SYNCDOG

WHITEPAPER

GDPR will bring the Teeth that have been Missing in Data Security Auditing and Compliance

Data security standards have been around for decades yet standards enforcement has been lacking. This paper explains why GDPR will change the playing field next year, what GDPR means for endpoint data management, and offer 5 tips to help maintain compliance.

The summer of 2016 was a remarkable one in the Information Security compliance world. In July, Advocate Health Care Network agreed to the largest HIPAA fine ever recorded, $5.5 million, surpassing a 2014 ruling against Presbyterian Hospital and Columbia University (New York City) at $4.8 million.

On the surface, the fine looks imposing enough but as a percent of revenue for the 2016 year, the Advocate penalty constitutes only about one-tenth of one percent.[1] Since 2012, HIPAA fines have steadily increased to last year's record-setter but in the grand scheme of things, punitive damages for enterprise healthcare violations of the standard continue to be just a slap on the wrist.

In industries where credit-card processing takes place (under PCI DSS compliance watch), fines can be as much as $200,000 per merchant violation.[2] However, the compliance enforcement for retail and other industry verticals burdened by credit card transactions lacks teeth.

When credit cards first started transacting on the World Wide Web, credit card theft was high. Rather than wait for the U.S. Government to act and create a standard,

1 *http://www.advocatehealth.com/documents/financialinformation/Advocate_AFS_12-31-2016.pdf*

2 *http://blog.securitymetrics.com/2015/02/visa-pci-enforcement-rules.html*

the payment card industry (PCI) founding companies, comprised of AMEX, Discover, MasterCard, Visa and JCB International, took matters in their own hands and formed the PCI Security Standards Council and shortly thereafter, the PCI Data Security Standard or PCI DSS. PCI DSS applies to every business – regardless of size – that processes a credit card; even if you conduct only a single credit card transaction this year, your business falls under the watchful eye of PCI DSS.

The problem with PCI DSS enforcement is that it's not "owned" by a government entity, nor is it law. It is a checklist of best-practices for handling credit card data and accompanying personal information. PCI DSS is not law but the standard does have teeth. The PCI Council could, in the event of a non-payment of fine, suspend a merchant's privilege to use their gateway to process credit card transactions, effectively constricting the merchant's revenue generating capabilities.

> Data security standards have been around for decades yet standards enforcement has been lacking.

GDPR Coverage Spans both Time and Space

The European Union (EU) data protection framework GDPR (General Data Protection Regulation) becomes official on May 28th, 2018, and the most notable aspect of the standard is its designation as "regulation," a replacement of the current Directive 95/46/EC.

The EU GDPR online portal states that the regulation was enacted to "harmonize data privacy laws across Europe and empower all EU citizens' data privacy" and "reshape the way organizations across the (EU) region approach data privacy." There are even provisions in the regulation that offer specific protection to children, declaring that children are "vulnerable individuals" deserving "specific protection."

No matter your geo-location, if someone in your organization accesses identifiable data of a "subject" who lives within the EU, as of May 25, 2018, your organization must comply with the GDPR. The regulation applies when the processing of the subject's data is "related to the offering of goods or services, irrespective of whether a payment of the data subject is required." Some exclusions apply,[3] but the scope of coverage in the regulation is as disruptive a compliance standard as we have ever seen. GDPR affects every corner of the globe that looks at, touches, or moves data to/from the EU

Points of Distinction for GDPR Compliance

Data File Types: It took the EU Parliament four years of preparation (and debate) to approve GDPR on April 14, 2016. GDPR applies to any organization that "offers goods or services to, or monitor the behavior of EU data subjects," regardless of the company's location.[4] The regulation centers around a "data subject" and the manner in which an organization handles any file type that can be used to directly or indirectly identify the subject – name, photo, email address, bank details, social media post, medical information, or computer IP address. All of these file types could constitute identity under GDPR.

3 *http://www.privacy-regulation.eu/en/2.htm*
4 *http://www.eugdpr.org/*

Appointing a DPO: The EU Parliament believes that GDPR is not regulation to be taken lightly and depending on your organization type, you may be required to appoint a Data Protection Officer or DPO. GDPR provides that you must appoint a DPO if your organization falls into one of the following categories: "(a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data (Art. 37)."

"Large scale" is loosely defined in GDPR.

Processing Child Data: Parental consent is required to process personal data of children under the age of 16. Member states have the option to reduce this age limit but not below 13 of age. If member states change the age minimum, it will just add another layer of complexity to what you need to watch for geographically and by data file type.

Data Breach Reporting: GDPR Article 33 states that in the case of breach "the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55…" Other than the obviousness of 72-hour time frame, it should be noted that GDPR recognizes two functions within your organization that need breach visibility – the "controller" and the "processor." The Controller generally determines purpose, conditions and means of data processing, while Processor is naturally the computation entity acting on behalf of the Controller.

Processing Activity for Goods or Services: GDPR stipulates that the regulation applies to all firms that offer goods and/or services to EU residents whether or not a payment is transacted. If you market your goods/services to any EU data subject, GDPR applies to both customers and prospects in your contacts list. GDPR identifies data subject as "an identifiable natural person" to any of the factors listed above in Data File Types.

Right to be Forgotten: Citizens under the protection of GDPR have the "right to obtain from the controller the erasure of personal data concerning him/her without undue delay and the controller shall have the obligation to erase personal data without undue delay…" There are

stipulations (and exemptions) here[5] too numerous to detail; the point to be made is you must have a method for data subjects to request erasure and the request needs to be vetted then acted upon, which may require both your auditing and legal teams to be in sync.

The Impact to Bottom Line: Non-compliance to GDPR regulation can result in fines up to four percent of global annual revenue, with a cap set at €20 million ($22.4 million USD at this writing). Penalties accrue on a scaling model where four percent is the max penalty. The lower-level fine is set at the two-percent-of-revenue (previous year) mark or €10 million, whichever is higher. Fines will be administered by individual member states. A list of criteria for fines determination can be found on the GDPR EU site here - http://gdpreu.org/compliance/fines-and-penalties/.

5 Steps to Help Maintain Compliance Leading up to May 25, 2018

The official text from the EU Parliament's April 2016 legislation (a repeal of Directive 94/46/EU) comes in at 88 pages. There are a lot of moving parts to this regulation and the penalty schedule is enough to cause financial hardship to even the largest global organizations. It is going to take a concerted effort from your organization's personnel, armed with real-time intelligence that gives them the visibility to immediately report a breach, and you need to do this all with transparency. "With transparency" means organizations will need to provide extensive information to individuals about the processing of their personal data. There will be a lot of complex interactions across your organization to maintain GDPR compliance, and when it comes to data security, you're only going to be as strong as your weakest link at the far reaches of your IT security perimeter. These 5 tips will help you comply with the regulation.

1. Reinforce your endpoint security.

Your organization is going to need sufficient end-point management that fortifies the security of your Enterprise Mobility Management (EMM) and Mobile Device Management (MDM) systems.

Your mobile workforce occupying the far reaches of your perimeter, outside the walls of your organization, and into the countries you do business in, will constitute the most vulnerable threat vectors to the data protected by GDPR. As stated earlier, GDPR is not confined to the EU, it is global data security regulation. Your enterprise's EMM is a separate infrastructure with its own operating system. Spread throughout the confines of this expansive and complex IT ecosystem, your mobile teams are managing app delivery, access control, asset management, provisioning, and hopefully doing this across a secure infrastructure.

EMM systems were never originally designed as security and anti-virus systems so fundamentally, they cannot operate as efficiently as these systems designed to watch, track then alert (sometimes with automated

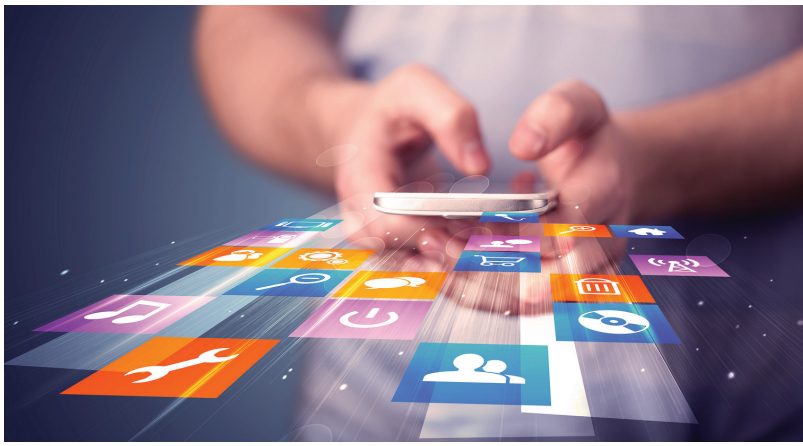
5 http://www.privacy-regulation.eu/en/17.htm

remediation) on cyber threats as they are happening in real time. One highly effective method of additional security at the device level is mobile containerization. A containerized application workspace provides a secure data platform that encrypts and transports data between your enterprise's back-end and a secure, "sandboxed" application container on your employee's mobile devices.

SyncDog, an independent software vendor headquartered in Reston, Virginia, U.S.A., provides Secure.Systems™ that protects an enterprise network by securing data on the device and data in transit using FIPS 140-2, AES 256-bit encryption. Secure.Systems™ is a software-based, secure mobile application framework, and is designed to be an extension of an enterprise's existing security and EMM infrastructure. More information on Secure.Systems™ can be found at secure.systems

2. Security Information and Event Management

To keep tabs on your data and who's accessing (or even looking at) your data, you need a 360-degree view of all user activity surrounding your data. At the heart of this security information and event management or SIEM practice is log management in conjunction with event correlation. Collecting event logs from endpoint devices, firewalls, routers/switches, desktops, servers, and applications (log management) and then correlating them against norms of user behavior (events) are the basics of SIEM. It is much more complicated than this, but the idea is to understand the norms of user interactions with your network data – for instance, 99 percent of the time Bill logs in between 8:00 a.m. and 8:30 a.m. from his normal IP address in Boston, and logs off before 6:00 p.m. Correlating this normal behavior to say five logins at 2:00 a.m. from an IP address in Saudi Arabia, when you know Bill is in Boston, is an anomaly and should be investigated immediately with appropriate action taken. A SIEM will collect events and correlate them, then notify your security team in a number of ways that something needs to be investigated.



3. MDM & SIEM Integration to your IT SOC

All this event logging and event correlation must be rolled up into a single view of data security truth within your IT Security Operations Center. Securing your data means visualizing and understanding the user interactions to your data in real time. Theoretically, we will never be able to build a hack-proof data store because humans are mistake-prone. The latest Verizon Data Breach Investigations Report[6] reveals that

> EMM systems were never originally designed as security and anti-virus systems...

6 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

81 percent of hacking-related breaches leveraged stolen and/or weak passwords. Security industry pundits agree that breach is inevitable and the focus should be on real-time threat visibility with instantaneous notifications of a breach, followed immediately by corrective action to stem the bleeding. And what makes this all possible is a security policy based on 100 percent visibility in your SOC of the activity across all the threat vectors in your network.

Where GDPR is concerned, this visibility will give the Controller a path to validate the technical and organizational measures they are undertaking to maintain compliance and in the event of a breach, an audit trail of forensics with which to determine the who, what, when and where of the breach.

4. **Your Security Policy should not Clash with your Mobile Application Functionality**

GSMA, the global association that represents the interests of mobile operators – Verizon, AT&T, and Sprint to name a few – estimates that by the year 2020, 1.3 billion individuals will access the Internet through mobile devices.[7] Today, business workflows have been re-engineered to such an extent that being out of the office is not an exemption from being able to complete a task. It is the norm of everyday business activity. There is now a mobile application for everything and whatever gap that once existed from an app not being available from a third party mobile developer, is now a custom-developed app in-house.

7 *http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/*

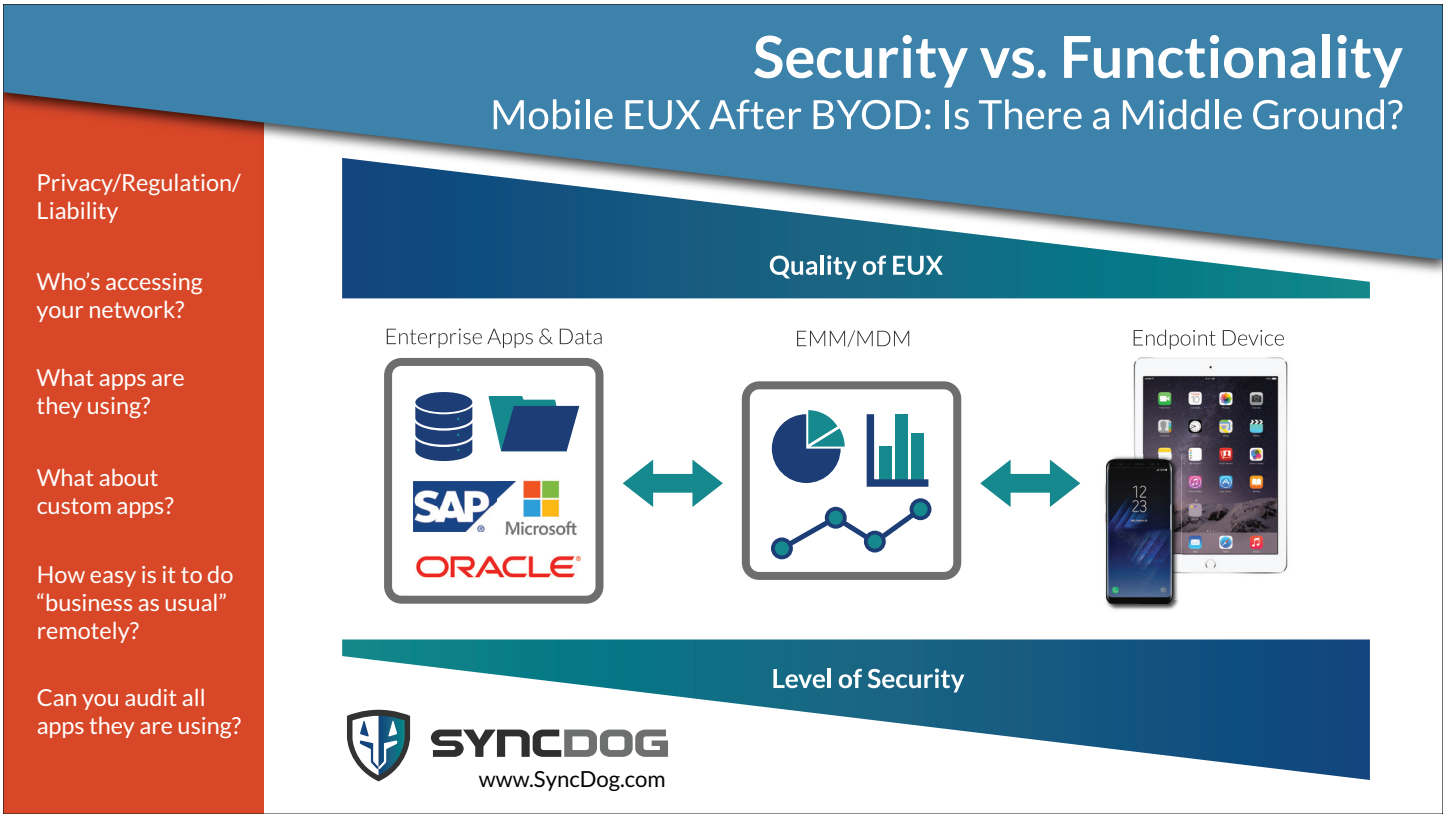


FIGURE 1. The quality of EUX diminishes as the level of security increases.

The problem with this everyone-can-develop-an-app mentality is security. App developers typically don't have the expertise as that of security architects, and security architects aren't generally application developers. More times than not, the end result is that the application end-user experience suffers as the level of security is increased (see Figure 1). This diminished functionality at the device level could serve as inhibitor to workflows and in-turn, productivity farther away from the datacenter.

App developers typically don't have the expertise as that of security architects, and security architects aren't generally application developers...

For example, Marketing VP Bill is traveling and needs to approve an ad in the organization's project management system that is due tomorrow. However, the ad is missing a sentence and Bill needs to annotate the document on his phone but the security policy in the datacenter trumps his phone policy and he can't even access the document. The ad will have to be late in this scenario as the workflow will have stopped until Bill can be back in the office or he can access on his laptop via VPN connection. The farther away from the network perimeter, the more diminished Bill's mobile app functioned.

Using an app development platform like Kony or Xamarin is a viable quick-to-market option for app development, but these solutions are designed to provide non-development resources the tools needed to leverage their existing (non-developer) skills to build mobile apps. In a similar scenario where an app developer may not have security expertise, these platforms are not security tools.

A containerized solution scenario such as described above with SyncDog's Secure.Systems™ remedies this situation as the device's corporate apps are segmented in an AES 256-bit protected workspace that is FIPS 140-2 certified. The containerized workspace operates as a highly-functioning extension of your in-house workflows.

5. Alerting system that's integrated into Service Desk

Automation is everything when answering the call for Infrastructure and Application Service Delivery. Every CIO has a service level percentage to maintain and his/her failure to comply can compromise organizational productivity and in-turn, profitability. All systems must be "go" all the time when it comes to performance and availability of manufacturing, HR, communications, and other vital systems that keep an organization's people up and running.

The Service Desk or Helpdesk has been instrumental in bringing visibility to Infrastructure and Application service delivery levels. The second an asset that an application is dependent upon goes off-line, an automated helpdesk ticket can be logged into a Service Desk system and immediate remediation can be undertaken. The app can be transferred to a redundant server or other automated response can be taken to ensure service outage is minimized.

Given the 72-hour time requirement for GDPR breach reporting, we need to bring this Service Desk notification process into the realm of your IT security and compliance. Your MDM and SIEM flow that is populating the IT SOC with real-time data, needs to have the capability to at least issue a trigger to a notification system that a ticket needs to be issued to investigate the threat. In addition to a help-desk trigger, an automated email or SMS text should also be generated to security admins to shut down ports or other immediate action, either manual or automated.

What's Next?

In the technology world, the word "disruptive" is thrown out all too often to describe a lot of concepts said to alter the way we conduct business-as-usual. Some of this labeling is accurate, but it is often an overused term to add hype to a new product or service. GDPR will absolutely be a disruptive piece of regulation that your organization – whether based in the EU or not – is going to have to navigate through.

If your organization is US-based and you only make a single phone call next year to an EU-based prospect, and your notes about the conversation go into your CRM system, you could be subject to the constraints of the regulation. This regulation affects the entire planet, regardless of where the data processing takes place.

Many of you with a best-practice approach to IT security and compliance won't need to change your approach that much at all. For those of you in this group, just stay the course.

For those of you still struggling with enterprise-wide visibility to user activity, privileged or otherwise, this whitepaper is designed as an educational tool with some best-practice guidelines for helping your organization manage GDPR compliance. SyncDog can be a trusted resource for providing a viable and fully-functioning app workspace for your mobile workforce that's NIST-certified secure. For more information please visit www.SyncDog.com.

SYNCDOG

11950 Democracy Drive, Suite 275
Reston, VA USA 20190
Call: (703) 430-6040 • Fax: (703) 997-8667
sales@syncdog.com • www.syncdog.com