

Securing E-commerce Mobile Apps

Armor of Trust: Threat Defense Best Practices
for E-commerce Mobile App Security

The Exploding E-commerce Market

E-commerce, the buying and selling of goods and services over the internet for both business-to-business (B2B) and business-to-consumer (B2C), has gone mainstream. In fact, e-commerce is the preferred method of browsing, selecting, transacting, and rating for a vast number of people.

As of mid-2021, the [UN Conference on Trade and Development](#) reported that global e-commerce had reached \$26.7 trillion. In its 2023 cybercrime report, [LexisNexis](#) revealed that in 2022, e-commerce transactions grew 17% Y/Y from 2021. And the annual growth rate of e-commerce revenue is projected to be 11.51% from 2023–2027, with user penetration expected to hit 66.6% by 2027¹. That's a lot of people transacting online!

Such a huge market opportunity is irresistible to hackers and other cybercriminals. Not only is there the potential to commit fraudulent transactions for immediate financial gain, but e-commerce sites capture and store huge amounts of customer data, which cyber-attackers love to exploit. That makes e-commerce one of the top targeted sectors for cybercrime worldwide.

A LexisNexis report noted that in 2022 there was a 195% increase in the number of automated bot attacks on e-commerce sites, as well as a 29% increase in human-initiated attacks on them. With online sellers incorporating more technologies to extend their reach and improve their users' experience, the number of targets grows exponentially. That includes mobile technologies, as customers turn to the convenience of shopping – and buying – from wherever they happen to be.

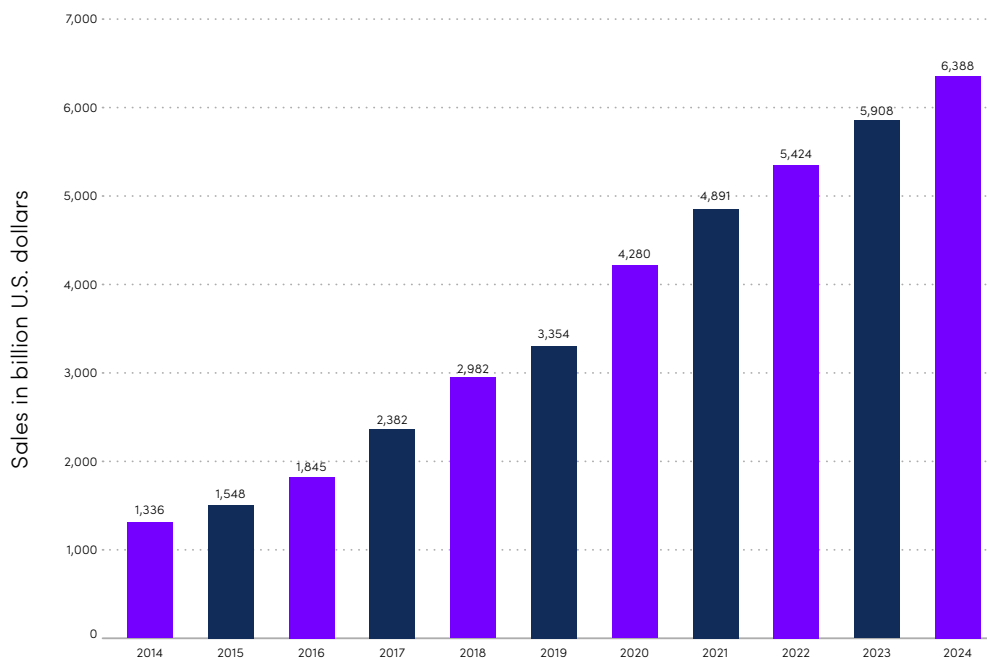


CHART: Global retail e-commerce sales worldwide from 2014 to 2024 (in billion USD)

Source: International Trade Administration

¹ Source: Statista e-commerce Report 2023

In 2022 there was a 195% increase in the number of automated bot attacks on e-commerce sites, as well as a 29% increase in human-initiated attacks on them.

Source: LexisNexis, 2022

CHAPTER 2

Common General Cyber Threats to E-commerce

There are a wide range of cyber threats facing e-commerce businesses. On e-commerce sites, it is common for companies to integrate multiple third-party applications and plugins to provide an engaging and convenient customer experience. The security and trustworthiness of those solutions can vary greatly. On the client side, which is frequently a mobile device, attacks are often aimed at the web browser, with customers not even realizing their device has been compromised.

Here are some of the most common threats:

- ▶ **Transaction fraud** - Hackers are adept at getting access to unsuspecting consumers' payment information and using it for fraudulent e-commerce transactions. Most consumers are never aware of the transaction until they check their credit card or bank statements. At that point, most victims challenge the transaction and request a chargeback. The e-commerce company is usually then stuck not only for the lost goods but the fees and other costs involved with settling the claim.
- ▶ **Phishing** - One of the leading ways fraudsters get that consumer information to commit fraud is through phishing. A tried-and-true form of social engineering, phishing tricks users into providing personal information – login credentials, account numbers, government identification numbers and more – by using legitimate-looking sources like emails or texts to ask for this data. In recent years, phishing schemes have gotten incredibly sophisticated, making them ever harder for users to detect.
- ▶ **Skimming and Magecart attacks** - Cyber criminals use a range of methods to skim code and capture payment card data and other personally identifiable information from e-commerce payment processing web pages. These attacks are often attributed to "Magecart" hacker groups who originally targeted the Magento (now Adobe Commerce) shopping cart and check-out e-commerce platform used by many popular e-commerce sites.
- ▶ **Bad Bots** - Automated bots are a growing mechanism for attacking e-commerce sites. They are used for a variety of malicious activities: price-scraping to gain competitive advantage in search optimization, scalping limited availability items to leverage their premium price, or fraudulently taking over accounts to get at customers' cash. It's common for bad bots to be masked as mobile web browsers, so as mobile e-commerce transactions increase, we can expect to see more bad bots being deployed.
- ▶ **SQL injection** - In this technique, hackers insert malicious SQL code that manipulates back-end databases into displaying information in e-commerce applications that wasn't designed to be and shouldn't be revealed – like sensitive customer or company data.

Estimated e-commerce losses to online payment fraud in 2021 were \$20B – a 14% increase over 2020.

Source: World Financial Review

40% of fraudulent traffic is hitting mobile applications.

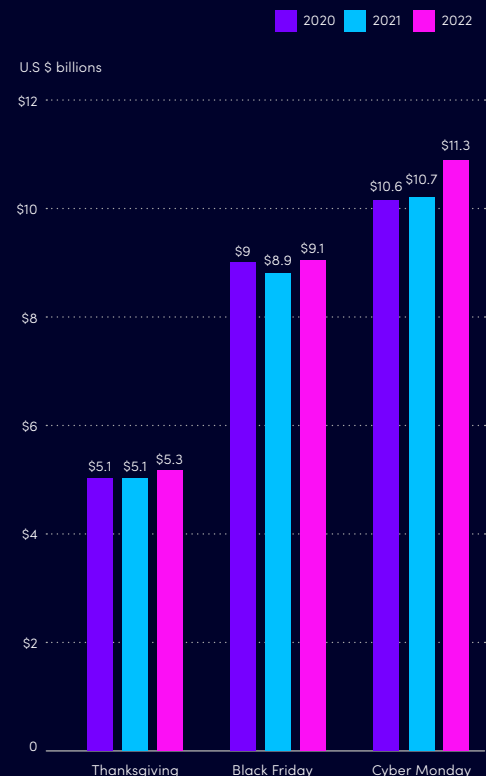
Two-thirds of e-commerce companies said that focusing on mobile application and API protection is a key priority for the next 12 months.

- ▶ **Cross-site scripting** - This type of attack involves inserting some malicious code (often JavaScript) into a webpage, where it captures customers' information in real time while they're using the checkout. The customer information is redirected to a server controlled by the attacker. Since this kind of attack directly affects customers who are transacting, there is a great risk to a brand's reputation.
- ▶ **API attacks** - As businesses want to make their websites usable, consistent, and optimized across whatever platform the customer chooses, e-commerce applications are now being architected to have a front-end and a back-end, in a move to "headless commerce." Application Programming Interfaces (APIs) are integral to this architecture, and attacks on them are escalating quickly. Many APIs are used to enable connections to and from end points like mobile devices. As more people perform e-commerce through such mobile devices, we can expect to see attackers turn their attention to this new opportunity.

Shopping Trends Affect Risk

Cyber-attackers see particular opportunity in certain shopping circumstances:

- ▶ **Buy Now, Pay Later.** This approach allows for financing at the point-of-sale, letting online shoppers make a purchase and pay for it over time, often with no or low interest or fees. BNPL is very popular with Millennials and Gen-Z, who are well known for their reliance on mobile devices. [Allied Market Research](#) projects the volume of BNPL transactions will reach \$3.98 trillion by 2030. Unfortunately, the increase in BNPL is also increasing opportunities for online fraud. Account takeover is most common, where a bad actor accesses and uses an existing BNPL account to make unauthorized purchases. But attackers can also create new "mule" accounts to use stolen identities and credit card information for purchasing.
- ▶ **Hyped product launches.** Skilled marketers excel at driving up demand for limited-edition items through hype campaigns when these products enter the market. Those launches are highly susceptible to scalping, an age-old practice that has simply been integrated into the digital age. Bad bot operators try to prevent legitimate buyers from getting the inventory so they can resell it at the very high prices enthusiasts are willing to pay. For example, during the Black Friday 2021 period, there was a [massive scalping attack](#) of 9 million bot requests in 15 minutes on a global retailer's launch of a limited-edition item.
- ▶ **Holiday shopping seasons.** The traditional holiday season is likely cyber-attackers' favorite time of year! Attacks during the period from American Thanksgiving Day through Cyber Monday, when a high volume of excited shoppers are seeking the best deals, increase each year. Adobe reported that for the 2022 shopping season, US consumers spent roughly [\\$35.27B](#) online—and for the first time, most sales were done via mobile devices. TransUnion found that the average number of suspected digital fraud attempts during that time was [82% higher globally and 127% higher for US transactions](#) than during the rest of the year.



**U.S. Online Retail Sales 2020-2022:
Thanksgiving, Black Friday, Cyber Monday**

Mobile Apps Pose an Increasing Cyber Threat to E-commerce

What is the most important asset that e-commerce companies have? It's their customers. And how do e-commerce firms communicate today with their customers? It's via mobile applications. Apps are a fundamental part of a company's business. If the app or the connection between the app and the backend is compromised, then there is a problem. Today, applications are not protected. And as it's becoming more and more difficult for hackers to bypass security solutions in the enterprise, they look for alternatives—and apps offer the path.

There are several types of mobile app attacks that e-commerce companies need to worry about.



A **Repackaging Attack** is where hackers take a legitimate e-commerce app and modify it by adding malicious code or malware. The modified app is then repackaged and distributed through unofficial app stores or malicious websites, disguised as a legitimate download. When users unknowingly install these repackaged apps, they can compromise their device's security and expose personal information to cybercriminals.

Verimatrix XTD places multi-layered shields around the app, preventing attackers from reengineering or modifying it. Verimatrix XTD also reports attempted repackaging attacks to its e-commerce customers.



A **Screen Overlay Attack** is a type of mobile app cyberthreat where a malicious app displays an overlay on top of a legitimate e-commerce app on a device. This deceptive technique tricks users into unknowingly granting sensitive permissions or interacting with fake interfaces, leading to potential data theft, unauthorized access, or fraudulent activities. By presenting an overlay that mimics the appearance of a trusted app or system prompt, attackers can manipulate users into providing sensitive information, such as login credentials or financial details. This type of attack capitalizes on the user's trust in the legitimate interface and their willingness to interact with it.

Verimatrix XTD identifies when overlay screens are triggered and data is sent to malicious servers. XTD alerts the app owner, and preventive or responsive countermeasures can be taken.



A **Supply Chain Attack** is a cyberthreat that targets the mobile development software supply chain to compromise the integrity or security of mobile applications. In this type of attack, attackers infiltrate the software development process by compromising a trusted and legitimate component or vendor involved in app development. By injecting malicious code or backdoors into the compromised component, the attacker gains unauthorized access to the mobile app's codebase, allowing them to manipulate or compromise the app's functionality or introduce vulnerabilities. When users download and install the affected app, they unknowingly expose their devices and data to potential harm. Supply chain attacks are particularly concerning as they can impact a large number of users and evade traditional security measures.

Verimatrix XTD detects app communications with blacklisted connections and provides these to its e-commerce customers. On the roadmap: whitelist monitoring, whereby XTD alerts the app owner about unauthorized communications, identifying the backdoor and allowing app owners to respond.



An **Open-Source Vulnerability** refers to a cybersecurity risk found in mobile apps that utilize open-source software components. Open-source software is publicly available and can be freely used by developers to build their applications. However, sometimes these open-source components may have security weaknesses or vulnerabilities that hackers can exploit.

Verimatrix XTD hardens apps using multi-layered security techniques such as obfuscation to prevent static and dynamic code analysis, mitigating open source code exploitation risks. Essentially, XTD makes open-source app code difficult for an attacker to understand, thereby reducing the chance that open-source vulnerabilities will be exploited by attackers.



A **Payload Delivery Attack** is a mobile e-commerce cyberthreat where attackers try to deliver harmful software, called a payload, to a device through a malicious app or file. The payload can be malware or other malicious code that can harm the device or steal sensitive information. When users unknowingly download or install the malicious app or file, the payload is delivered, allowing hackers to gain control over the device or access the user's data. Think of the cyberattack as a cruise missile. The missile has two main parts: the rocket and the warhead. The rocket's purpose is to deliver the warhead to the target without being detected or intercepted. The warhead's job is to create damage. Often, a mobile app is the rocket and not the warhead. It helps deliver the attack to the right place without being detected or blocked. The rocket does not cause the damage, but without it, there is no attack.

Verimatrix XTD prevents payload delivery attacks by shielding the app from modification and infection. XTD detects connections from emulators and can immediately prevent the app from opening.



Geo-spoofing is a mobile app cyberthreat where attackers trick an e-commerce company's app into believing it is located in a different geographic location than it actually is. They can use special techniques to manipulate GPS signals or network information to make it appear as if the device is in a different city, country, or even continent. Or they can use a VPN. This can lead to various risks, such as accessing geo-restricted content, evading location-based security measures, or engaging in fraudulent activities.

Verimatrix XTD detects VPN connections, as well as any banned locations specified by the customer, and can immediately block the app or even shut it down.

A hand holding a smartphone is the central focus, set against a dark blue background with a bokeh effect of colorful light spots. A large, thin purple circle is overlaid on the left side of the image. The text is centered in white, sans-serif font.

Publicly traded businesses may also experience a drop in their market value. For instance, a Comparitech study of 40 data breaches at 34 companies listed on the New York Stock Exchange found share prices fell an average of 3.5% following an attack.

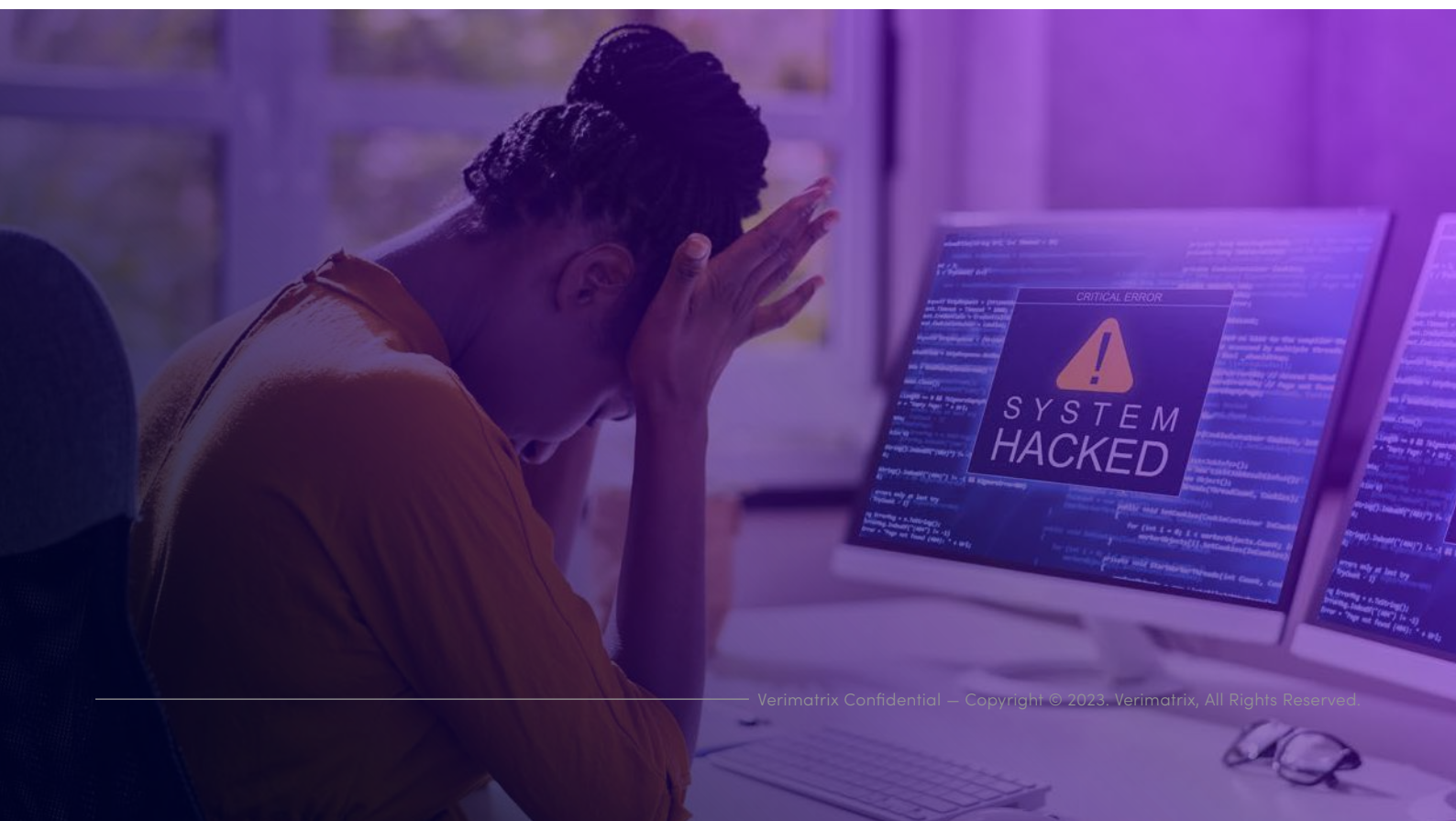
Source: Comparitech

CHAPTER 4

Potential Impacts of Cyberattacks on E-commerce Services Institutions

A successful cyberattack significantly impacts an e-commerce business. Negative effects can be far-reaching and may only become fully evident over time. Generally, impacts fall into a few categories:

- ▶ **Economic.** The most obvious financial losses can come from fraud, customer chargebacks, and theft of bank or credit card data, which result in the loss of actual cash. There are other potential associated costs—expenses related to recovering from a data breach; repairs to affected systems and networks; lost revenue due to halted transactions; even increased insurance premiums. Publicly traded businesses may also experience a drop in their market value. For instance, a [Comparitech](#) study of 40 data breaches at 34 companies listed on the New York Stock Exchange found share prices fell an average of 3.5% following an attack.
- ▶ **Operational.** Attacked e-commerce businesses can face interruptions to normal business operations that will increase overhead costs and result in lost revenue. There may also be a need to re-design systems for collecting, processing, and storing customer data to keep it more secure.
- ▶ **Reputational.** Customers are increasingly concerned about how businesses handle their information. When their data is compromised or they are victims of a fraudulent transaction, customer trust in an e-commerce business can be damaged. That can lead to losing those customers or even potential new customers as the negative reputation spreads. With online reviews and instant information sharing, that can happen very quickly.
- ▶ **Legal.** As explained in Chapter 5, there is a growing list of regulations to which e-commerce businesses are subject. These regulations exist across the US and in many countries around the world. Businesses that don't adhere to these regulations and apply appropriate security measures can face fines and sanctions from government entities, whose patience with data breaches, user tracking, and other technical issues seems to be getting shorter all the time.

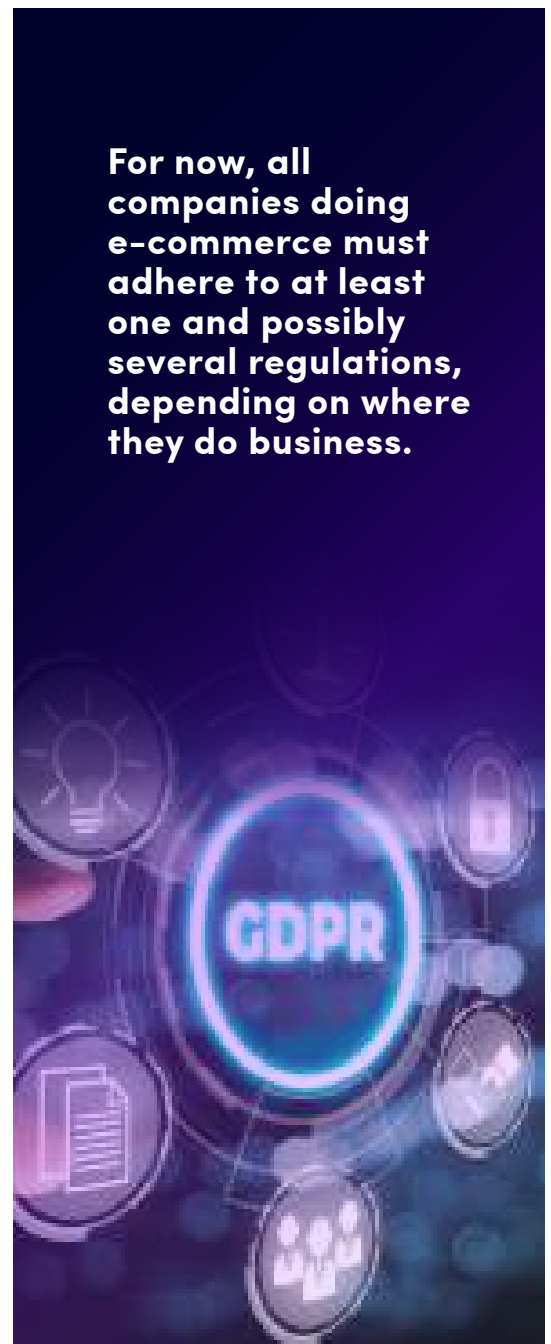


Growing Regulatory Pressure on the E-commerce Industry

There are several strict regulations already in place that affect companies doing e-commerce, particularly around payment information and personal data. As e-commerce transactions increase, there will most likely be more. For now, all companies doing e-commerce must adhere to at least one and possibly several regulations, depending on where they do business.

- ▶ **Payment Card Industry Data Security Standard (PCI-DSS):** Launched in 2006, the Payment Card Industry Data Security Standard (PCI DSS) is a security standard for ensuring that all companies that accept, process, store, or transmit credit card information maintain a secure environment for that data. The intent is to improve payment account security throughout the transaction process. PCI DSS is defined by the independent PCI Security Standards Council (SSC), but it is enforced by credit card companies.
- ▶ **General Data Protection Regulation (GDPR):** Adopted in 2016 and enforced as of 2018, the GDPR is a European Union law protecting the personal data and privacy of European Economic Area (EEA) citizens. It applies to e-commerce companies that sell to any of these citizens, regardless of where those companies are located worldwide. The GDPR sets firm rules for collecting, processing, and storing personal data of e-commerce companies, and the EU is known to be quite strict on enforcement.
- ▶ **California Consumer Privacy Act (CCPA) and other US state regulations:** Following the implementation of the GDPR, the state of California developed its own consumer data protection law to protect the data privacy rights of its citizens. It requires companies to provide consumers with transparency about how their data is collected, stored, and used and empowers them to opt-out of activities they are not comfortable with. The CCPA was amended by the California Privacy Rights Act (CPRA) to have even stricter consumer protections and is enacted as of July 2023. Besides the California laws, the [National Conference of State Legislatures](#) reported that in 2021, at least 13 states will have enacted 17 consumer data privacy bills, with comprehensive privacy legislation introduced in at least 25 more states.

For now, all companies doing e-commerce must adhere to at least one and possibly several regulations, depending on where they do business.






CHAPTER 6

The Value of Extended Threat Defense Technology in Combating E-Commerce Cyberattacks

The multitude of cyber-related challenges facing e-commerce institutions demands an elevated level of security to address the greatly increased risks in the modern environment of ubiquitous transacting. The current reality is that most mobile applications used by e-commerce businesses are not well protected. Since it's becoming more and more difficult for hackers to bypass enterprise-level security solutions deployed by larger e-commerce organizations, bad actors look for alternative entry vectors and discover the app path.

Extended Threat Defense (XTD) is the leading cybersecurity solution that secures e-commerce institutions from risks originating from mobile applications at the edge. While many companies have some form of cybersecurity protection for employer-issued managed devices and personal "bring your own devices" (BYOD), XTD addresses multi-vector threats stemming from unmanaged (consumer) mobile devices like smartphones and tablets.

That specifically includes the range of multi-vector threats that previous cybersecurity solutions like mobile threat defense (MTD) and extended threat detection and response (EDR) miss.

 MTD	 XDR	 XTD
Provides real-time protection against threats and allows organizations to remotely manage and secure their mobile devices.	Provides continuous monitoring of endpoint devices and can detect and respond to a wide range of security threats, including malware, ransomware, and advanced persistent threats.	Helps prevent, detect, respond to and predict cyberattacks originating from the mobile app to the edge, and specifically multi-vector threats.
Works on managed smartphones, laptops and tablets.	Works on managed endpoint devices.	Works on unmanaged devices; any device with an app.
Requires an agent to be installed on the device – protects institution employees' mobile devices, but impractical for end customers.	May take a more comprehensive security approach (continuous monitoring, incident response, and the ability to identify and remediate vulnerabilities). Lacks integration, limiting visibility into the security posture and slowing response.	Uses behavioral analysis like EDR (for detection) combined with other EDR and MTD elements. Ideal when numerous unmanaged consumer devices are connected to an e-commerce enterprise via the app.

XTD monitors new entry vectors from the fastest-growing attack surface—connected apps, APIs, and unmanaged devices. That makes XTD an essential component of effective cyber defenses for e-commerce businesses.

Polymorphic Protection: An Important App Security Attribute

An effective XTD platform should include polymorphic protective capabilities. This innovative approach involves constantly changing an application's code and structure to make it more challenging to hack. It's a bit like changing the password of your online accounts every so often to reduce your cyber vulnerability. Some savvy e-commerce firms are already protecting their mobile apps with polymorphic protection.

Developers can use various techniques to make an app's code and structure more resistant to attack. One approach is to use obfuscation, which involves modifying the source, byte, or machine code so that it becomes significantly more difficult for hackers to read and understand. In essence, polymorphic protection transforms mobile apps into moving targets, making it much harder—even annoyingly complicated, if not nearly impossible—for hackers to reverse engineer code and develop malware that can penetrate the app's defenses.

That way, the code cannot be used to potentially reveal an app's inner workings or any exploitable vulnerabilities that may be found within it. Obfuscated code is also far less susceptible to tampering. Given the e-commerce sector's particular vulnerability to cyberattacks, this approach is crucial for protecting customer information.

To implement polymorphic protection, e-commerce businesses must invest in tools that not only shield mobile apps but also provide threat detection and response capabilities.



The Verimatrix XTD Approach

Verimatrix XTD offers an affordable and user-friendly solution that utilizes cutting-edge technology to secure mobile apps. With its ability to detect and respond to attacks promptly, Verimatrix XTD ensures the safety of mobile applications and prevents potential damage. Our military-grade, multi-layered security is very difficult for hackers to penetrate. We also help customers monitor the fastest-growing attack surface: consumer endpoints. By analyzing extensive data, Verimatrix XTD can predict future attacks and provide proactive protection.

► **Covering a Wider Attack Surface with Zero-Code Protection**

Verimatrix XTD offers a truly distinct differentiator. Unlike those solutions that necessitate agent installation, Verimatrix XTD offers an agentless, zero-code approach. This capability enables the rich protection, attack detection, and response capabilities to be quickly and easily deployed without cumbersome development or coding—making speed to market a reality. This is especially valuable for the mobile transaction environment, where consumer devices with various levels of protection are always in play.

► **Addressing Multi-Vector Threats from Consumer Devices**

Verimatrix XTD monitors and mitigates cyber threats originating from apps downloaded to unmanaged consumer devices. While many organizations implement cybersecurity measures for managed devices such as BYOD, Verimatrix XTD is one of the few solutions designed to address the multi-vector threats arising from unmanaged mobile devices. XTD can do this because its telemetry is built into its app protection and is automatically passed on to every app instance downloaded. That means any device using the app can be monitored, effectively expanding the coverage of the attack surface into new realms. With Verimatrix XTD, e-commerce institutions can secure a broader range of devices, providing comprehensive protection against potential threats.

► **Detecting and Responding to Active Attacks**

Verimatrix XTD's proactive defense strategy involves the swift detection of active attacks and an immediate response to neutralize potential damage. By leveraging advanced threat detection techniques, Verimatrix XTD identifies attacks in real-time, enabling security professionals to disconnect compromised devices promptly. This decisive action safeguards sensitive data and prevents malicious actors from exploiting vulnerabilities.

► **Proactive Protection through Predictive Analytics**

One of the standout features of Verimatrix XTD is its capability to analyze vast amounts of data to predict potential attacks. By employing predictive analytics, the solution can anticipate threats even before they occur. This proactive approach empowers e-commerce businesses to stay one step ahead of attackers, ensuring enhanced security for their mobile applications and connected infrastructure.

► **Understanding Risks and Empowering Security Professionals**

Verimatrix XTD is dedicated to helping security professionals comprehend the risks associated with mobile applications and their connections. Highlighting the existence of blind spots by assigning a risk score to every threat found, Verimatrix XTD prompts e-commerce businesses to acknowledge and address potential vulnerabilities. XTD provides security professionals with a meticulously designed Software-as-a-Service (SaaS) offering. There is also an optional service incorporating the services of human data scientists to review your account and take response actions on your behalf, adding an extra layer of expert assistance to combat evolving app threats effectively.

Fight Back with Verimatrix XTD!

As the reliance on mobile applications grows in the e-commerce sector, so does the need for robust cybersecurity measures. Verimatrix XTD is an exceptional solution, providing affordable and user-friendly mobile app protection. With its agentless, zero-code approach, it allows for easy and painless deployment, allowing customers to monitor a wider attack surface, including unmanaged consumer devices.

Verimatrix XTD effectively detects active attacks and responds promptly, minimizing the potential for damage. By analyzing data and predicting attacks, it enables organizations to proactively protect their mobile applications. Armed with Verimatrix XTD's comprehensive security offerings and expert support, security professionals can effectively mitigate the risks associated with e-commerce app vulnerabilities and secure their digital assets.



Verimatrix — Award-winning Cybersecurity

Verimatrix helps power the modern connected world with security made for people. We protect digital content, applications, and devices with intuitive, people-centered, and frictionless security. We enable the trusted connections our customers depend on to deliver compelling content and experiences to millions of consumers around the world.

We are proud of the market recognition our innovative solutions have earned.



2023 Global Infosec Award for Hot Company in Mobile App Security – Cyber Defense Magazine



2023 Cybersecurity Excellence Awards – Gold Winner for Artificial Intelligence Security and Biggest Brand Growth



2023 Product of the Year, AI and Machine Learning – National Association of Broadcasters (NAB)



2022 Gartner® Hype Cycle™ for Application Security

[Get A Demo](#) of the Verimatrix XTD cloud-native platform, deployed in minutes to protect your apps!

Sources

<https://news.un.org/en/story/2021/05/1091182>

<https://www.statista.com/outlook/dmo/e-commerce/worldwide>

<https://risk.lexisnexis.com/about-us/press-room/press-release/20230517-cybercrime-report>

<https://www.trade.gov/e-commerce-sales-size-forecast>

<https://thehackernews.com/2022/11/top-cyber-threats-facing-e-commerce.html>

<https://www.bigcommerce.com/articles/e-commerce/e-commerce-website-security/>

<https://www.imperva.com/learn/application-security/magecart/>

https://niccs.cisa.gov/sites/default/files/documents/pdf/ncsam_eskimming_508.pdf?trackDocs=ncsam_eskimming_508.pdf

<https://datadome.co/bot-management-protection/survey-mobile-app-threats-critical-bot-protection-online-commerce/>

<https://www.alliedmarketresearch.com/buy-now-pay-later-market-A12528>

<https://www.imperva.com/resources/reports/2022-Imperva-Bad-Bot-Report.pdf>

<https://www.imperva.com/resources/resource-library/reports/the-state-of-security-for-e-commerce-2022/>

<https://www.practicalecommerce.com/sales-report-2022-thanksgiving-black-friday-cyber-monday>

<https://iapp.org/resources/topics/ccpa-and-cpra/>

https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

<https://www.practicale-commerce.com/sales-report-2022-thanksgiving-black-friday-cyber-monday>

https://www.imperva.com/resources/reports/The-State-of-Security-Within-eCommerce-in-2022_report.pdf

<https://www.trade.gov/e-commerce-sales-size-forecast>

<https://www.getcybersafe.gc.ca/en/blogs/e-commerce-cyber-security-introduction-online-merchants>
<https://www.helpnetsecurity.com/2021/12/16/mobile-application-api-protection/>

<https://worldfinancialreview.com/reshaping-e-commerce-to-the-new-global-market/>

<https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx>

<https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/>