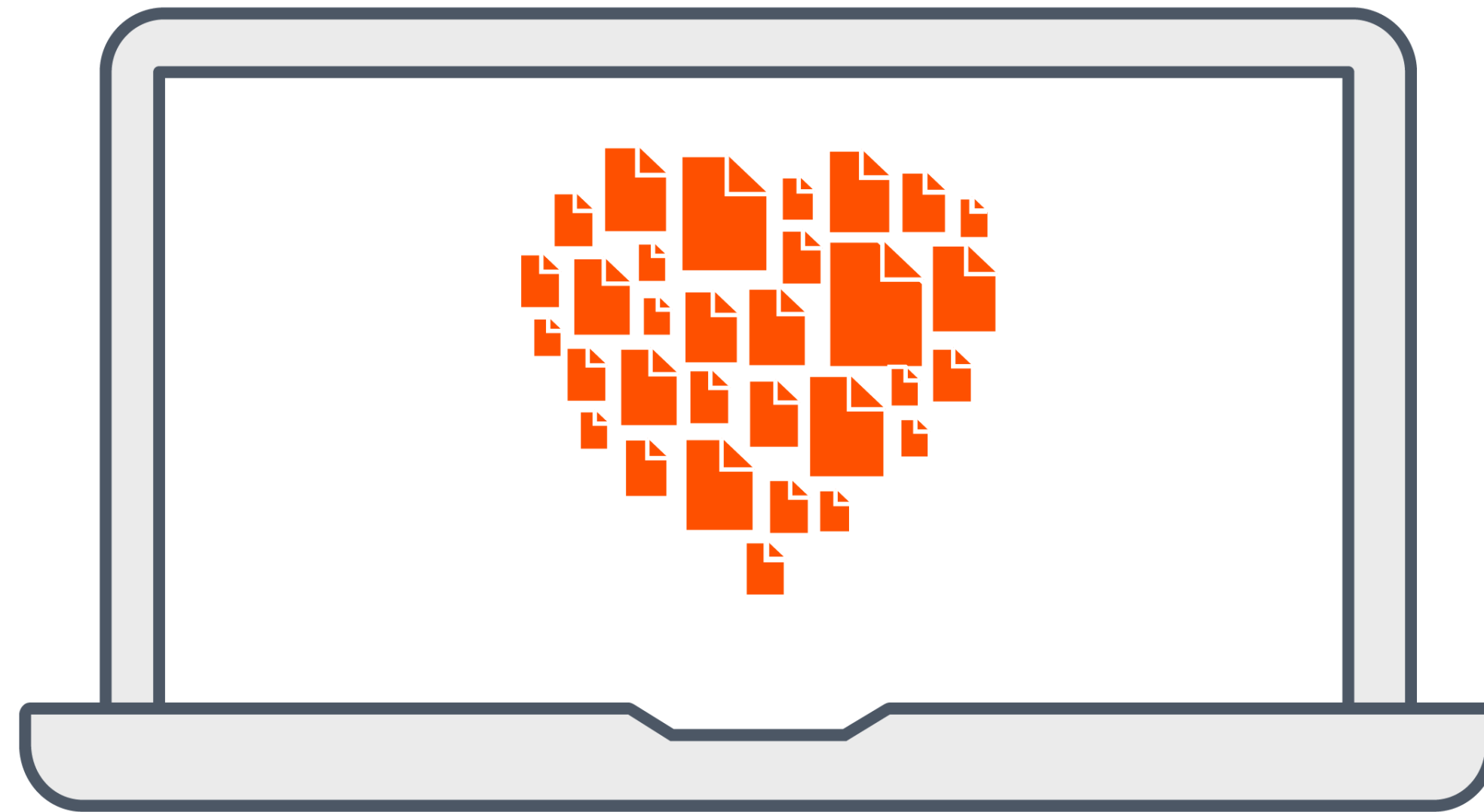


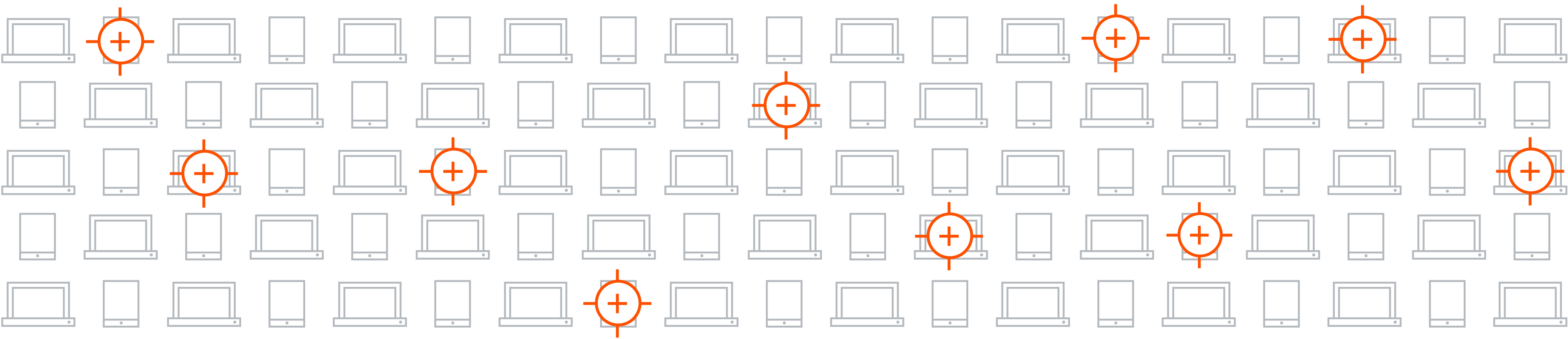


Code42 | CrashPlan

Compliance Simplified



Whether you're protecting the data of patients, cardholders, or everyday citizens, you expect it to be easy and cost effective to comply with ever-changing requirements.



Compliance regulations abound across industries and geographies. Our platform helps you comply with regulations governing where and how your data is stored, who can access it, and who can decrypt it.

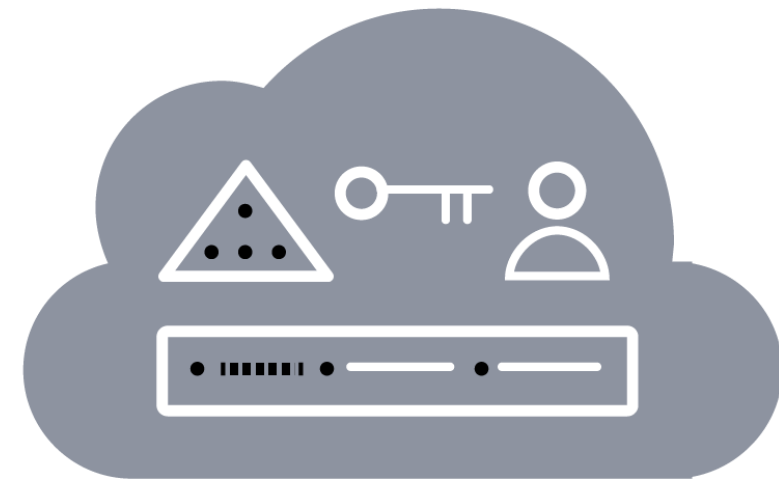
A photograph of three men in an office setting, overlaid with a semi-transparent orange filter. The man on the left, wearing glasses and a grey t-shirt, is pointing at a tablet held by the man in the middle. The man in the middle, wearing glasses and a grey blazer over a white shirt, is looking down at the tablet. The man on the right, wearing a plaid shirt, is also looking at the tablet. They are all focused on the device. In the background, other office workers are visible but blurred. On the desk in the foreground, there is a laptop, a small potted plant, and some papers.

All our deployment options provide

- Customer choice of where data and encryption keys are stored
- Centralized policy management
- Enterprise-wide administration with complete visibility of data and users
- Tamper-proof audit trails
- Compliance with data export laws
- Decryption strictly via authenticated customer credentials
- Permanent data destruction when an account is deactivated
- Single-click Compliance Settings to automatically restrict data access based on your regulations



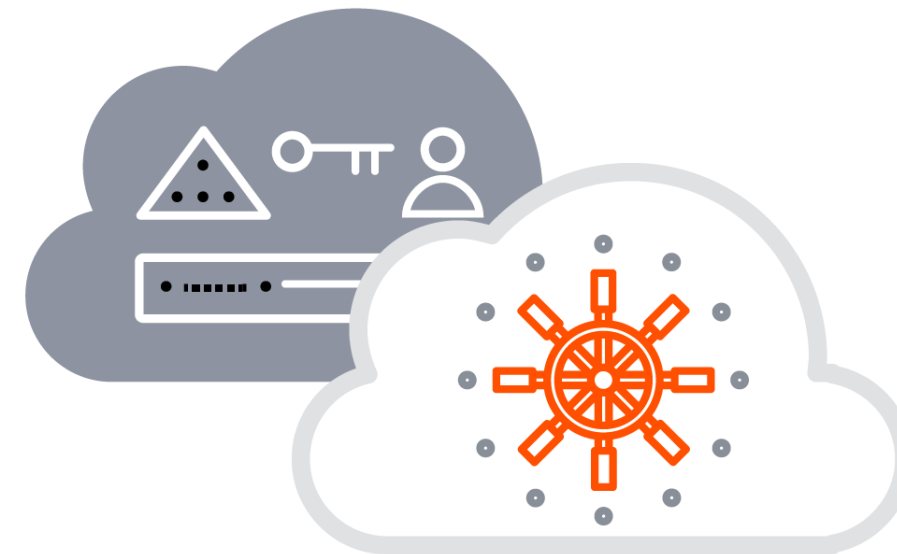
Choice in Where Data is Stored



Managed Private Cloud

100% on-premises

You keep the keys



Hybrid Cloud

Some data on-prem,
some in the Code42
cloud

You keep the keys



Code42 Cloud

Data stored in secure
Code42 cloud

You can keep the keys

Endpoint protection is a key component of most security and privacy regulations. Code42 helps customers meet their applicable compliance and risk management requirements, including:

GDPR <i>General Data Protection Regulation</i>	ISO/IEC 27001: <i>Information Security Management System</i>
SOC Reporting: <i>Service Organization Control Reporting</i>	NIST 800-53: <i>Security and Privacy Controls for Federal Information Systems and Organizations</i>
NIST 800-171: <i>Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations</i>	DFARS: <i>Defense Federal Acquisition Regulation Supplement</i>
HIPAA: <i>Health Insurance Portability and Accountability Act</i>	FISMA: <i>Federal Information Security Management Act</i>
ITAR: <i>International Traffic in Arms Regulation</i>	GLBA: <i>Gramm-Leach-Bliley Act</i>
FERPA: <i>Family Educational Rights and Privacy Act</i>	

