verimatrix™

EU Cyber Resilience Act

Security First: The European Union's Cyber Resilience Act and Its Pending Impact on the Mobile App Development Ecosystem

Table of Contents

1 Security Risks in the Everything-connected World

Connected devices are proliferating, as is our dependence on them. Mobile and Internet of Things (IoT) devices are integral to everything from consumer goods like smartphones, televisions and tablets to agricultural equipment, industrial control systems, aircraft and much, much more. Per Cisco's 2022 Annual Internet Report, there will be 3.6 global devices and connections per capita by the end of 2023. Market research firm IoT Analytics predicts there will be roughly 27 billion connected IoT devices by 2025.

Connected devices can create blind spots

Many of those devices run some software application to make them useful. Any mobile app connected to the internet or a cloud service can unfortunately be weaponized. For instance, hackers may download apps from any app store and install a Trojan Horse—converting a legitimate app into malware, which becomes dangerous when re-marketed to unsuspecting users. Enterprises also face considerable risk from unmanaged and uncontrolled devices on which their apps are installed. Across enterprises, that can mean millions of endpoints connecting to back-end systems, posing new threats.

Applications can also face security risks from flaws in their design or coding. For instance, the zero day vulnerability in the Log4j 2 logging library framework, found in late 2021, quickly became a global problem because Log4j open source code is freely distributed by the Apache Software Foundation and used in countless numbers of apps.

Application Programming Interfaces (APIs), widely used to enable different software components to communicate with each other, can present a backdoor way for hackers to access a networked environment. And, the growing practice of incorporating reusable, pre-packaged run-time components known as containers to accelerate application development cycles also presents a unique vulnerability if containers are not properly secured or become corrupted.

These and other vulnerabilities that can exist in connected applications and devices put enterprises – and their users – at risk.

The fastest growing digital attack surface is mobile. New attack vectors are evolving from the weakest links – connected apps, APIs and unmanaged devices.

According to Verizon's 2022 Mobile Security Index:

45%

of organizations had recently experienced **mobile-related compromise,** almost twice as many as in Verizon's 2021 survey.

74%

of organizations that experienced mobile-related compromise described their compromise as **"major".**

Market research leader Gartner found that

75%

of all mobile apps & devices are **unprotected.**

2 Cybersecurity vs. Cyber Resilience

Countering cyber threats has spawned a breadth of solutions and an entire industry focused on addressing different pieces of the puzzle.

The principle of **cybersecurity** is now well known and practiced, although to a different extent, by a majority of organizations. Cybersecurity involves taking a structured approach to protecting organizational assets against cyber threats and mitigating associated risks. That is done through applying a range of technologies, services and practices, targeted to securing a specific networked environment—from an individual's mobile device to a large enterprise's cloud-based infrastructure.

The list of cybersecurity solution types is long: firewalls, anti-virus, intrusion detection, extended protection and response, application security, virtual private networks, and much more. Each has a different role to play in an organization's overall security infrastructure.

Despite this breadth of available resources, no security measures are completely fail-safe, as evidenced by the ongoing number of successful cyberattacks. Knowing it's 'when' not 'if' attacks will occur, the concept of building **cyber resilience** is being increasingly popularized.

Cyber resilience involves putting measures in place to minimize and recover from a cyber incident as quickly as possible. While cyber incidents are often externally-driven (such as direct attacks), they can also be the result of human error or malicious acts on the inside. So going a step beyond cybersecurity, preparing to be cyber resilient requires proactively examining all areas of technology-centered risk, and how best to fortify them while preparing measures to respond to disruption when it occurs.

One major global governing body is about to take cyber resilience to an unprecedented level.

Cybersecurity vs. Cyber Resilience

Focus of Cybersecurity	Focus of Cyber Resilience
Networked IT Infrastructure (including on-premise and cloud assets)	IT
	People
	Insurance / Financial
Mobile / IoT devices	Operations
	Business Continuity
Connected applications	Legal

3 Europe's Leading Approach to Cyber and Privacy Protection

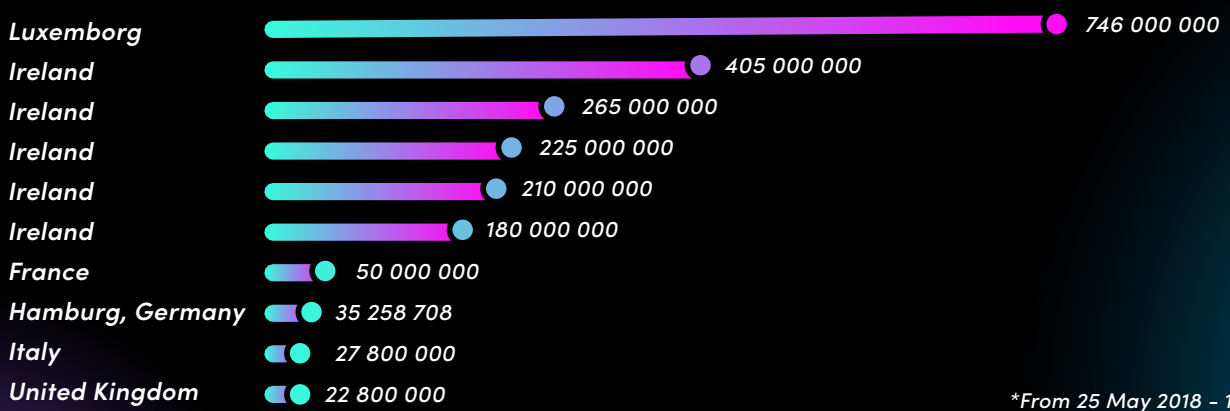
The European Union (EU) has led the world in regulations to improve cybersecurity and data privacy. The European Commission (the EU's executive body) does so in the interest of advancing digital sovereignty for its citizens and business enterprises. The European Parliament has expressed strong concerns about the economic and social influence of non-EU technology companies threatening EU citizens' control over their personal data, constraining growth of EU technology companies, and limiting European rule-makers' ability to enforce their own laws.

Since the 1990s, the European Commission has enacted multiple regulations to strengthen Europe's ability to act independently in the digital environment and increase its defenses against digital threats. Any enterprise doing business in the EU (or in some cases simply with EU citizens) needs to comply with Europe's strict regulatory environment or risk significant penalties.

Some of the most important regulations include:

- The General Data Protection Regulation (GDPR), described as the toughest privacy and security law in the world. Enacted in May 2018, it applies to any organization that targets or collects data about EU citizens, and establishes specific protections for processing of that data. The law was in large part a response to the growing numbers of people providing their personal data to cloud service providers.
- The EU Cybersecurity Act, providing an EU-wide cybersecurity certification framework for information and communication technology (ICT) products, services and processes, rather than leaving a swath of differing regulations across member countries. The Act also grants a permanent mandate and increased resources for the watchdog European Union Agency for Cybersecurity (ENISA).
- The Network and Information Security (NIS) Directive 2, replacing the original NIS, the first EU-wide cybersecurity legislation. Slated for enforcement by 2024, NIS2 will improve cybersecurity risk management practices across the EU, and expand its scope to more sectors like energy, transportation, health, and other critical infrastructure.

Top ten largest fines imposed to date under GDPR



*From 25 May 2018 - 10 January 2023

Source: DLA Piper GDPR fines and data breach survey: January 2023

4 The Next Step? The European Cyber Resilience Act

In fall of 2022, the European Commission introduced its proposed Cyber Resilience Act (CRA), another first of its kind. Their intent is to set common security standards for connected devices and services, which would make the CRA the first IoT legislation anywhere in the world.

The goal of the Act is to bolster cybersecurity rules to ensure more secure hardware and software products, which are increasingly subject to successful cyberattacks. Per the Commission, such products suffer from two major problems, adding costs for users and society:

- a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them
- an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner

The current EU legal framework does not address cybersecurity of increasingly targeted **non-embedded software** like applications. The Cyber Resilience Act will change that.

The bottom line is that products lack sufficient security and consumers lack enough information to make informed decisions.

European Commission President Ursula von der Leyen pointedly stated that "If everything is connected, everything can be hacked…we need a European cyber defense policy, including legislation setting common standards." The CRA will provide just that.

The Commission notes that while there is existing internal legislation that applies to certain products with digital elements, there is no EU cybersecurity legislation that covers most hardware and software products. They particularly call out that the current EU legal framework doesn't address the cybersecurity of non-embedded software (e.g., applications), even if cybersecurity attacks increasingly target vulnerabilities in these products. That translates into big implications for application developers and their surrounding ecosystems.

The bottom line is that **products lack sufficient security** and **consumers lack enough information** to make informed decisions.

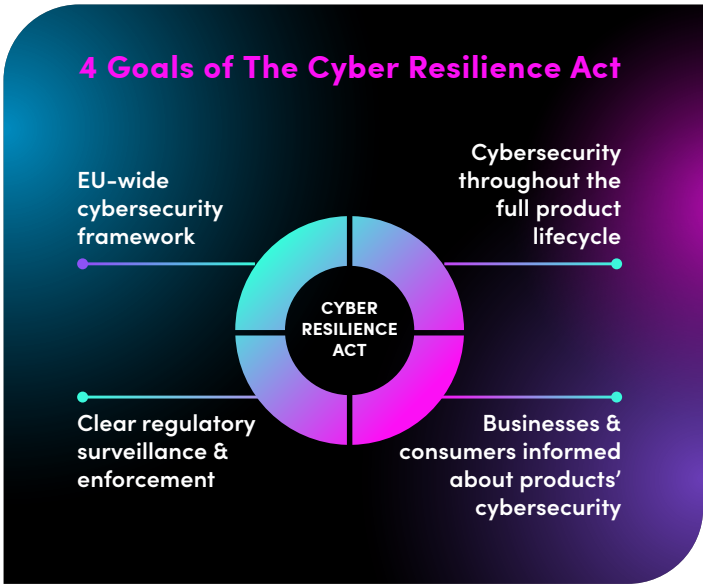
5 What Will the Cyber Resilience Act Require?

The CRA will apply to manufacturers, developers and distributors of both hardware and software products that contain connected digital elements. The proposed legislation outlines four specific goals to ensure that:

- connected products sold in the EU market are more secure due to having a coherent cybersecurity framework that manufacturers and developers must comply with
- manufacturers remain responsible for addressing cybersecurity throughout a product's entire lifecycle, from design through retirement
- there is increased transparency about connected products' security properties so that businesses and consumers are properly informed about the cybersecurity of the products they buy and use
- there are clear rules on regulatory surveillance and enforcement of the new rules and regulations

The implications for the manufacturers, developers and distributors impacted by this new law will be significant. Just a few examples of the proposed requirements stipulate that connected products:

- are designed, developed and produced with limited attack surfaces and to ensure an appropriate level of cybersecurity based on the risks
- are delivered without any known exploitable vulnerabilities and with a secure by default configuration
- protect against unauthorized access through appropriate control mechanisms



Additionally, manufacturers will be required to:

- protect the confidentiality of stored, transmitted or otherwise processed data, and process only data that are necessary for a connected product's intended use
- identify and document vulnerabilities and components in products, remediate them without delay, and disclose them as soon as security updates are available
- provide detailed information and user instructions about a specific product's cybersecurity and how to install security-relevant updates

There are many more defined requirements, all intended to empower users to make informed choices and understand their available forms of recourse if products they purchase impose undue cyber risk. This will stretch vendors' cybersecurity efforts to new levels.

Anyone working in the technology sector knows it will be challenging to meet these demands. While developers and manufacturers may already address some of these provisions, it is highly unlikely anyone incorporates all of them. Looking over the full list shows how daunting this effort may become.

6 CRA Certification Requirements by Product Type

There are three categories of "products with digital elements" proposed under the CRA, based on a product type's level of risk: Critical Class I, Critical Class II and Default.

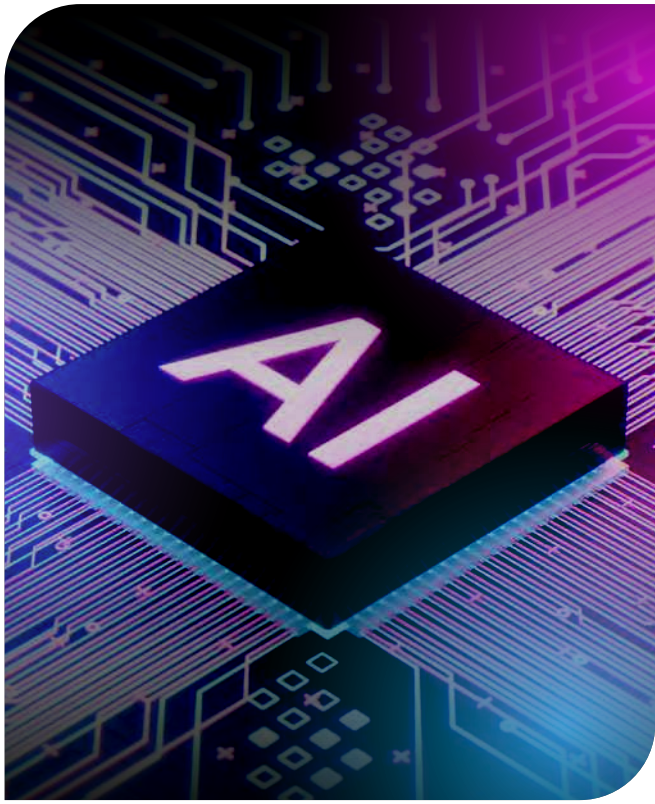
Default

The Default category includes products without critical cybersecurity vulnerabilities. For example, those might include things like word processors, hard drives, video games, photo editors, smart appliances and the like. It is estimated that 90% of products sold into the EU will be in the Default category.

While they must comply with the CRA's terms, manufacturers of Default products will be permitted to self-assess and self-certify as to their product's compliance with those requirements. They will need to complete certain technical documentation, submit a written EU declaration of conformity with the CRA's requirements, and affix a "conformity mark" to the product. They will also need to conduct regular testing for vulnerabilities and update their self-certification as products are upgraded or otherwise changed over their life span.

Critical

Critical Class I and II products are considered, as the name suggests, higher-risk – such as mobile and desktop devices, IoT devices, virtualized operating systems, microprocessors and more. Manufacturers of these products will not be permitted to self-certify but instead will be required to undergo a compliance process with the regulatory body designated by each EU Member State into which the manufacturer sells the product.



- Class I products have a higher level of risk than Default products, but a lower level of risk than Class II products. Class I will require the application of a standard form or third party-assessment to demonstrate compliance

- Class II products have the highest level of risk, and will therefore require completion of a third-party assessment to demonstrate compliance with their more stringent CRA obligations

A full current list of Class I and Class II products is available on page 7, although the EU may expand or reduce it over time.

Each European Union member state will be required to designate its own market surveillance authority to ensure effective CRA implementation and manufacturer compliance. Those authorities may be required to cooperate with each other and ENISA regularly regarding concerns about particular products and enforcement of CRA terms.

Does your product fall into one of these categories?

Cyber Resilience Act: Critical Products with Digital Elements

Class I: Requires application of a Standard a Third-Party Assessment

- Identity management systems software and privileged access management software
- Standalone and embedded browsers
- Password managers
- Software that searches for, removes, or quarantines malicious software
- Products with digital elements with the function of virtual private network (VPN)
- Network management systems
- Network configuration management tools
- Network traffic monitoring systems
- Management of network resources
- Security information and event management (SIEM) systems
- Update/patch management, including boot managers
- Application configuration management systems; Remote access/sharing software
- Mobile device management software
- Physical network interfaces
- Operating systems not covered by class II
- Firewalls, intrusion detection and/or prevention systems not covered by class II
- Routers, modems intended for the connection to the internet, and switches, not covered by class II
- Microprocessors not covered by class II
- Microcontrollers
- Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities
- Industrial Automation & Control Systems (IACS) not covered by class II, such as PLCs, DCS, CNC, SCADA
- Industrial Internet of Things not covered by class II.

Class II: Requires a Third-Party Assessment

- Operating systems for servers, desktops, and mobile devices
- Hypervisors and container runtime systems that support virtualized execution of operating systems and similar environments
- Microprocessors intended for integration in programmable logic controllers and secure elements
- Firewall, intrusion detection and/or prevention systems intended for industrial use
- Public key infrastructure and digital certificate issuers
- General purpose microprocessors
- Routers, modems intended for the connection to the internet, and switches, intended for industrial use
- Secure elements
- Hardware Security Modules (HSMs)
- Secure cryptoprocessors
- Smartcards, smartcard readers and tokens; Industrial Automation & Control Systems (IACS) intended for the use by essential entities, such as PLCs, DCS, CNC and SCADA
- Industrial Internet of Things devices intended for the use by essential entities
- Robot sensing and actuator components and robot controllers
- Smart meters.

7 How Might the Cyber Resilience Act Impact Technology Development?

In Chapter 1 we discussed several of the leading challenges that make connected devices inherently risky, including widely adopted development practices on which the industry relies. Under the CRA, developers and manufacturers of connected products will face a reckoning on how they need to revise many of those practices to make their products as secure as possible.

DevSecOps

The growing use of the Development Security Operations (DevSecOps) methodology offers a starting place. DevSecOps is an extension of the Development Operations (DevOps) method of iterative software development, which integrates security into the product development cycle from the beginning. The term "shift left" is frequently used to describe this practice. As manufacturers undertake new product development, security professionals along with architects and engineers will need to collaborate to address CRA's impacts on the entire product lifecycle. It makes sense to start from the very beginning.

Open Source

It is also very commonplace for developers to incorporate open source code into new products or updates. By its nature, open source software is publicly accessible and available to anyone to see, modify or use, free of charge. Peer review and community input help ensure quality, but there are no guarantees that any piece of code is secure. In fact, experts predict significant growth in bad actors' efforts to intrude through overlooked attack surfaces like open source software.

Currently, the proposed CRA text says that

> *"In order not to hamper innovation or research, free and open source software developed or supplied outside the course of a commercial activity should not be covered by this Regulation. This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable."*

However, per global advocacy organization the Internet Society, that requirement could negatively impact not-for-profit open source organizations that sustain themselves by selling consulting or other support services or are sponsored by commercial entities. The fear of liability could stifle open source development on which the IT industry depends. Undoubtedly this issue is integral to EU Member Country debate on modifying and adopting the CRA.

Cyber Insurance

An important business issue for connected device manufacturers and those who buy their products to consider is **cyber insurance.** The number of companies purchasing cyber insurance has risen steadily over the last decade. In the last two years, the massive increase in cyberattacks and the growing exposure of IT-dependent organizations have forced cyber insurers to broaden what their policies cover. Premiums are skyrocketing (by an average of **28% in Q1 2022** compared with Q4 2021), and policy underwriting has become far more strict. New regulations like the CRA will increase the pressure on connected devices manufacturers to **strengthen their defenses and reduce liability claims.** Organizations operating in the EU will likely need to prove to cyber insurers that their IT infrastructure is CRA compliant.

8 The Shifting Policy Landscape

As it progresses through the legislative process, the draft Cyber Resilience Act text is subject to a thorough debate and negotiating process among the EU Member States. The final text will be different from the starting place. However, it is a near certainty that the Act – in some similar form – will pass.

While ENISA will have EU-wide oversight of the CRA, each member state will need to designate a market surveillance authority for enforcement. Those entities may already exist and have their responsibilities expanded; or, a country may elect to create a new entity for this purpose.

These authorities will be able to order the withdrawal or recall of a product deemed non-compliant from the market. They will also be able to levy fines, with the proposed amounts up to the greater of €15 million or 2.5% of total worldwide annual turnover.

We've already seen this with the GDPR. The table in Chapter 3 listed just the largest fines imposed under the GDPR since its May 2018 implementation, but there have been many additional fines and over 1660 enforcements as of early 2023. While trying to not be excessively punitive, the EU has made clear that it takes data protection very seriously.

They will also be able to levy fines, with the proposed amounts up to the greater of

€15 million

or

25%

of total worldwide annual turnover.

After nearly five years, the GDPR has also had a significant global impact on data governance, data monitoring, and business and public awareness of improving data privacy and usage. More than one hundred twenty countries, from every developed continent, have now enacted international privacy laws and standards. As the EU now actively develops this sweeping new regulation, we may see the CRA as the hallmark of another seminal change.

The U.S. joins the movement

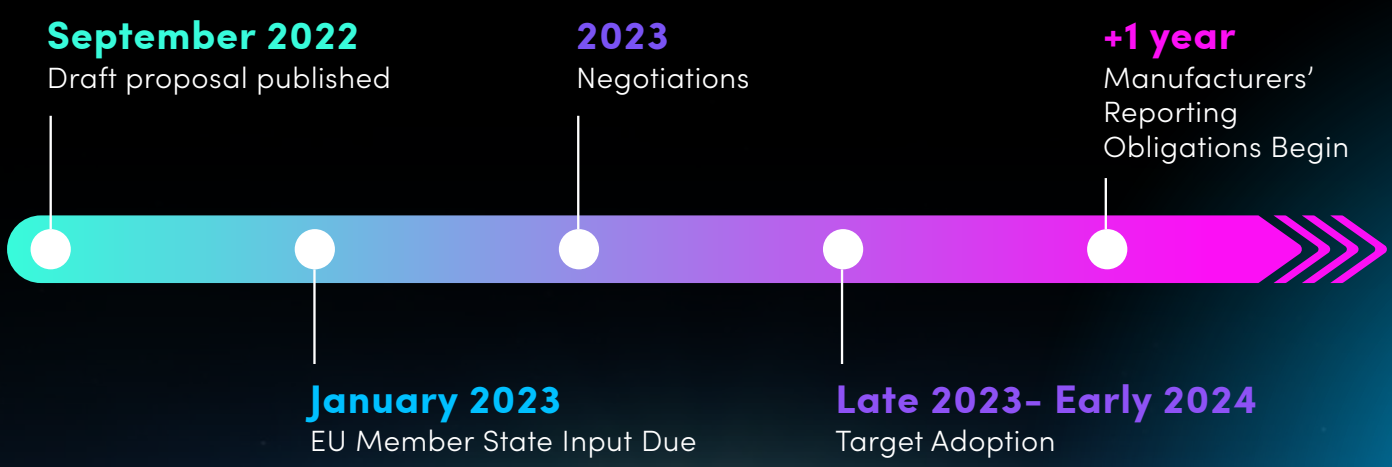
The U.S. federal government is also significantly shifting its stance on cybersecurity. Noting that to date, individuals, small businesses and local governments have been left to fend for themselves, the Biden Administration's March 2023 National Cybersecurity Strategy emphasizes rebalancing the responsibility to defend cyberspace by shifting the burden "onto the organizations that are most capable and best-positioned to reduce risks for all of us." That means the industry creating cyber vulnerable products. At the same time, the head of the U.S. Cybersecurity and Infrastructure Security Agency (CISA) is also calling for software manufacturers to be held legally liable for the insecurity of their products. CISA is working to push specific secure-by-design and secure-by-default restrictions for technology developers.

The writing on the digital wall

Clearly, governments are starting to take a firm stance on new policies that will change the market's approach to cybersecurity as we have known it throughout the history the internet and connected technologies. While details are still being worked through, a major shift is coming. It makes no business sense for technology developers to maintain multiple product lines fitted to slightly different policy regulations across their global operations. A more comprehensive, greatest common denominator approach will help prepare for a breadth of regulatory eventualities that technology creators will likely soon be facing.

Many companies waited too long to prepare for the GDPR, leading to near panic during the final months before implementation. Considering the CRA is being actively debated as of this writing, connected device developers and manufacturers will be well served to start preparing now for what may be a very different market reality in the next two to three years – a short time in the overall process of bringing new products to life and to market.

Estimated Cyber Resilience Act Timeline



9 How Should You Start Preparing for the Cyber Resilience Act?

As of early 2023, it is unclear if the final provisions of the CRA will apply to third-party application and device developers and non-manufacturing application device development, or be limited to manufacturers who produce applications and devices. If the former, that broad application will have enormous impact on those in the IT business. But even if the scope is more narrow, the impact will still be great. For those entities who intend to keep the EU as part of their market, several steps can be taken to get started:

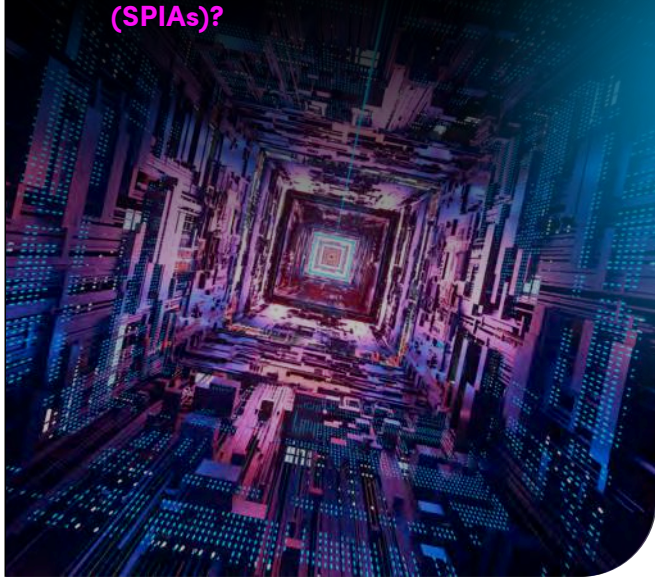
- Audit and assess your current application inventory and add in-app protection to all active applications. Note it's best to allow only apps identified as low-risk to connect to your cloud and server environments. That way, during the next high-profile exploit age, a new exploit can only be effective by overcoming installed app security protections and "tricking" them to report the exploit as low-risk – not an easy feat.
- Integrate application security into continuous integration/continuous (CI/CD) development processes
- Implement detect and response tools to monitor all connected devices, including unmanaged consumer endpoint devices utilizing your apps
- Implement attack pattern detection and prediction capabilities into SOC teams to mitigate future threats

Taking these steps now will not only help prepare for the CRA and other policy changes, it will go a long way to overcoming blind spots in specific products and the entire networked environment.

Will We Soon Need "SPIAs"?

The GDPR requires that organizations perform **Data Protection Impact Assessments (DPIAs)**, a type of risk assessment of their high-risk data processing activities could impact data subjects.

Might the CRA require Security Protection Impact Assessments (SPIAs)?



10 How can Verimatrix help?

One of the fastest-growing enterprise security threats today is from millions of mobile apps and the billions of connected consumer devices. Surprisingly, most of these apps and devices are unprotected and unmanaged. Any business that has an app is at risk. There are several vendors in-market who provide mobile app security or offer cybersecurity for connected devices (typically managed employee devices), but very few that can protect apps and defend the enterprise against the myriad of unmanaged devices powered by those apps. Verimatrix excels at doing both.

Verimatrix XTD (Extended Threat Defense) expands defense to the new endpoint, defending against endpoint attacks by preventing apps from being weaponized. XTD enables configuration capabilities that only allow apps with low-risk scores to connect, adding an independent second factor of security to the enterprise security ecosystem.

The Verimatrix XTD cybersecurity suite includes:

XTD Prevent

Start by securing your Android and iOS apps with RASP and multi-layered shields, plus DDoS protection, to develop bulletproof apps. Deploy immediately with our agentless, zero code cybersecurity with telemetry.

XTD Detect and Respond

Monitor, detect and respond to a new type of endpoint cyberthreat; unmanaged, connected consumer devices.

DevSecOps Toolkits

Code Shield and Key Shield – Protecting app code and protecting cryptographic keys with customizable engineering toolkits to disrupt hackers from reverse engineering code.

Verimatrix XTD can help you be compliant with CRA, while also protecting your bottom line and your valuable reputation. Empowering you to mitigate cybersecurity risks and safeguard consumer data, Verimatrix XTD closes vulnerabilities in your enterprise security wall and helps you overcome blind spots that are putting you – and your customers – at risk.

Contact us to discuss how Verimatrix can protect your applications, content, revenue, and business with frictionless security.

11 Glossary

API	Application Programming Interface
CRA	Cyber Resilience Act
DevOps	Development Operations
DevSecOps	Development Security Operations
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation
IoT	Internet of Things
XTD	Extended Threat Defense

12 Sources

- https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
- https://www.dataprotectionreport.com/2022/10/the-proposed-eu-cyber-resilience-act-what-it-is-and-how-it-may-impact-the-supply-chain/
- https://www.internetsociety.org/blog/2022/10/the-eus-proposed-cyber-resilience-act-will-damage-the-open-source-ecosystem/
- https://www.weforum.org/agenda/2022/12/cybersecurity-european-union-nis/
- https://dr2consultants.eu/european-cyber-resilience-act/
- https://datamatters.sidley.com/2022/11/09/european-commission-publishes-draft-cyber-resilience-act/
- https://datainnovation.org/2022/09/an-overview-of-the-eus-cyber-resilience-act/
- https://datamatters.sidley.com/2022/11/09/european-commission-publishes-draft-cyber-resilience-act/
- https://www.techtarget.com/searchitoperations/definition/DevOps
- https://www.internetsociety.org/blog/2022/10/the-eus-proposed-cyber-resilience-act-will-damage-the-open-source-ecosystem/