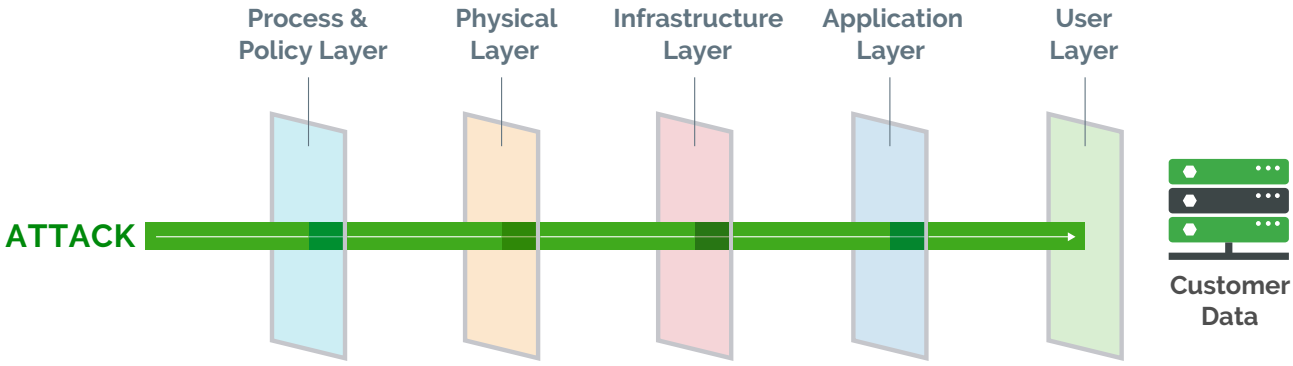
ARENA SECURITY

Bring Innovation to Life

Arena offers a dependable, scalable, and secure solution to our customers.

In addition to our dedicated focus on infrastructure and process security, we know transparency is critical to our customers' trust and confidence when achieving success with our product realization platform. In this document, we provide a detailed primer on the technologies and measures we use to protect our customers' product information.



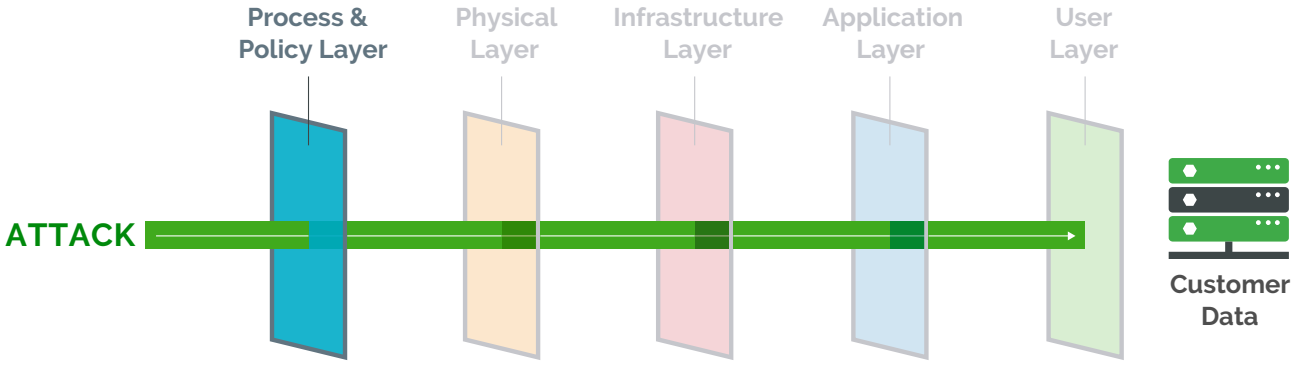
Layers of Defense to Protect Valuable Data

Arena's security model is robust, protecting our customers' valuable product and quality information managed through the application layer as well as the administrative user data configured by customers. This data is crucial to our customers' business, so protecting it is our core priority. By prioritizing security in our platform architecture, we provide customers one of the most secure places for data at scale, in or out of the cloud.

Arena uses a multi-layer approach to protect customer data. Arena is architected to address every layer of security—from physical data center provisions to access privileges that control user access to product information and processes. Each security layer provides a specific level of protection. The remainder of this document explains the type of security provided at each layer of the solution.

Process & Policy Layer

The first layer of defense is a well-defined and comprehensive set of security processes and policies to ensure the security of our customers' data and user accounts. Our customer data protection policies and rigorous internal procedures ensure that there is no unauthorized access to customer data.



ptc

Service Control Organizations

Arena's solution is SOC 2 Type 2 compliant. The American Institute of Certified Public Accountants (AICPA) Service Organization Controls (SOC) reports give assurance over control environments as they relate to the retrieval, storage, processing, and transfer of data. The reports cover IT General controls and controls around availability, confidentiality, and security of customer data and are issued for 6-month periods each year. Arena's platform undergoes a regular third-party audit to certify against this standard.

Change Control

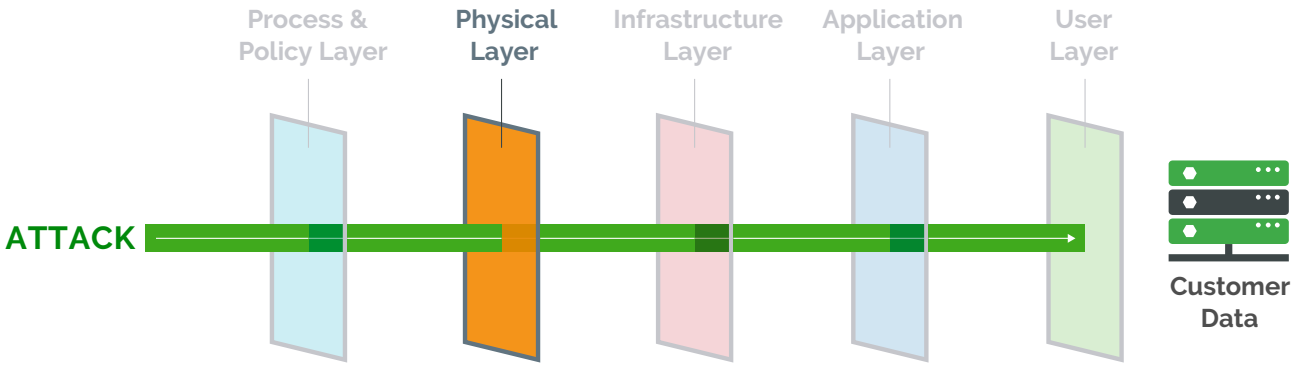
A formal change control process addresses the risk associated with system and standard operation procedure (SOP) changes. The process tracks changes made to the hardware and software systems and SOPs, then assesses risk, explores dependencies, and considers and applies necessary policies and procedures before any change is released.

Training

All Arena employees and contractors train annually to ensure employee awareness of and compliance with corporate security policies using Arena Solutions Training Management module.

Physical Layer

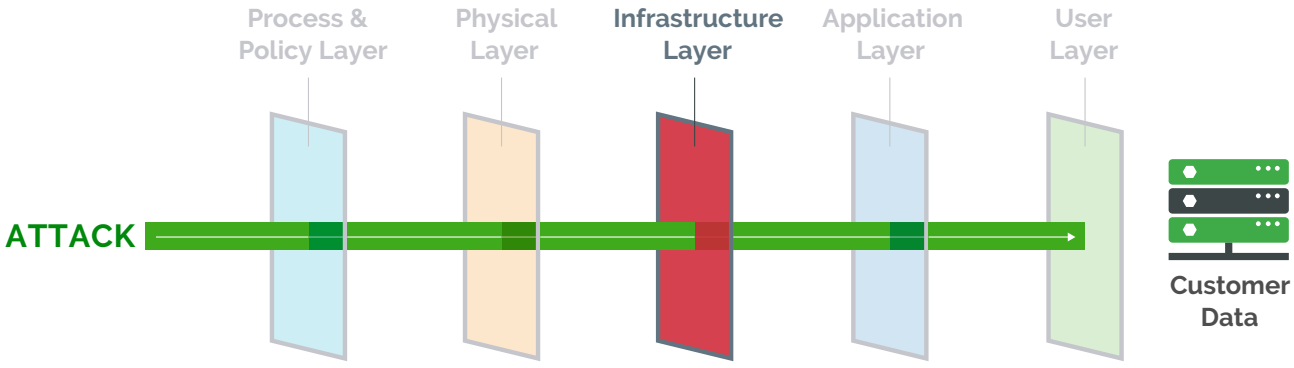
All Arena production equipment is owned and operated by Arena Solutions and is co-located at a world class facility. Our co-location partner maintains 24-hour security at the facility, with all visits logged against customer-defined access lists. Once authorization is confirmed, a cardkey lock allows visitors to access only their own equipment area.



Authorized Access

In addition to restricting personnel from entering the production area, operational access is limited to a restricted set of Arena operations employees. Operational access to the production system is controlled by an isolated, restricted network. Only key, highly trained personnel have access to this network.

Infrastructure Layer



Perimeter Defense: Firewalls

A strong perimeter defense is essential to prevent unauthorized and/or inappropriate system access. Arena secures the perimeters of both production and corporate networks with multiple firewalls. Primary production firewalls are managed by in-house technicians. We employ an independent third party to actively scan all public Arena IP addresses on all production and corporate networks for unauthorized open ports and known protocol vulnerabilities.

A multi-layered firewall operating in a deny-all mode protects all network access to the application and database servers. Internet access is only permitted on explicitly opened ports for a subset of specified hosts. For an additional layer of security, all database servers reside behind an additional firewall.

Operating Systems Security

Arena Solutions enforces tight operating system-level security by using a minimal number of access points to all production servers. For security, all operating systems are maintained at each vendor's recommended patch levels.

Networking

Arena platform servers are allocated to the respective security groups, characterized by specific security settings (TCP/IP level). Separate VLANs are used to split production, testing, and development environments as well as to segregate end-user and administrative traffic. Access to internal production networks require two-factor authentication.

Arena employs a two-tier security model:

- Web servers within the demilitarized zone
- Database servers behind an additional firewall

No Root Access

All customer access to Arena is controlled through user interfaces (UI), application programming interfaces (API), and/or dedicated tools. Use of any of these methods of access require a username and password with privileges appropriate for the requested access.

Customers do not have root or administrative access to any portion of the platform technology stack. Access is permitted only via the Arena application layer (UI or API).

Shutdown All Unnecessary Ports

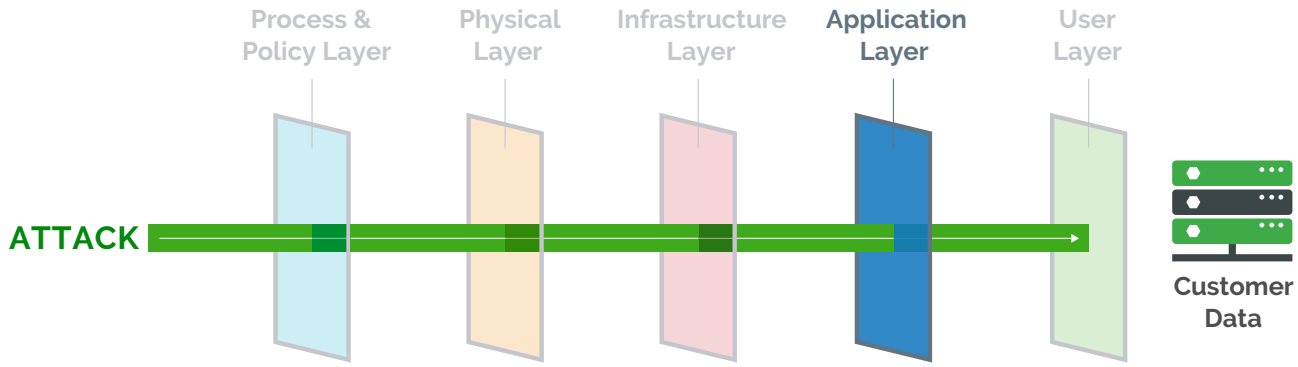
Any ports on any server and/or virtual host not required for the operation of Arena are disabled eliminating additional opportunities for external intrusion.

Security Patches

Arena follows policies and procedures to update all components of the Arena platform, including operating systems, virtual machine (VM) hypervisors, middleware, databases, etc. with their vendors' security patches. These security patch activities are subject to SOC 2 auditing and are subject to rigorous standards.

Application Layer

Arena provides end users with access to product designs and processes. It also integrates with other systems to share this information seamlessly. Arena uses many security measures to enable the secure flow of data from when it is loaded into Arena through the delivery to the workspaces for end-user consumption.



Encryption-in-Transit

Arena leverages the strongest encryption currently supported by browsers allowing users to access data with 256-bit encryption from their browsers. An extended validation (EV) secure sockets layer (SSL) certificate—signed by authentication leader Comodo and bearing the Arena domain name—as well as the lock icon in the user's browser assure customers their data is fully protected while in transit.

Encryption-at-Rest

All files are stored on Arena servers in encrypted form.

Application Access

Customer data may be accessed only through the application layer. Whether this access is through the user interfaces or through the publicly available API, all access is encrypted via SSL/TLS over HTTP. Access through the UI or API enforces user access controls to regulate access to the customer data only to authorized users and personnel. Arena does not provide direct access to any database. This approach prevents unauthorized services or systems from accidentally or maliciously retrieving and/or modifying customer data.

Integration

Integrations use the Arena application programmatic interface (API) over encrypted SSL/TLS HTTP connections. The API follows the user security model, enforcing data retrieval to be subject to the same user authentication and access controls.

Reliability and Backup

Arena stores all customer data on redundant disks for added reliability. To maintain a robust disaster recovery strategy, all customer data is backed up hourly to the last committed transaction to a warm production-capacity disaster recovery site with the same level of physical and infrastructure security described above but in a separate, geographically diverse location as the primary data center. All backups are transferred over an encrypted channel to the disaster recovery data center. To further protect against data loss, archival backups of all customer data are created on a weekly basis and maintained for 26 weeks.

Maintaining Security in the Multitenant Architecture

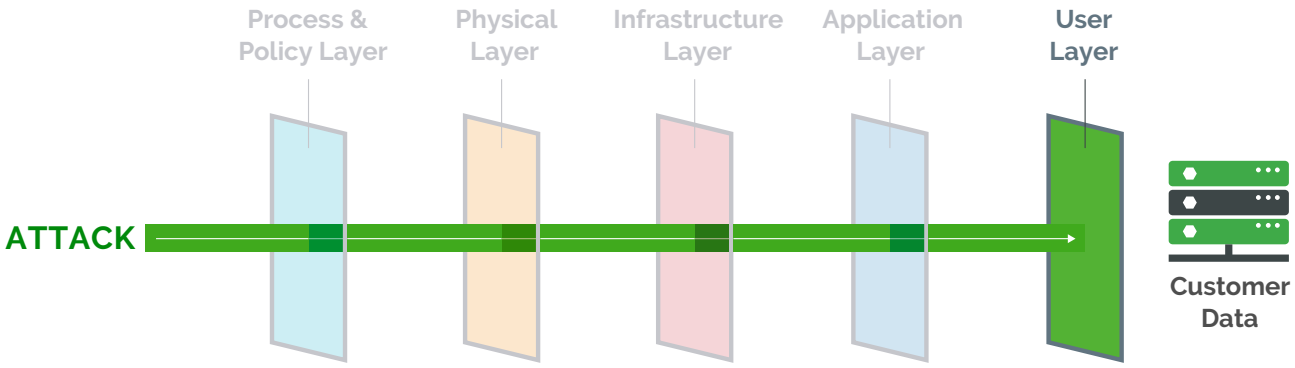
Arena's robust application security model prevents one customer from gaining unauthorized access to another customer's data when accessing Arena's system.

- Arena customer data is isolated into unique and separate workspaces within the application.
- Arena's architecture ensures customers can connect only to one workspace at a time.
- Customers can connect to a workspace only through Arena-provided application methods (e.g., main web client, Arena Exchange, API).

Quality assurance (QA) testing includes test cases to assure data is isolated in multitenancy.

User Layer

User security is enforced with a variety of security measures allowing only authorized users to view and modify a strictly defined set of objects and data, enabling users to have access to the information they need to perform their task. When a user changes product information, the changes are logged in the database.



Authentication

Arena customer data can be accessed only with a valid username and password combination, which are encrypted via TLS 1.2 for Internet transmission (backward compatible with TLS 1.0 and 1.1). Username and password verification are provided by a hardened authentication service that is maintained separately from the main application service.

Passwords

Passwords are stored using a one-way hash algorithm. Arena users can set and use secret security questions to reset passwords.

Two-Factor Authentication (optional)

Arena customers have the option to enable two-factor authentication, which sends a unique code to the user's email address or mobile number when the user logs in from an unknown computer.

SSO

Arena offers single sign on (SSO) as an option for username and password management. SSO enables a customer's information technology (IT) team to manage all employee's usernames and passwords (along with password rules) for multiple independent software systems from a single corporate IT application. SSO allows the same credentials from a directory server to provide authentication for multiple software systems. Arena Solutions has partnered with Ping Identity to integrate Arena's authentication process with Ping Identity PingOne® product to provide part of the required SAML 2.0 compliant SSO workflow. For more details regarding user management tools supported and implementation, please refer to the Cloud SSO for Arena Tech Note.

IP Whitelisting

Arena offers the option for customers to restrict access to Arena workspaces by IP address. Customers can define unique access restrictions for different user groups so that customer administrators can ensure each user accesses the UI only from a trusted client network. This feature includes the capability to monitor and log user attempts to access the workspace from untrusted networks.

User Session Expiration

Once an Arena session has been established, a randomized session ID cookie that does not contain username or password information identifies the user. Ninety minutes of inactivity causes the session to time out, after which a new session must be established to access customer data.

Access Policies

Access Policies let customer administrators define user access to Arena data from top-level worlds and views down to specific data filters including categories and attributes for precise level of access needed for each type of user. Policies utilize user groups defined by the customer (e.g., location, function) and allow for secure and efficient policy management. Out-of-the-box policies provide fast initial configuration with modification and replication.

Conclusion

Arena Solutions is vigilant in protecting customers' data assets. We believe a mature security organization requires coordinated dedication across technologies, policies, procedures, and people. Therefore, Arena adopts a risk-based approach as discussed in this document. This approach provides demonstrated strength at every layer of security, minimizing any potential vulnerability or weakness.

Arena was built on the cloud and for the cloud with governance policies and features designed for the security of our customers—the 1300+ innovative high tech and medical device companies changing the world.