Clarity eCommerce Security Overview

CLARITY

Executive Summary

Ecommerce security is an absolute requirement in today's environment. A key requirement is PCI-DSS compliance, making sure that there are role-based authentication and authorization formats in place. Specifically, in role-based authorization that there are physical separations between the critical aspects of the eCommerce platform. So that administrative versus user-facing, even different roles and what those roles have access to have physically separate areas of the application when needed.

> In addition, simple validation that the user is who they say they are, like multi-factor and authenticator options. Then finally being able to ensure that the system's overall capability, where it's hosted, how the APIs and various endpoints are accessed, the infrastructure itself, the database persistence layer, any caching, application, and application files are all hardened and secured is critical.

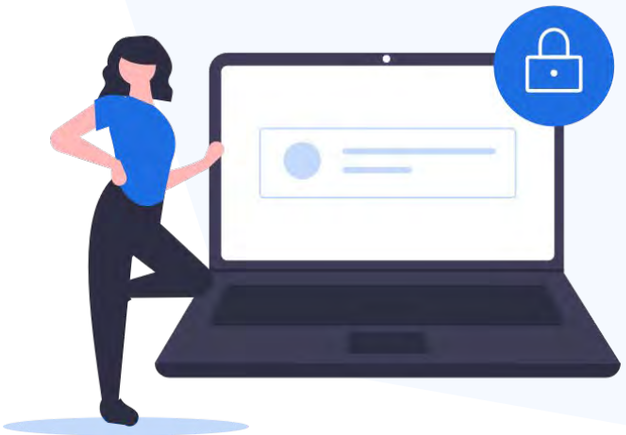
> Clarity specializes in delivering custom results within a timely fashion – read more below to find out how we can deliver for your organization.

eCommerce Security Protocols

Unfortunately, there are a lot of threats today to public-facing web-facing sites, and these threats will be ever-increasing and persistent in the landscape of the future eCommerce platform. So, what we recommend is that your team evaluates eCommerce platforms' baseline security as a requirement. Now its also possible for eCommerce systems to meet higher standards and requirements or capabilities. This can include the requirement to meet: HIPAA, GDPR, NIST, CMMC, and various other security requirements. This might also include ongoing penetration tests, ongoing active support and patching, and automated security patching as needed.

We encourage that you work with a vendor and team that offer a highly secure capability with a systematic approach to patching and updating while incorporating options for you to turn on more advanced security features without incurring significant additional costs.

Vendor Selection & Infrastructure



We encourage that you work with a vendor and team that offer a highly secure capability with a systematic approach to patching and updating while incorporating options for you to turn on more advanced security features without incurring significant additional costs. We do have multi-factor authentication built into our core platform and a robust set of role-based authorization and per endpoint security access by role. They can have an infinite number of roles and users within roles that make it possible to control who has access to what. We can physically separate parts of the application to differentiate different parts of the APIs and application.

Although this isn't standard, this is a capability based on the scenario and what is needed. For the administrative branches of the application, we typically have that as a physically separate infrastructure so that it isn't accessible by the public in any way. This is just an option you can consider depending on the security footprint you need to maintain or restrict.

In addition, just going into the infrastructure side of things. This is something we heavily specialize in as we work with clients who must meet HIPAA, GDPR, NIST, CMMC, and other various compliance requirements that may not be prevalent but are very restrictive. We have had to comply with these at scale for large medical and bio-science organizations, which are processing hundreds of thousands of transactions in a short period. So, whenever you look at your security infrastructure, you will need to ensure a hardening process. We work with both cloud infrastructure and physical or virtualized infrastructure.

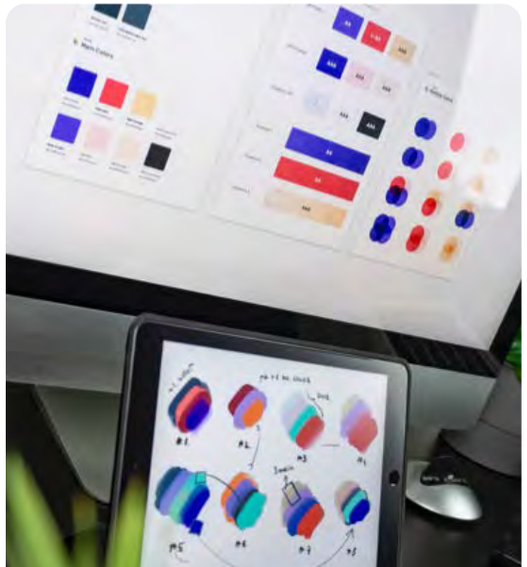
Vendor Selection <cont.>

Depending on the infrastructure, there are various nuances and use cases unique to each type of infrastructure. This can provide a means for a weakness or a hole in the infrastructure. We do recommend not just penetration testing but also Whitehat hacking attempts depending on the scenario. We conduct these internally with our certified Whitehat hackers who have government clearance and have passed advanced government training to be Whitehat hackers.

- Bluprints for Securing the Data at Rest
- Tokenization processes to reduce the data that is stored on publicly facing infrastructure
- A multilayered infrastructure would have to get through several layers of increasingly complex encryption to get to the layer that stores the data.

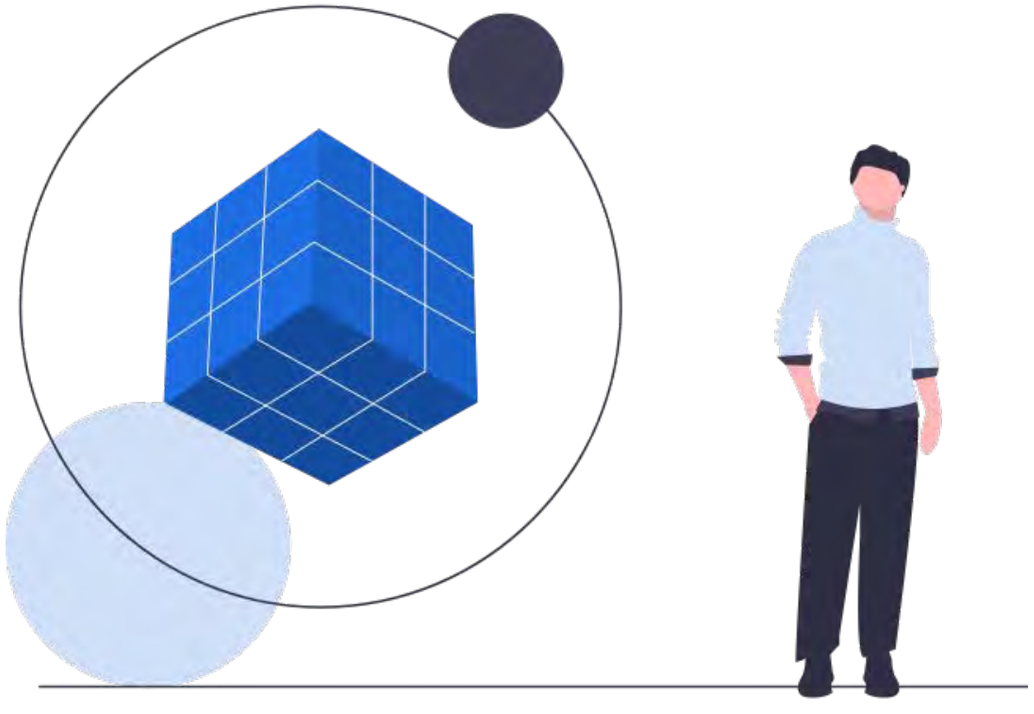
Fundamentally, infrastructure security is heavily reliant on the following best practices:

Although these are things that we will get into further during discovery, the core concepts are to follow best practices and blueprints that are well documented.



Infrastructure <cont.>

We do have hardening guides and infrastructure recommendations, and best practices that we can provide on request. If we are using Azure, we will use the security and compliance center to ensure that we are constantly updating and keeping the infrastructure up to date. In addition to the infrastructure side of things, we also have specific hardening steps such as; CMMC, NIST, HIPAA, GDRP, etc. These all take quite a bit of detailed planning and decision making but ultimately are aspects that we have delivered on for dozens of clients. We can provide demos and reviews of how we completed these implementations if you're interested in more information. Fundamentally, when operating and configuring the platform, we encourage and focus on security as an absolute requirement and development in the architecture.



General Data Protection Regulation

GDPR Compliance

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). Since the Regulation applies regardless of where websites are based, it must be heeded by all sites that attract European visitors, even if they don't specifically market goods or services to EU residents.

- Data Processing Lawfulness, Fairness and Transparency
- Data Collection Explicity Stated to Data Subject
- Collect & Process Absolutely Necessary Data
- Personal Data is Accurate and Up to Date
- Limited Storing of Personally Identifying Data
- Ensure Security, Integrity, and Confidentiality
- Data Controller Responsible for GDPR Compliance

Health Insurance Portability & Accountability Act

HIPAA Security Rule

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

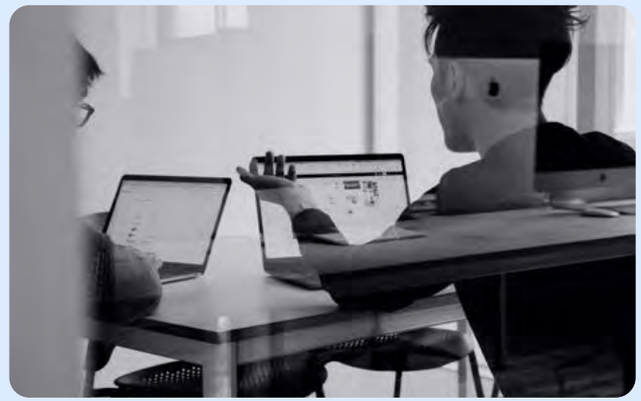
- Basic design of home page and an internal page, based on your design requirements.
- Light customization of header, footer, menu and color palette for professional presentation.
- $100 credit towards free graphics / graphic work to ensure great site imagery.
- More extensive design is available and very commonly includes robust designs of all pages and detailed branding and
  style guide – often times with detailed UI/UX analysis as well.

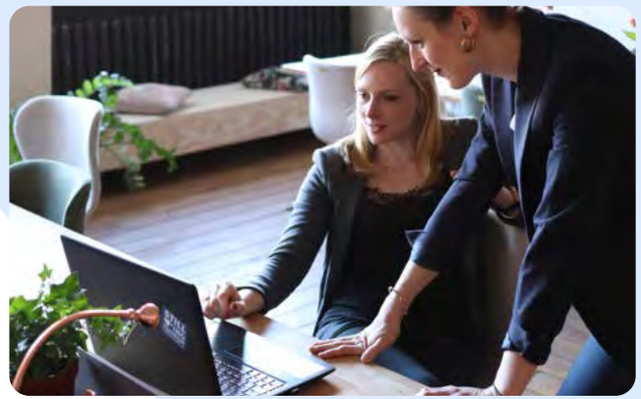
National Institute of Standards and Technology

NIST Cybersecurity Framework

NIST standards are based on best practices. That's why the government has been recommending them for use by companies or organizations. Among NIST's standards and guidelines, the most widely adopted is the NIST Cybersecurity Framework (CSF), used for assessing cybersecurity risks. There is also NIST 800-171 and NIST 800-53, which tackle unclassified information. The NIST CSF uses these 5 core areas to evaluate security controls:

- Identify
- Protect
- Detect
- Respond
- Recover





CMMC Compliance

Cybersecurity Capability Maturity Model

Cybersecurity Capability Maturity Model (CMMC) certification is the US Government's solution to fix low rates of compliance associated with NIST SP 800-171. CMMC is not optional and is designed to permit only allow businesses with a valid CMMC certification to bid on and win contracts with the US Government.

Organizations must show assessors that they demonstrate the institutionalization of both processes and practices, and in cases where an organization demonstrates differing levels for one or the other, the organization will be certified at the lower of the two levels.

- CMMC level 1: Safeguard federal contract information
- CMMC level 2: Serve as a transition step in cybersecurity maturity progression to protection controlled unclassified information
- CMMC level 3: Protect CUI
- CMMC levels 4-5: Protect CUI and reduce the risk of advanced persistent threats

Get in Touch with Clarity

If you are a business, ready to move forward with credit card processing savings, please give us a call so we can help.

+1 (800) 928 - 8160

clarity-ventures.com

Jeremy Howell

Director Business Development

jeremy.howell@claritymis.com

Philip Ganoe

Director of Sales

philip.ganoe@claritymis.com

CLARITY