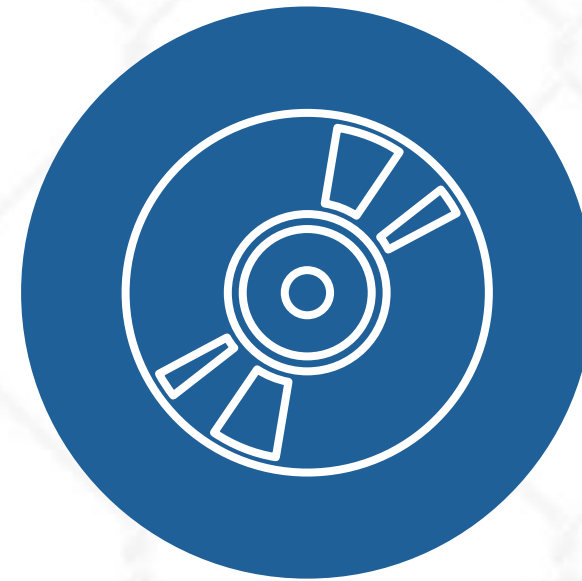
Much of that data is highly sensitive, regulated, and confidential.



Healthcare
Records



Credit Card
Information



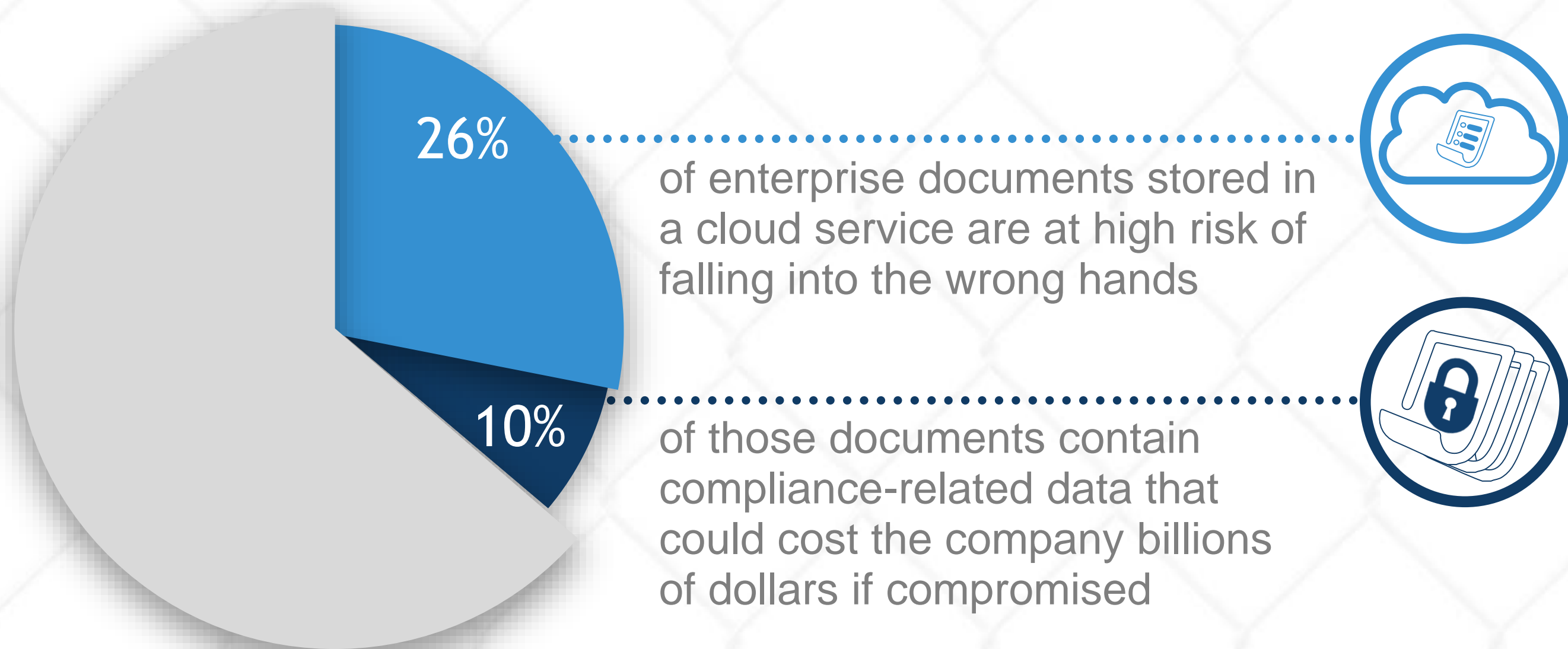
Software
Code



Enterprise R&D,
Financial,
HR Records

Collaboration puts data at high risk.

Our embrace of new ways to share information has outpaced our ability to secure it.



Seamless access to data is expected.

- In a diverse data sharing environment, that often means:
 - No visibility to where data travels once downloaded—inside and outside the enterprise
 - Danger of sensitive information being mishandled and out of compliance
 - Data is fragmented across platforms and collaboration tools, making it challenging to manage and archive

Globally, unsecured data costs business \$4B—and rising.*

Shadow IT is on the rise.

‘Shadow IT’ refers to use of software and IT services without the knowledge or consent of the company’s IT department.

- Shadow IT used to be confined to employees using non-approved Excel macros and boxed software purchased at a retail outlet
- Shadow IT is now driven by file sharing, collaboration tools, social media and cloud-based services
- The use of such applications leaves companies vulnerable to the loss of sensitive information

How Zyber addresses Shadow IT

What Gartner recommends	What Zyber delivers
Develop data security policies for access to approved services	Zyber addresses compliance issues by providing control and audit functionality within the enterprise's data centre. Zyber addresses data residency concerns and hands back control of confidential information to the enterprise, out of the cloud.
Use encryption to protect intellectual property or to address compliance and data residence issues	Zyber provides strong 256-bit encryption controlled by the enterprise to protect intellectual property and other confidential information in shared files within appliances at the location of the enterprise.
Implement enterprise level access controls	Zyber implements enterprise-determined access controls for all cloud and private cloud file-sharing services.

Zyber:
seamless data sharing
with uncompromised data security.

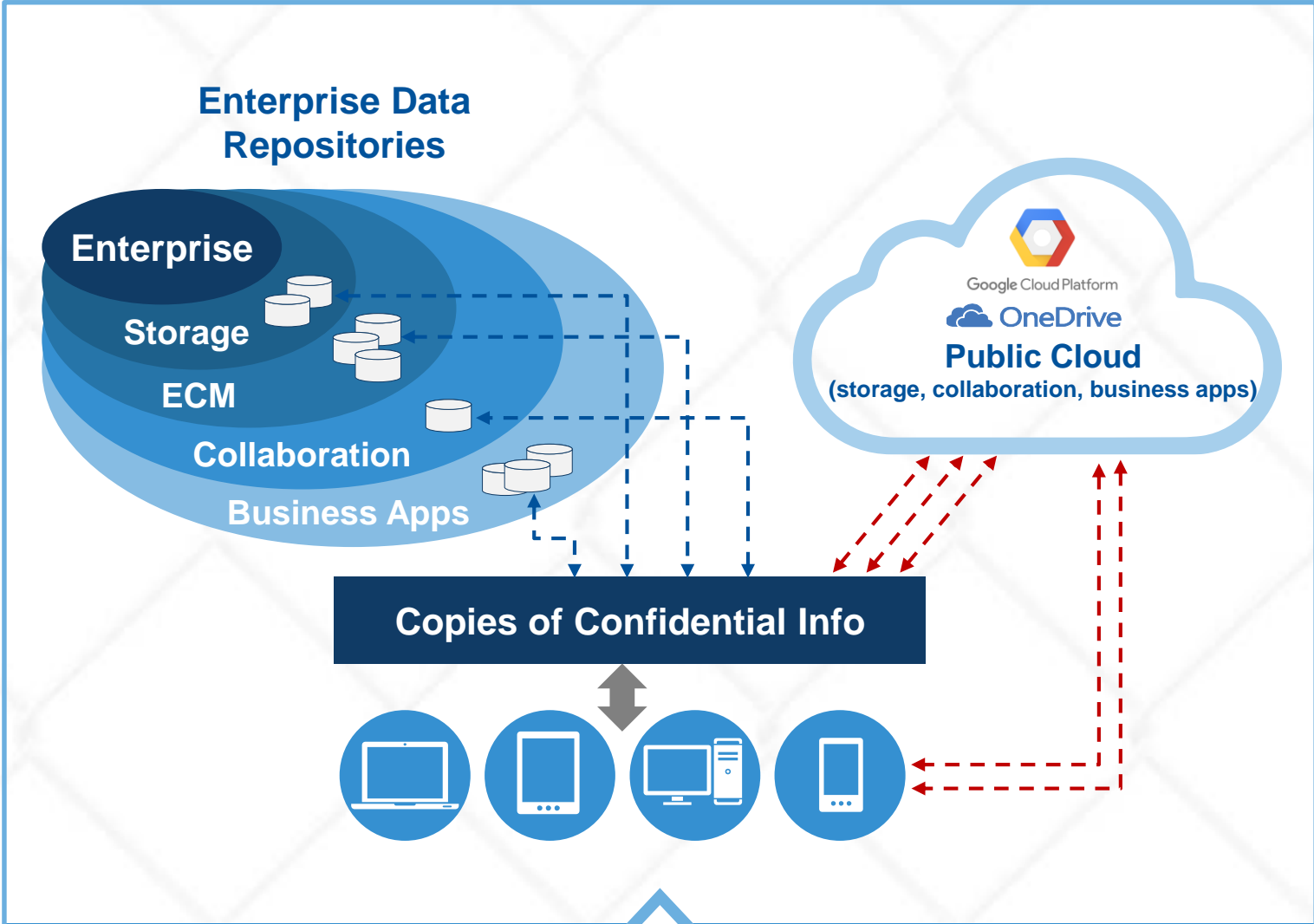
Zyber platform: any to any, securely.

- **On-premise** data translation and acquisition platform
- Communications service bus **normalizes** a full spectrum of data transactions to open standards
- Zyber is **technology-agnostic**. It links back-end IT systems across environments, homogenizing silos and establishing secure links to devices, third party apps and services
- Zyber-enabled enterprise can **securely** deploy and communicate with any edge device, web service or company based back-end information system
- **Horizontally** scalable, with multi-deployment model for enterprise and SMBs

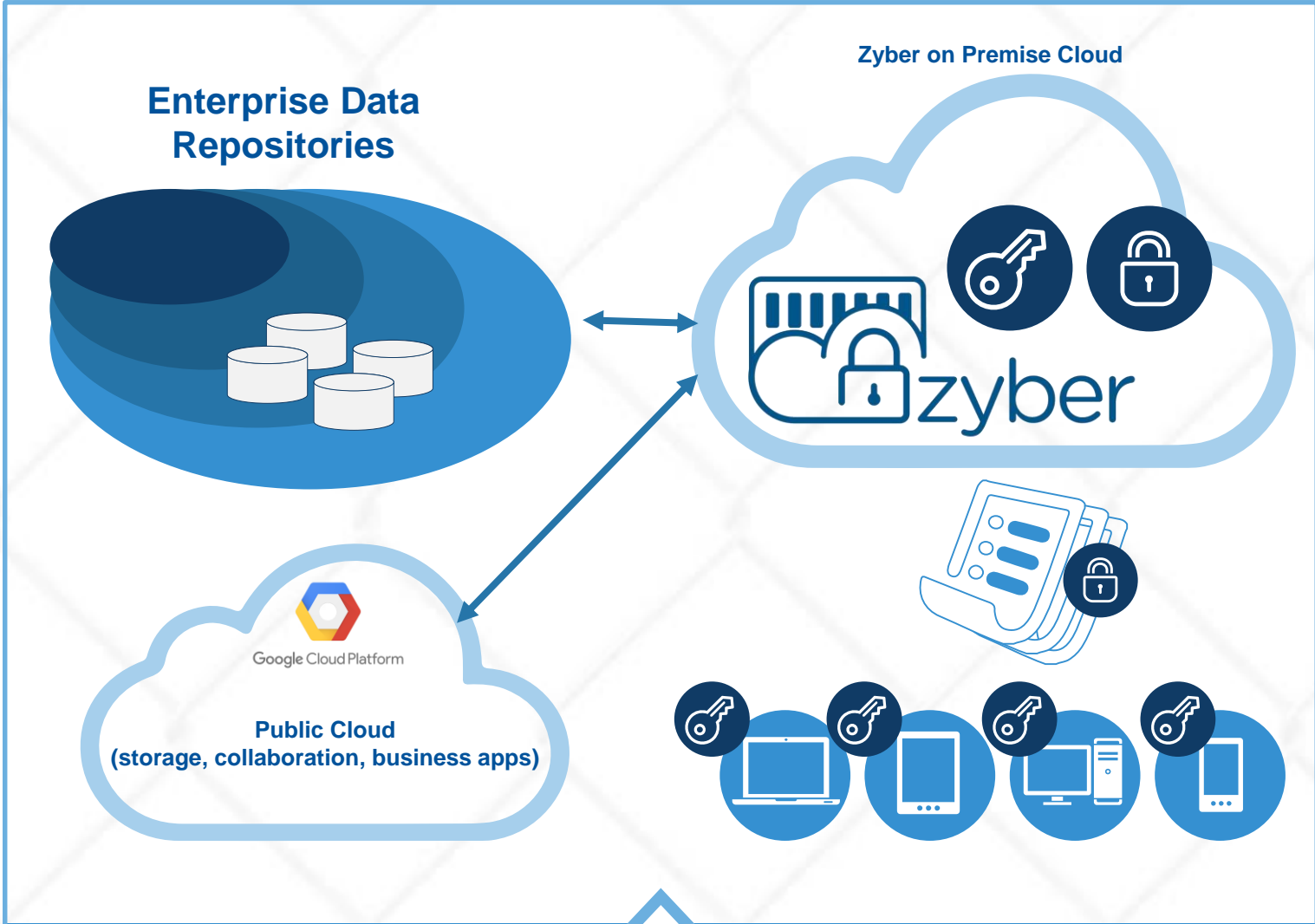
Zyber's value to customers

- Sensitive information is always under company control. Data and files are stored on premise, protected from mishandling, misplacing, or “going rogue”
- Virtual copies of files are available for access by end users via encrypted streaming
- End users can edit files and collaborate with others, but the working files and originals remain resident on premises
- Zyber data leaves no digital footprint: loss of mobile device doesn't mean loss of data
- Built from the ground up to seamlessly work with current enterprise IT systems
 - Current solutions focus on ‘plugging holes’ in existing data-sharing software
 - Vulnerabilities will always remain with existing software due to decentralized nature of data transfer and residency

Zyber won't let your data go rogue.



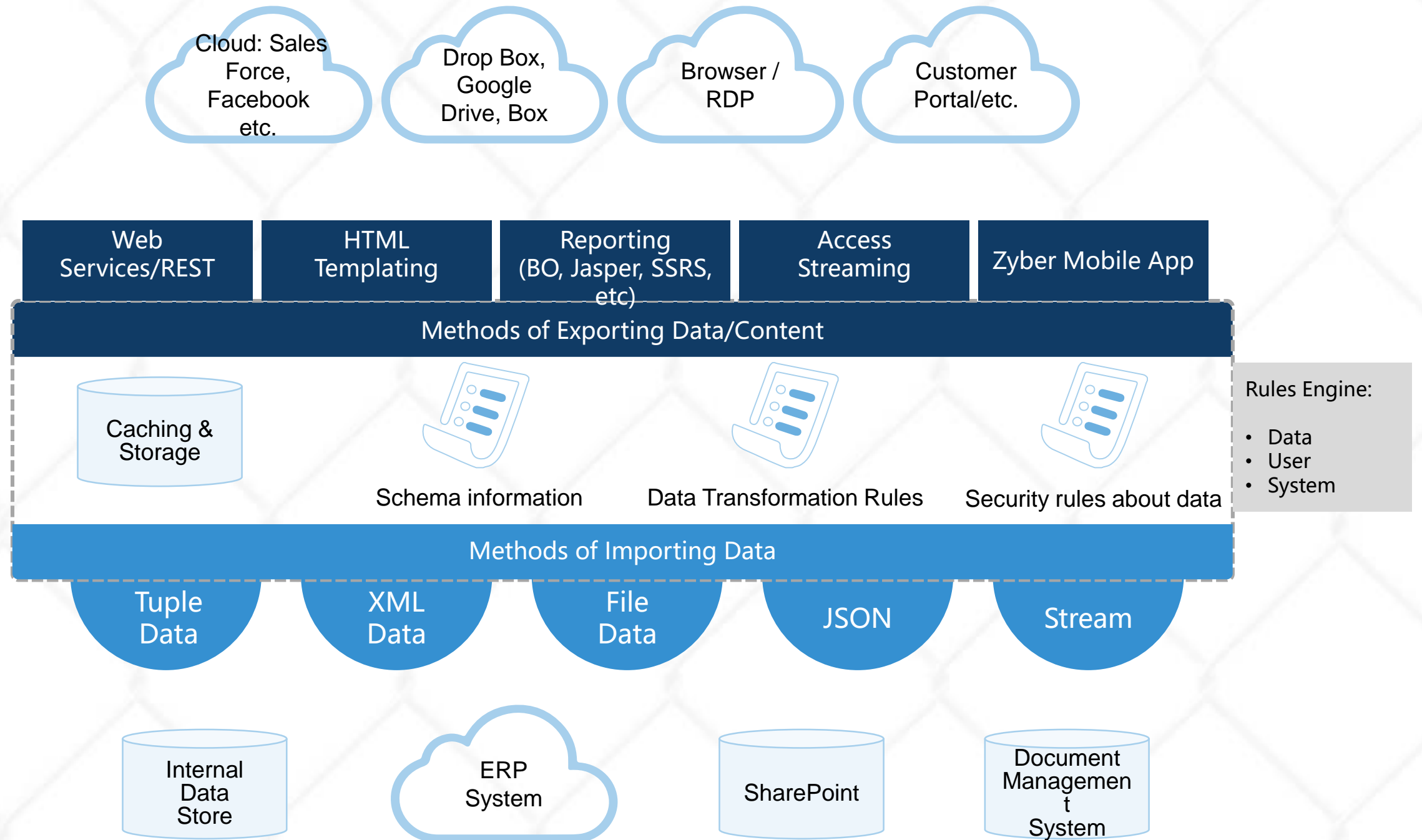
Without zyber
decentralised platform means
multiple vulnerabilities



With zyber
centralised platform for
better information control

How the platform works

- Protects data in motion by setting rules around security, access and data transformation.
- Uses 256-bit military/banking grade symmetric encryption
- Portal creates connectivity “heartbeat” and uses connection pointers to secure edge devices.



Zyber Benefits

- **IT can eliminate rogue file-sharing by managing user access, monitoring how company data is being disseminated, and taking action immediately if a security breach occurs.**
- **Compliance teams can easily audit to ensure sensitive information is only shared with those who need it, and rest assured that data is safely residing on local company servers.**
- **End users can easily share and access the latest version of their files anytime, anywhere, from any device.**

Summary

- Secure data/file-sharing solution for the management of an organisation's most confidential data
- Homogenises data silos across enterprise systems
- All files are stored on premise, using military- and banking-grade encryption
- Virtual copies are transmitted to users' devices only when needed
- Robust reporting for data monitoring and real-time compliance auditing
- Easy to deploy and manage user access
- Uncompromised file-sharing security with the ease and simplicity users expect



Sharing is good. Sharing securely is essential.

July 2016

Thank You

For further information contact:

Erik Tyler, Investor Relations

ir@zyber.com

www.zyber.com

