If future matters more than the past, because we can influence it, why do we have far more historians than futurists?

The Age of EM, 2016 Robin Hanson

Ready for the next round of cyber security and privacy protection tasks on HPE NonStop?

Executive summary

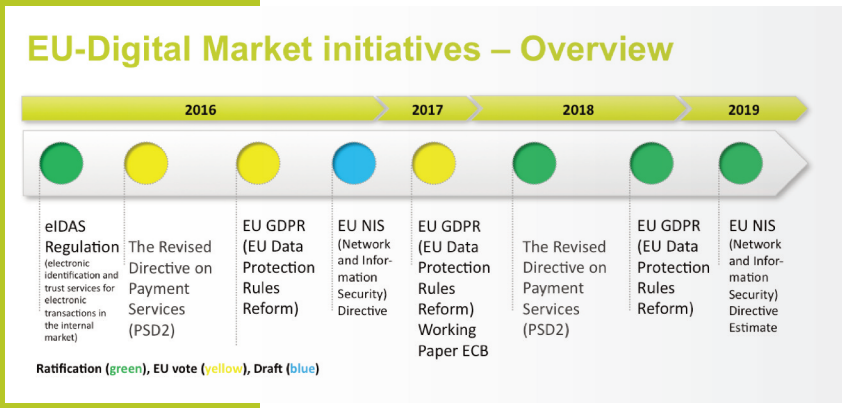
With new worldwide and regional regulations (e.g., EU GDPR – General Data Protection Regulation), there is a need for a new cyber security and data privacy architecture. The current hardware, user interfaces, applications, etc., were often designed without privacy in mind. Developers don't have the time or resources to redevelop existing tools; however, poor security and privacy propagates into new applications. This white paper describes how to cope with these challenges, how to design a future-oriented cyber security and data privacy architecture on HPE NonStop and integrate it into a corporate IT infrastructure.

Introduction

The pressure of the regulatory bodies on service providers, data processors and data controllers is getting tougher every day. Now, GDPR penalties for data breaches will be executed with a fine of up to 4 percent of the organization's global annual revenue.

Now is obviously the right time to take a step back as a customer and ask the following questions:

- For what problems can security professionals help provide solutions?
- Is an autofill-generator template for ISO 27001 compliance the level of security I want?
- Psychologist Abraham Maslow famously stated, "I suppose it is tempting, if the only tool you have is a hammer, to treat every thing as if it were a nail." Are we treating every security topic as if it is a nail?



The current landscape of cyber security threats (e.g., DDoS, penetration attacks, applications misuse/abuse) and data privacy requests – data subject requirements, data controller, relevant legislation, etc., along with Logging/Auditing processes based on Government, Risk and Compliance (GRC) requirements – can be protected only by a multifaceted and multilayer approach. Following our address of the problem is an overview of comforte solutions.

Problem definition

Egress Software Technologies research found that 87 percent of CIOs believe they would be exposed if the regulations came into force today, while Netskope-commissioned YouGov research found 80 percent of IT professionals in medium and large businesses are not confident of ensuring GDPR compliance by April 2018.

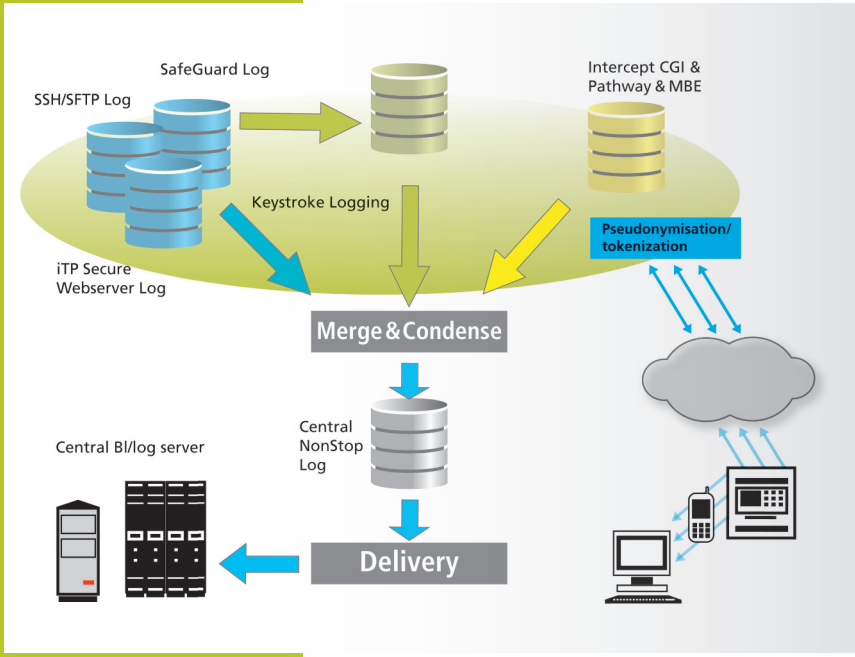
GDPR is not the only initiative with implications on the overall GRC strategy. Following are some details of other regulations to be included in such a strategy:

High level Solution Description

comforte cyber security and data privacy solution framework has the following four pillars:

1. Enhancing the status quo operations – collect, consolidate and merge existing logging mechanisms like application, Safeguard and iTP Secure WebServer without application modifications.
2. Extending cyber security architecture with system-alerting functionality, including in-depth NonStop Safeguard coverage, keystroke logging for all NonStop subsystems (e.g., TACL, OSS, Pathway, etc.) and an SSO (Single Sign-On) architecture compliant with the rest of the IT infrastructure of the respective customer.
3. Enabling a generic intercept architecture (e.g., all CGI and Pathway server-based application subsystems) to support a smart cyber security and monetization architecture.
4. Pseudonymization/tokenization based on several regulations (e.g., upcoming EU GDPR, PCI-DSS, etc.) is an integral part of comforte's cyber security architecture.

Most importantly, all parts should be connected to a central SIEM system (security information and event management) to permit a company-wide coordinated GRC operation.



Business benefits

comforte's cyber security and privacy approach provides customers the following key benefits:

- A clear strategy for and implementation of cyber security and privacy in their businesses, help understanding cyber security's role in business decision-making, identifying and solving modern business security issues and how comforte business solutions fit.
- Ability to capitalize on current global and regional regulation principles, including a comforte cyber security and privacy briefing about standards and design guidance for NonStop environments.
- Maximum use of security requirements to solve business issues with either proprietary or comforte-prepared case studies and recommendations on how cyber security and privacy solutions can be applied, plus discussion and/or implementation of monetization as a security add-on.

Case studies (overview)

Customer A wants to protect PAN (primary account number) data to ensure compliance with PCI DSS (Payment Card Industry Data Security Standard) and upcoming PSD2 (Payment Services Directive).

- comforte's SecurData is a great fit, with deep integration available for applications like Base24 (a global electronic retail payment switch used by banks, retailers, and processors).

Customer B wants to protect mobile phone numbers, SSN, etc., to be compliant with EU GDPR.

- SecurAudit focuses on specific telco requirements (e.g., intercept of in-memory databases, etc.).

Customer C wants to control and audit access to applications and data both from a security and monetization standpoint.

- SecurData/Audit to allow application-independent logging and subsequent work in Business Intelligence for intrinsic and extrinsic purposes.
- SecurSSO to merge NonStop users with corporate Single Sign On.

Summary

Security and data privacy regulations like GDPR and PSD2 introduce a huge number of data-governance obligations (i.e., use of personal data must be scrutinized and justified.)
The implementation strategy of appropriate technical and organizational measures must ensure a level of security commensurate with the risk. Timing is critical, as the latest April 2018 key privacy standards have serious commercial implications, including penalties for noncompliance.
As the front-runner in the NonStop encryption and tokenization arena, comforte offers deeply integrated solutions to protect sensitive and personal data, while providing low-risk, rapid for customers in the cyber security and data privacy space that are based on the references of and experiences with leading worldwide operating service providers.

comforte offers different security workshops to meet your requirements:
https://comforte.com/fileadmin/Media/comforte_KT_workshops_1_2016.pdf

Please contact us: www.comforte.com/contact or call 0049 611 931 99-00