productboard

Security Overview

productboard deploys industry-standard security practices to keep your data safe and secure at all times.

productboard Security Overview

This paper describes the security features of productboard and the operational controls put into place to protect your data.

Security has been integrated into the architecture, policies, and procedures of productboard. In this paper, you will learn about the design, credentials, change management, and other security mechanisms.

This paper covers the following topics:

productboard Security Summary
A high-level overview of productboard's security layers.

productboard Security Certification
Certifications earned by productboard.

Amazon Web Services (AWS) Cloud Security Implementation
An overview of security implementation across multiple layers (physical, virtual infrastructure, software infrastructure security, and more) and application and administrative security features.

Application-Level Security
productboard has implemented features to secure users and operations within the web application.

Data Security
An overview of security features implemented to ensure that your data is safer with productboard.

Organizational Security and Change Management Processes
A description of productboard's operational security practices, including organizational security and change management processes, data backup and disaster recovery, and compliance with industry regulations.

productboard Security Summary

productboard is designed to organize functional and security aspects into a well-defined, multi-tenant model.

productboard provides robust product management capabilities while protecting the privacy and security of your enterprise data. Our service accommodates a large number of customers without requiring a separate instance for each customer. Currently, more than 1,000 companies use productboard.

Application security
Logical security measures and relationships between individual users and projects are configured within the control layer. Users can be authenticated with a combination of an email address and a password or via Google Authentication. A single user can be a member of multiple projects, but data in projects are strictly separated.

Data security
User authentication and authorization on the web API layer verify that a valid identity is attached to each request and is authorized for access to required resources. Input and output are protected by SSL encryption technology, and all data at rest is encrypted for our Scaling plan customers for added security.

Operational security
We maintain industry-standard operational security practices, including organizational security and change management processes, as well as data backup and disaster recovery policies to keep your data protected and available.

productboard Security Certification

productboard participates in relevant industry certifications to provide you a high level of assurance regarding productboard operations, infrastructures, and controls in place.

When it comes to regulatory compliance, productboard knows that its customers often operate within a complex statutory environment that governs the retention and management of customer data. As safe and secure management of data becomes a global issue, productboard keeps up with international security compliance mandates, and continues to monitor and improve compliance with the specific regulatory requirements in customer industries and locales.

productboard participates in and has certified its compliance with the EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield as set forth by the U.S. Department of Commerce and the European Union.

productboard's Amazon data center infrastructure has been accredited under:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

productboard also provides a range of technology tools and measures to assist you in meeting your security requirements. These features include data and transport encryption technologies, data access application program interfaces (APIs), and administrative controls. For data archiving, information managed by the productboard infrastructure can be retrieved by customers using the productboard

AWS Cloud Security

productboard's on-demand platform is built and hosted within Amazon's secure data centers and utilizes the Amazon Web Service (AWS) technology, a scalable, distributed computing infrastructure that is used worldwide to host and manage enterprise applications.

AWS provides a robust suite of security features, which productboard automatically inherits. These features are augmented by specific productboard security features and policies, mostly around securing the application and its data.

Physical Infrastructure
productboard's physical infrastructure is hosted and managed within Amazon's secure data centers and utilize the Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards.

Amazon's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

productboard's infrastructure is located in the U.S. at the AWS US East 1 data center, with the option and flexibility to provision additional infrastructure in the EU, if needed.

Physical Security
AWS's data centers are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors to AWS data centers are required to present identification

and are signed in and continually escorted by authorized staff.

Amazon only provides data center access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical and electronic access to data centers by Amazon employees is logged and audited routinely.
For additional information see: https://aws.amazon.com/security

Network Security
Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, are established on each managed interface, which manage and enforce the flow of traffic. ACL policies are approved by Amazon Information Security. The AWS network provides significant protection against traditional network security issues, and you can implement further protection. The following are a few examples:

- **Distributed Denial Of Service (DDoS) Attacks**. Proprietary DDoS mitigation techniques are used. Additionally, AWS' networks are multi - homed across a number of providers to achieve Internet access diversity.
- **Man in the Middle (MITM) Attacks**. All of the AWS APIs are available via SSLprotected endpoints which provide server authentication. Amazon EC2 AMIs automatically generate new SSH host certificates on first boot and log them to the instance's console.
- **IP Spoofing**. Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.
- **Port Scanning**. Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy. Violations of the AWS Acceptable Use Policy are taken seriously, and every reported violation is investigated. When unauthorized port scanning is detected by AWS, it is stopped and blocked.
- **Packet sniffing by other tenants**. It is not possible for a virtual instance running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance.

Penetration Testing and Vulnerability Assessments
Regular vulnerability scans are performed on the host operating system, web application, and databases in the AWS environment using a variety of tools. Also, AWS Security teams subscribe to news feeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches.

Heroku Data Replication, Backup, and Archiving
productboard utilizes the default Amazon RDS automated backups of our Postgres DB instance. Automated backups are created on a daily basis and stored on encrypted Amazon S3 systems all managed by AWS. We retain daily backups for past 7 days, and we also archive additional backups ad-hoc as needed. We periodically attempt a "restore" from these backups to confirm that the backup process is working as designed as part of our Business Continuity and Disaster Recovery test plan.

Application-Level Security

The productboard service provides a range of application-level security mechanisms that allow you to fine-tune your productboard project to meet specific requirements. Permissions on granular actions are grouped to a variety of user roles.

Security and privacy are enforced at the productboard project level. A project contains user content and users themselves. Users in a project never have access into other projects, unless specifically invited. User roles inside projects are either Admin, Editor, Contributor, or Viewer. productboard is built as a self-service Web 2.0 application, users can administer their own accounts and easily collaborate with the other users within each project.

The following activities are completely self-service in productboard:

- Account registration and activation
- Password reset
- Project creation and administration (admins only)
- Project invitations and sharing (admins only)
- Suspending user access to projects (admins only)
- Selecting which features will be visible to Viewers on the roadmap (admins only)
- Feedback and research creation (all user roles except Viewers)
- Creation and editing of all user content (admins, and editors only)

productboard architecture relies on a centralized authentication and authorization security framework to control access to services. productboard supports sign-in, and Google Authentication for all user roles. For users using email and password sign-in, ownership of the email address has to be confirmed first by clicking on a confirmation link sent in a verification email. The security framework enables the enforcement of security policy by ensuring password strength. We use bcrypt for creating hashes of passwords for storage.

The email address of users using Google Authentication has to match the productboard user account address. Our Startup and Scaling Company plan customers can enforce the usage of Google Authentication in their projects.

OAuth authentication is supported for native integrations with third party services, like Zendesk, and Intercom.

Each productboard project features an email inbox for inbound market insights. The inbox address includes a random token ID to prevent spam.

We utilize Cloudflare's enterprise-class web application firewall (WAF) and Screen.io Security Platform to protect our servers from common vulnerabilities like SQL injection attacks, cross-site scripting, and cross-site forgery requests. Our application employs protections against clickjacking using the X-Frame-Options header. We use Content Security Policy (CSP) header for additional protection against XSS attacks.

productboard employs third-party security experts to perform a penetration test at least once a year. Results of the most-current results from these tests will be provided to paying subscription customers upon request.

A security audit of our dependencies and vulnerability scanning with tools based on static code analysis is a part of our continuous delivery pipeline. Besides that we use Mozilla Observatory, ssllabs.com, and securityheaders.io to scan our server configuration.

For our Scaling plan customers, productboard can be configured to only allow access from specific IP address ranges.

For our Scaling plan customers, productboard can also be configured to only allow access from SAML2.0 enabled identity providers or centralised access management system like OKTA.

Data Security

productboard features active monitoring using situational awareness algorithms and logging. We actively track all sign-in attempts, including failed attempts and attempts to access revoked resources and promptly respond to anomalies and outliers identified in our monitoring.

Strict process separation (sealed) is a built-in design feature of all productboard software development and operational lifecycles. The deployed multi-tenant security patterns provide effective isolation and sealing of data and metadata, even while sharing the same physical storage grids.

Data transport and, for subscribers who purchase the Scaling plan, storage (encryption at rest), are protected using industry standard methods of encryption (SSL/TLS, strong symmetric-key cryptography). We use HTTP Strict Transport Security (HSTS) security policy mechanism to protect against protocol downgrade attacks and cookie hijacking. Our servers offer forward secrecy using ECDHE ciphers for clients that support it.

productboard API is SSL-only and you must be a verified user to make API requests. You can authorize against the API using your username and password, or using Google Authentication. We utilize cookies for storing temporary authentication tokens for subsequent API requests. All cookies use the Secure flag and all session cookies use the HttpOnly flag. We require CSRF tokens to be present for all POST, PATCH, PUT or DELETE request to prevent Cross-Site Request Forgery.

If a customer chooses to end its relationship with productboard, productboard maintains its backups and archives for a period of time. Customers may request complete and permanent deletion of their data by contacting productboard Support. The unit on which data destruction is applied is an entire project.

We have detailed access and activity logging for our admin CLI interface our developers use when accessing production data to resolve an incident. Every command is recorded and logged. This log is reviewed by our CTO every 14 days.

Organizational Security and Change Management Processes

With productboard, secure operations extend beyond putting the right systems and technologies in place. Our effective security infrastructure is also embedded into our organizational culture and everyday business processes.

productboard has deployed several layers of operational security to eliminate the risks associated with human activities. All employees with access to customer data are subject to a periodic criminal background check. productboard policy is to provide system access only to appropriately trained staff, who require a specific level of access to perform authorized tasks. Internal systems enforce unique user IDs and strong passwords and limit password reuse. To manage access, productboard relies on industry-standard security systems and standards including two-factor authentication and RSA.

Physical Security and Logical Access
There is physical security that requires individuals to show badges and input access codes at all company buildings, and only authorized users can gain access to servers, logs, customer information, and system configuration information.

Logical access to the production environment by productboard employees is limited to the core operational personnel only. All access keys are stored within an encrypted credentials vault. Access requests, grants, and revocations are periodically reviewed. And all changes to access rights are based on roles and job responsibilities. The approval process maintains audit records of all changes.

productboard's internal office network is protected by firewalls, best-in-class router technology, secure HTTPS transport over public networks, and regular audits.

Employee computers are password protected and the default configuration for such devices causes the devices to be automatically locked after maximum 10 minutes of inactivity. All employee computers are installed with strong file system encryption. Employees are provided with a tool to backup/sync company data to either a physical local location or to cloud storage. Each employee receives a laptop computer with an assigned unique company asset tag for identification. productboard employees are required to contact IT in an event of laptop theft or loss.

Secure Development and Change Management

At productboard, software development is a two-phase process. First, the discovery phase focuses on understanding of customers' needs and validation of solution approaches. After a feature has been successfully vetted during the discovery phase, it is signed-off by Product Management, and DevOps. It then enters the Delivery phase, which includes another round of testing, and a thorough security review before it is deployed to production. Testing and staging environments are separated physically and logically from the production environment. No actual customer data is used in the development or test environments.

Throughout the Delivery phase, all source code and other artifacts that are part of the product are subject to version control and are managed in centralized version repositories. When code for a feature has been completed, the new code artifacts need to pass multiple quality controls, and are extensively manually tested in separate branches, before they are allowed into the main product code base. The main product branch is then subject to continuous integration (automated testing) so that any regressions not captured by the other quality controls are discovered and corrected as soon as possible. The continuous integration process includes the full cycle product build, packaging, and deployment in order to simulate the actual production deployment as closely as possible.

The development cycle for larger features and product components includes further testing behind a feature flag. All tests have their own written record of passed and failed test cases linked to the defect.
Functionality that passes all acceptance criteria is subsequently scheduled for a full production release. If the result of the test upgrade passes all of the prescribed tests and validations routines, the release is subsequently applied to the production environment. A deployment plan and a deployment log are kept for each production deployment separately for both frontend and backend.

Monitoring

productboard then proactively monitors the platform for security incidents, including alert notifications generated by productboard systems, alerts generated by Heroku, and Amazon, open source and industry alerts, and community alerts. State-of-the art tooling is put in place to automatically notify and escalate any incidents to the security team. The team is on call 24/7, 365 days a year, and all employees are trained on security incident response processes, including communication channels and escalation paths.

When an alert is raised, the risk level is assessed first. Based on this assessment, the prescribed response process is chosen and launched. Documented escalation procedures and communication protocols clarify when and how an escalation takes place, and who is notified. Users of our service will be notified of any security breach involving their data as soon as practicable following when we become aware of the breach.

Reporting Vulnerabilities

productboard welcomes security reports on vulnerabilities from outside security researchers. Security researchers can submit their reports by contacting productboard support at security@productboard.com or support@productboard.com.

Privacy

productboard maintains a strong privacy policy https://legal.productboard.com/privacy_policy, to protect customer data. productboard is obligated to protect access to customer information while also abiding by the law. Information can only be obtained from productboard through a valid legal process, such as a search warrant, court order, or subpoena. If legally permitted, productboard notifies the organization whose information is being sought.

Employee Vetting and Training

productboard hiring practices ensure that all staff are qualified for their functional responsibilities and hold appropriate certifications or accreditation, if required. At a minimum, these practices include verification of the individual's education and previous employment, as well as a reference check. Based on the statutory environment and the employee's position, additional background checks may be performed. All new hires are screened through the hiring process and required to sign Non-Disclosure and Confidentiality agreements.

The employee on-boarding process includes a mandatory security orientation session during which new employees are instructed about security policies and procedures. At least annually, engineers participate in secure code training. This training covers OWASP Top 10 security flaws, common attack vectors, and productboard security controls. We utilize Ruby on Rails framework security controls to limit exposure to OWASP Top 10 security flaws. These include inherent controls that reduce our exposure to Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), and SQL Injection (SQLi), among others.

productboard uses commercially reasonable efforts to make productboard service available 24 hours a day, 7 days a week. productboard has a clearly documented disaster recovery plan to ensure availability of the service in case of a disaster.

Evolution of our Security

Security is a dynamic field, therefore productboard regularly reviews and updates the technologies, policies, and programs described in this document based on changes in our products, emerging threats, and industry standards. For more information please contact us as at security@productboard.com or support@productboard.com.

Conclusion

To ensure effective information security, productboard has implemented the organizational, procedural, and technical protection measures demanded of a leading-edge enterprise solution.

productboard is hosted on AWS Amazon. A provider that is consistently rated among the top-line service providers. The base security features offered by AWS Amazon are augmented by applying select technologies, such as data encryption, platform monitoring, as well as policies for change and incident management.

Additionally, wherever possible, the productboard security model is designed to be open and pluggable to accommodate customer-specific requirements, such as third-party authentication, user account management, or primary storage encryption.

productboard has designed the service to ensure the security of its customer's data. By partnering with AWS Amazon, productboard leverages cutting-edge physical and virtual infrastructure, and software and infrastructure security. productboard also ensures security at both the application and data levels, and has implemented rigorous change-management processes as a critical part of its security profile.