Differentiation through compliance — It's the new black!

It's hot. It's the latest trend. It's on point.

It's the positive correlation between implementing a cybersecurity compliance solution and a reduction in the number of cyberattacks.

That means: Put content protection in your organization to meet compliance regulations, and you have a better chance of preventing data leakage of your confidential and proprietary intellectual property, emails and documents. It's a strategy that sets you apart from the competition—and establishes you as conscientious and forward thinking. Meeting compliance regulations, reducing cyber threats and setting standards for the industry—three key performance indicators demonstrating why differentiation through compliance is the new black.

Data breaches and hacking are an unfortunate reality and a constant global threat in the digital age. No private-sector company, government agency or country is immune. Cybersecurity should be top of mind in every industry around the world—and it's quickly becoming so, with organizations implementing content protection solutions, U.S. federal and state legislation (16 states enacted cybersecurity laws in 2017 alone), and international regulations on the books. Here's a brief list of the cybersecurity laws we need to be fully versed on to ensure compliance for content protection.

- **Financial services**:

    - Federal Financial Institution Examination Council Handbook (FFIEC-IT) controls cybersecurity nationally
    - New York State Department of Financial Services (DFS) Cybersecurity Requirements is one of many laws regulating bank and insurance cybersecurity on a state level
    - Payment Card Industry Security Council's Data Security Standard (PCI DSS) protects payment cardholder personal information worldwide
- **Consumer data:**
    - Protected in 47 states and the District of Columbia through compliance laws requiring notification to states of breaches compromising PII including Social Security numbers and payment-card data
    - Federal Trade Commission (FTC) has the authority to penalize organizations that provide inadequate data protection
- Health Insurance Portability and Accountability Act (HIPAA) federal **healthcare** law protects confidential patient history, PHI.
- U.S. Department of Defense (DoD) requires **federal government contractors** to meet cyber requirements in accordance with the Defense Federal Acquisition Regulation Supplement (DFARS) and Procedures, Guidance, and Information (PGI) law to protect corporate information systems according to the security requirements published in NIST SP 800-171, "Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations." The DFARS regulation requires all DoD contractors to be fully compliant by December 31, 2017.
- General Data Protection Regulation (GDPR) provides guidelines governing the collection and processing of **EU personally identifiable information**. All EU- and foreign-based organizations that process the data of EU citizens must comply by May 25, 2018.

Complying to these regulations is pivotal to secure digital operations. But there are also the hundreds of emails and documents your organization processes daily, which fall out of the scope of these specific laws but still require the same high level of protection—like HR documents, legal contracts, project specs.

This means: In addition to complying to government cybersecurity regulations, it's vital that you create rules in your organization to protect content inside and outside the firewall—managed by corporate governance policies—with a solution that provides access rights and implements persistent content protection for your confidential information. In other words, all cyber content must be protected.

Is it possible to comply with all these cybersecurity regulations? Yes! It! Is!

Let's flip things around and look at it from the perspective of what we can do on the front end so that adhering to mandated cybersecurity compliance regulations easily falls into place.

It's all possible with GigaCloud™, the SaaS service from GigaTrust™. GigaCloud delivers persistently protected emails and documents for collaboration anytime, anywhere, on virtually any device. It is the first and only secure email and document protection, consumption, and collaboration service that is an easy-to-use, easy-to-deploy private or multi-tenant cloud service powered by the Microsoft – Active Directory Rights Management Services (AD RMS) security ecosystem.

GigaCloud delivers security for HIPAA compliance. It can protect the safety of the over 500 million EU citizens—a requirement as of May 2018. GigaCloud for DoD Supply Chain addresses over 25 of the NIST SP 800-171 security requirements—a necessity by the end of 2017.

Cybersecurity compliance is a given. The best solution is a choice. Are you ready for the new black?