ioXt alliance

Pledge Booklet

The Global Standard for IoT Security®

The Global Standard for IoT Security®

ioXt Alliance, the global standard for IoT security, is a group of manufacturers, industry alliances and government organizations dedicated to harmonizing best security practices and establishing testable standards that give retailers and consumers product confidence in a highly connected world.

Table of Contents

Executive Summary

With all our digital devices, chosen and unchosen, connected to the internet as part of daily life, we have convenience, speed and flexibility like never before. And it just keeps evolving.

How do we as industry guide manufacturers and service providers with best design practices so that the result is a more stable and secure national and global landscape?

But in this still fairly new age of connectivity, there's also a healthy amount of well-founded fear. Consumers wonder if their devices bleed data and betray privacy. Manufacturers wonder what liability they may face for selling insecure products.

The exponential growth of the Internet of Things (IoT) compounds the threats to our cybersecurity on a daily basis. How can manufacturers protect consumers from the real threat of hackers and how can consumers know they're safe? How do we as industry guide manufacturers and service providers with best design practices so that the result is a more stable and secure national and global landscape?

The answer lies in the ioXt Security Pledge. It's a direct result of "big tech" working together as the ioXt Alliance to set security standards that bring security, upgradability and transparency to the market and directly into the hands of consumers.

Welcome to the solution for the fear, worry and need to get security right—and to make it easy. It's courtesy of ioXt, the global standard for IoT security.

Introduction

With so much connectivity today—over 30 billion devices as of this writing—and ever more tomorrow, it's never been more important to get serious about cybersecurity. Too many data breaches, hacks and attacks have occurred to think otherwise.

Device upgradability and transparency between manufacturer and consumer is likewise critical. With things like motion sensors in the home controlling lighting, the HVAC and security systems and even the sleep mode for the office printer, consumers need to know their devices will receive the latest updates and for how long.

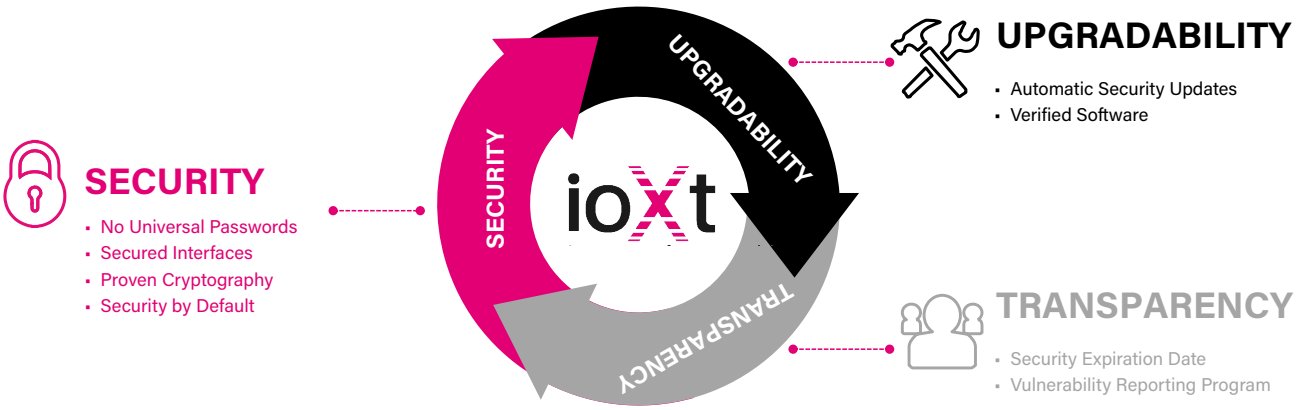
The solution is to start at the beginning—to build security into Internet of Things (IoT) products. By identifying and clearly defining best practices, supporting the implementation of those best practices and establishing consistency in labeling of products and services, we can create consistency and compliance across industries and protect consumers.

The ioXt Security Pledge is the foundation for making this happen. It removes any guesswork from creating secure-by-design products and establishes a way to identify all products and services that comply with ioXt Pledge standards in the marketplace.

By ensuring device security, upgradability and transparency, the Pledge assures retailers they're offering safe products and assures consumers they're making an intelligent (not just a "smart") buy.

As industry coming together to provide a framework for securing products and for certifying those that make the grade, we at the ioXt Alliance are proud of forging a path to cybersecurity that is much needed and long overdue.

ioXt Security Pledge



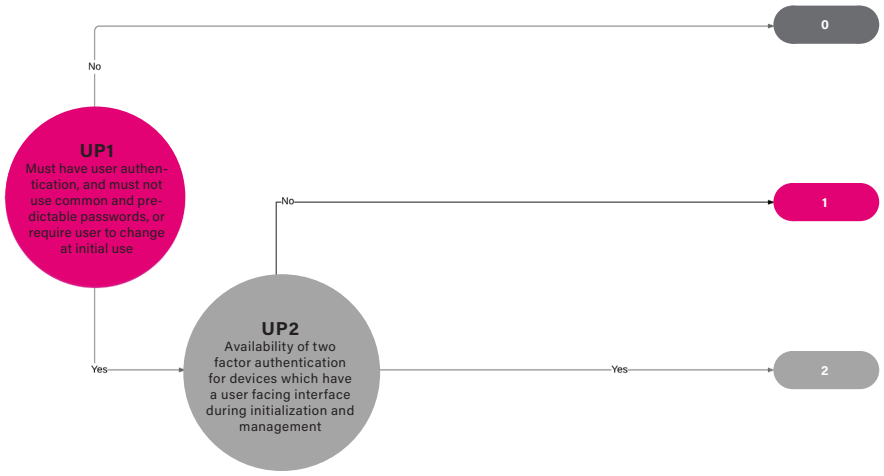
The ioXt Security Pledge is composed of eight clear principles:

1. No Universal Passwords
2. Secured Interfaces
3. Proven Cryptography
4. Security by Default
5. Signed Software Updates
6. Automatically Applied Updates
7. Vulnerability Reporting Program
8. Security Expiration Date

The rest of this booklet further describes each of the Pledge principles and how they are included in the design and manufacturing of consumer products.

No Universal Passwords

The product shall not have a universal password; unique security credentials will be required for operation.



Must have user authentication, and must not use command and predictable passwords or require user to change at initial use

All connected devices must authenticate the user prior to use. One common method is to have the user enter a password. The core issue for every designer is deciding what the initial password should be when a device ship from the factory. Many companies have picked well-known and easy-to-remember passwords. The problem is this practice allows for widescale attacks as many consumers never change the default password.

The ioXt Alliance requires that all devices have a password. This password must either be unique to the device or require the user to change the password prior to initial use. A unique password must not be predictable. For example, a password consisting of a common phrase plus the serial number would not be allowed.

At this time, the Alliance does not require specific password lengths or validation against known password lists. It is highly recommended that the manufacturer follows the password best practices as defined by NIST and other organizations.

Availability of two-factor authentication for devices that have a user-facing interface during initialization and management

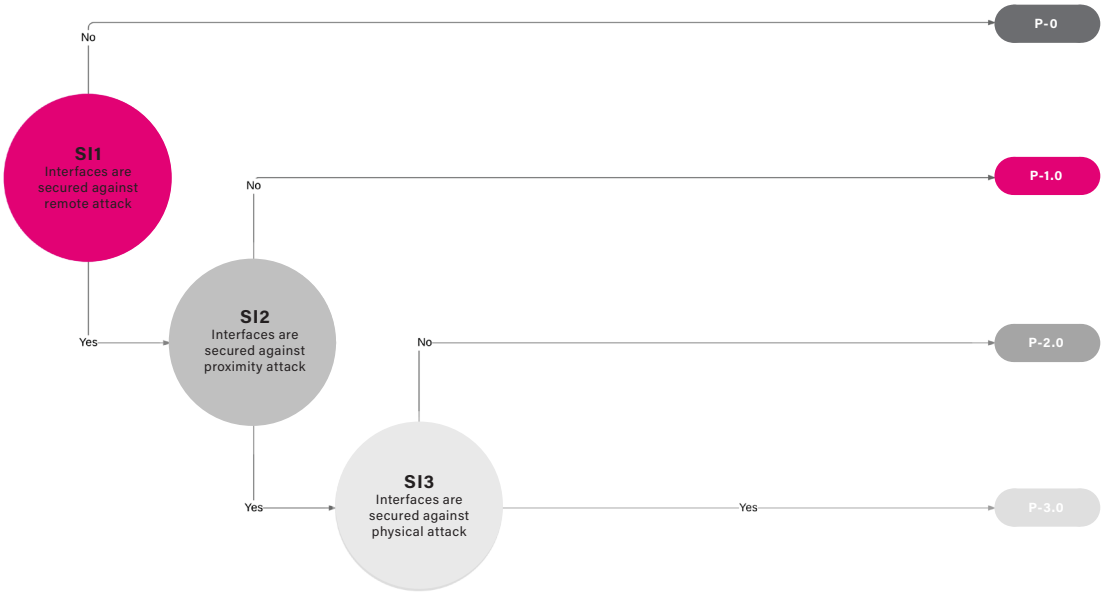
A higher level of authentication can be achieved through two-factor authentication. A common method of two-factor authentication is for a user to enter a password, followed by a pin code which is sent from the service to the user through a communication channel other than the device. However, two-factor authentication can be achieved through the combination of a multitude means of authentication, such as a user password, fingerprint, face ID, iris scan, ID chip, pin code from a text/email message, Bluetooth beacon, key fob, etc. The ioXt Alliance requires the use of two-factor authentication during device initialization. This phase of a device's life is critical, as the initial trust relationship between the device/service is being tied to the user/administrator of the service. Often, an attacker will attempt to reinitialize the device to add themselves as the administrator or transfer the credential ownership of the device.

Equally important, two-factor authentication must be used during management operations. Management is defined as management of the security material in the device. For example, the modification of user accounts associated with the account must require two-factor authentication. However, there are many other device-specific management features which must be protected. For example, a WiFi camera may support streaming to multiple IP addresses (phone and DVR). An attacker may wish to change the DVR address. Though an address may appear to be an operational item, it can have serious privacy impacts if maliciously changed.

The ioXt Alliance highly recommends the use of multiple account levels, in which configuration features are assigned to either the user or administrator level. All administrator functions should require two-factor authentication.

Secured Interfaces

All product interfaces shall be appropriately secured by the manufacturer.



Interfaces are secured against remote attacks

All devices must be protected from large scale remote attacks. For devices which use IP protocols, the network should not be trusted. Further, it should not be assumed that a firewall is present. The number of network connections should be kept at a minimum, strong authentication should be used and key lifetimes should be managed. If a device requires a gateway to connect to the internet, and the gateway truly terminates the sessions between the LAN and WAN, then the device may assume the network is protected from remote attacks. However, the device may still need to protect against proximity and local attacks. Typically, remote attacks are focused on logical interfaces.

Interfaces are secured against remote attacks

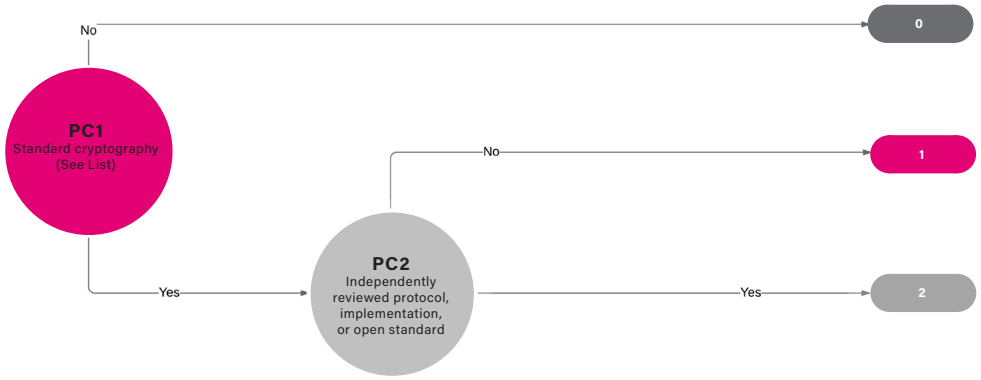
In general, a proximity attack requires the attacker to be near the device but not have possession of the attack. A typical example is an RF-based attack by an attacker located just outside the consumer's home. However, a local network attack would also be considered a proximity attack—like when a remote attacker takes control of a consumer's computer and then uses the computer to attack a printer on the network. The computer in this example fell victim to a remote attack, while the printer was under a proximity attack.

Interfaces are secured against physical attacks

Physical attacks are any type of attack in which the attacker has unlimited possession of the device. The attacker may attempt all remote and proximity attacks. However, the attacker may also disassemble the device and probe the circuit board. For consumer electronics, industry-recognized secured processors and secure elements are considered secure against local attack. However, unsecure processors are not considered secure against local attack. Further, power analysis side channel attacks are in scope, along with JTAG and debug port attacks. Attacks in which security material is extracted from a device but cannot be used to attack another device are out of scope.

Proven Cryptography

Product security shall use strong, proven, updatable cryptography using open, peer-reviewed methods and algorithms.



Standard Cryptography

Cryptography is a complex art that requires specialized mathematical skill and training. There is a great deal of subtlety involved in both designing and implementing cryptographic algorithms. The mere order of cryptographic operations can leak secret information to attackers. For many reasons, device manufacturers must use industry or government recognized standards-based algorithms and libraries.

Independently reviewed protocol or implementation

The final protocol used for communications may include multiple cryptographic primitives, replay protection, key exchange and rotation mechanisms, user and device authentication, access control and many other items. Therefore, it is highly recommended to use standards-based protocols—those which many organizations have collaborated on and reviewed—whenever possible. However, there may be instances where this is not suitable, such as for market or business requirements. If a proprietary protocol must be used, it is critical that the protocol be independently reviewed. This review should be conducted by a security researcher who have the appropriate experience and independence from the product line to give an unbiased opinion of risk.

Secured by Default

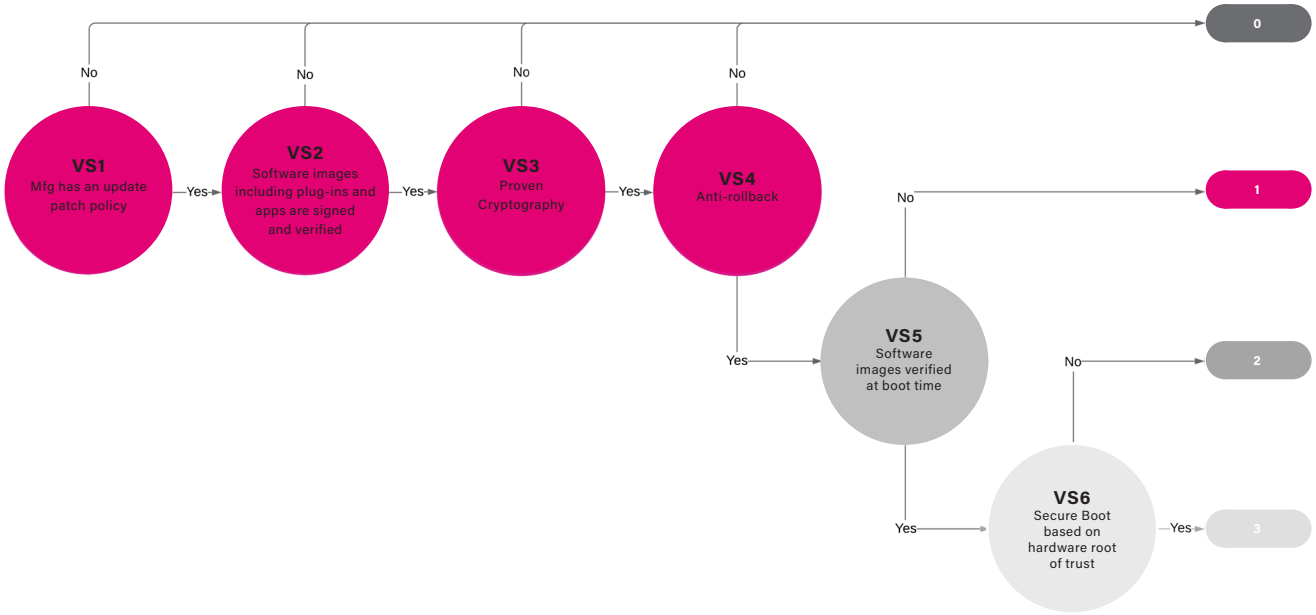
Product security shall be appropriately enabled by default by the manufacturer.

Base security requirements for the profile that the device is being certified under has been met

Security by default is highly dependent on the eye of the beholder. For example, some phones do not allow applications to be loaded outside of the curated store. If a user wishes, they can go into the security settings and disable third-party application protection. In enterprise applications, the administrator is allowed full rights, while the user has very limited rights. To address these market complexities, the Security by Default pledge item shall be defined by the certification for which the device is being tested.

Signed Software Updates

The product shall only support signed software updates.



Manufacturer has an update patch policy

Because software is not static, every device must have a means to be updated. The manufacturer shall have a clear policy in which they inform the consumer how they will support software updates. Ideally, this policy should follow the same guidelines as the security expiration date pledge item. However, this requirement describes the entire firmware image for the device and any other manufacturer-supplied libraries. The primary goal of this requirement is to inform the consumer that the devices are capable of being updated, and the manufacturer will provide updates whenever new vulnerabilities are discovered.

Signed update images

All firmware images must be signed such that an attacker may not modify the image and inject malicious code into the device. The signature may be based on either a symmetric or asymmetric key. Highly asymmetric keys reduce the potential loss of the signing key through a local attack of the device. Further, some means to limit the scope of the signing key should be made. The firmware images must include the device firmware, operating system and any manufacturer-supplied plug-ins or applications.

Proven cryptography

All cryptography used to sign the image must be held to the base level of the proven cryptography pledge item. Proprietary means of signing and validating firmware images introduces significant risk.

Anti-rollback

Once an image has been deployed, the device shall not be allowed to roll back to a previous version. Otherwise, an attacker with an exploit on a previous version simply has to roll back to the known bad version and then execute the attack. If a company must re-release a previous version to address a defect introduced in the upgrade, they may simply update the version number and redeploy the previous version. However, the device shall not accept previous version numbers.

Many companies perform a staged rollout of new firmware updates, and thus a subset of the overall deployed devices may be considered as "lab" devices—which are exempt from this requirement. Further, this requirement is only for devices in the normal operating state. If a device fails to update, and stays at the previous version, it would not be considered a violation of this requirement.

Software images verified at boot time

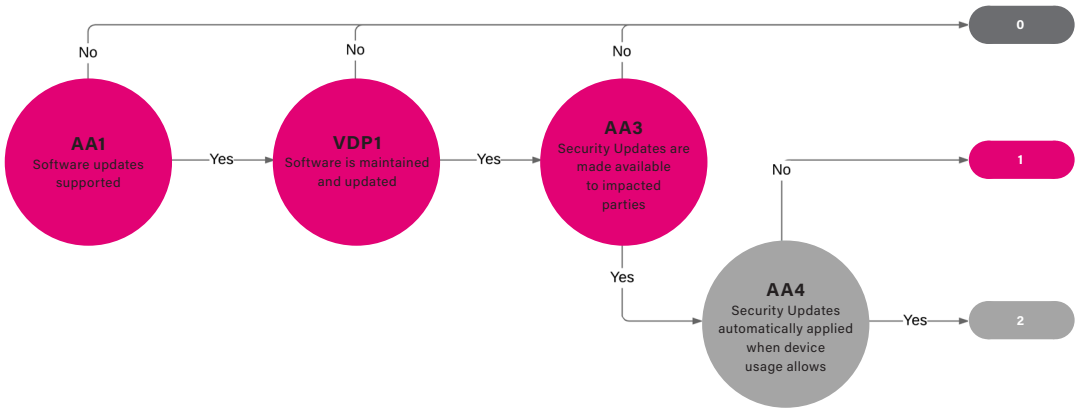
All software images should be verified at boot time. But not all devices have secure boot hardware. Software-verified boot does provide significant improvements in reliability and security. This requirement shall only cover the firmware and software provided by the device manufacturer and is not required to cover third-party modules or user-added programs.

Secure boot based on hardware root of trust

The only sure way to trust the code running on a device is to build all security on a hardware root of trust. The hardware root of trust must be appropriate for the market in which the device is intended to operate. For consumer equipment, secured processors or secure elements must be used with at least the initial unique key stored in the processor or secure element. Security features in the process (or secure element) shall be used to prevent the main application from executing if the image has not been validated. Further, the hardware-based security features of the processor or secure element should be immune to side channel attacks. Currently, the ioXt Alliance does not have strict guidelines around the secure processor hardware.

Automatically Applied Updates

The manufacturer shall act quickly to apply timely security updates.



Software Updates Supported

Connected devices must be updatable. With an ever-increasing reliance on third-party software packages, and device complexity, there will be an issue which must be addressed in devices that have been deployed.

Device updates can be accomplished in many ways, each of which optimize device cost, usability and/or reliability. In an ideal world, the device would have enough memory to store both the current version and the update image. The device would communicate with the device management cloud service at a regular interval, retrieve any updates, apply the update and report back to the management cloud service when the update has been completed.

However, not all devices have the memory, connectivity or ability to support the cost of performing these tasks in a secure manner. For example, medical devices may support this requirement through a process whereby devices which must be updated will be replaced by the manufacturer. Though the deployment time would be based on the postal service, this requirement would still be met.

Software is maintained and updated

It is critical that device manufacturers maintain and update their software whenever new vulnerabilities are identified through vulnerability disclosure programs, security notices from third-parties, or national vulnerability databases. Further, third-party libraries and operating system updates should be applied soon after they are released. A device which can be updated without the manufacturer providing updates does not meet the ioXt Alliance baseline security requirements.

Security updates are made available to impacted parties

Devices may be deployed directly to consumers or into managed ecosystems. In a managed ecosystem, the ecosystem operator will typically require operator validation. Further, the operator will typically manage the deployment of the updated device. For devices which are sold directly to the consumer, the manufacturer is responsible for the security update, validation and deployment. Thus, the "impacted parties" for this requirement may be either the ecosystem operator or the consumer; however, the updates must be made available.

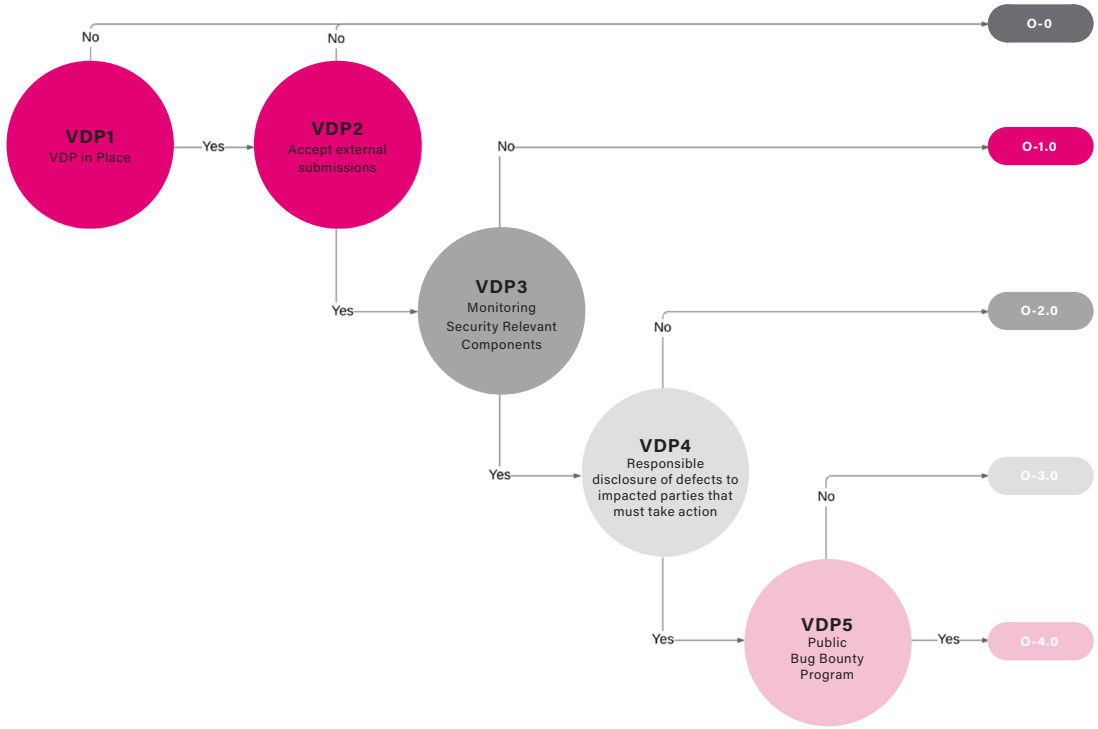
Security updates automatically applied when device usage allows

The consumer should not be required to search for updates or be in the decision loop as to when to apply the update. Many device manufacturers may choose to fix other defects in the same image. However, only security updates are required to be automatically applied to meet this requirement. In some deployments, only critical security updates may be automatically applied, as device connectivity bandwidth or cost may be prohibitive.

Many devices may have operational or regulatory reasons to delay the security update. However, once the device has entered into an acceptable state, the update must be applied. Further, managed ecosystems or corporate policies may prevent the device manufacturer from issuing the automatic update. In this case, the operator of the network shall be responsible to automatically push the security update based on the deployment policies. For example, the updates may be deployed and tested in a phased manner to prevent the entire user base from being negatively impacted if the update fails.

Vulnerability Reporting Program (VDP)

The manufacturer shall implement a vulnerability reporting program, which will be addressed in a timely manner.



A fully compliant vulnerability reporting program should listen to researchers, monitor security components, inform impacted parties and motivate researchers to disclose vulnerabilities to the manufacturer.

Have VDP in place and accept external submissions

All companies must have a means to accept and track defects in their products and services. Security vulnerabilities are just another type of defect. However, a company should not limit the submission of vulnerabilities to internal employees but should engage the researcher community. Most researchers want to improve the general security of devices connected to the network. The researchers will publish their results with or without the company's approval. Thus, not engaging with the researcher will not stop the release of the vulnerability but does greatly reduce the ability to address the issue before potential bad actors are informed of the issue.

At a minimum, all companies should have an email of security@company.com. Further, the company must monitor the email and respond in a reasonable amount of time. See ISO 29147 for further information on running a vulnerability disclosure program.

For this requirement, the manufacturer needs only a means to accept external submissions from researchers. To achieve level 1, a company does not need to disclose the defects outside of the company.

Monitor security relevant components

A company should monitor their security components for vulnerabilities. The secure components may be software libraries from third parties or open source projects. However, the components may be hardware modules or devices which also include security libraries or hardware accelerators. A company should maintain both a hardware bill of material, along with a software bill of material. Any contract with a third party that supplies security components should include a notification of vulnerabilities clause. At a minimum, the manufacturer shall monitor vulnerability databases such as the Common Vulnerabilities and Exposures (CVE) maintained by MITRE or the National Vulnerability Database (NVD) maintained by NIST.

Responsible disclosure of defects to impacted parties which must take action

Listening to researchers and monitoring security components are important in identifying vulnerabilities in the product. However, it is equally important to inform impacted parties of the vulnerability and provide information as to what action they should take. Often, providing a security solution takes time to develop and deploy, but actions to limit the exposure can also be prescribed.

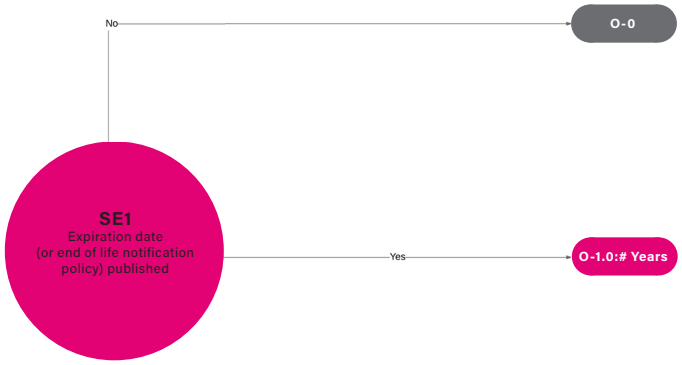
Many devices and components are sold to other businesses or into managed networks. For those situations, the impacted parties are typically well known. Further, there may be contractual requirements around disclosures to allow for the operator of the network to communicate with their customers. The ioXt Alliance recognizes both the direct-to-consumer and the business-to-business operating models. Thus, the impacted parties are those parties that need to take action and may not always be the end consumer.

Public bug reward program

The best way to motivate a researcher is to reward them for their effort. Further, there should not be a limit to who is allowed to participate in the program. Thus, the program must include rewards that anyone can earn and that fall within the regulatory framework in which the company operates. The public bug reward program may be outsourced to another company that has the means to engage with the research community, mediate disputes and process payment. While the ioXt Alliance recommends the rewards be competitive in the marketplace, it does not have firm requirements around the bounty.

Security Expiration Date

The manufacturer shall be transparent about the period of time that security updates will be provided.



Expiration date (or end-of-life notification policy published) (Level 1)

Consumers or channel managers must know how long a device manufacturer will support the security of the device. This is accomplished with either a minimum-security expiration date or an end-of-life notification policy. The explicit minimum expiration date is clearest to the buyer of the product. However, many companies may choose to support a device beyond the initial date printed on the packaging. Regardless, consumers may perceive the date on the package as an actual expiration date and prematurely dispose of the device.

An end-of-life notification policy is another method in which support periods can be passed to the consumer. For example, one manufacturer may state the device is supported for two years from the date of purchase. Another manufacturer may state they will provide at least two years notice before discontinuing support. In either case, the consumer has a clear understanding of the length of time the device's security will be maintained.

This requirement does not imply that the device will not be operable beyond the date at which the security updates have been terminated. Though it is not advisable to use a device beyond the supported security update period, many markets may require continued device operation.

ioXt Alliance Profile

A profile defines the security requirements for a specific set of products or services. A profile contains three components: a definition of which devices may be certified under the profile, a threat analysis for the device or service, and the test plan. The test plan is based on the ioXt Alliance Pledge and draws from the common set of test cases defining the different levels for each pledge item. When a device passes all test cases in the profile's test plan, then the manufacturer may use the ioXt compliance mark on their product.

The goal of the profile is to provide a single stamp to the end consumer which indicates that the product security has been met for the use of the device. A profile provides a means for different devices to be held to different security levels, yet all compliant products would receive a single ioXt certification mark.

ioXt Certification Program

The ioXt Alliance created the ioXt Certification Program to provide a common method for the assessment and rating of a product's (and organization's) fulfillment of the ioXt Security Pledge. For each of the eight Pledge principles, rating levels serve as clear guidelines for quantifying the appropriate level of security needed for the channel or use of the product.

A manufacturer may certify their products with a third-party test lab or manufacturer certification method. The third-party test labs provide a means for independent researchers to validate the device's security against the ioXt Pledge. The bonded manufacturer certification method is a means in which the manufacturer states the security of their device against the ioXt Pledge, and then offers a reward to any researchers who find mistakes in the statement.

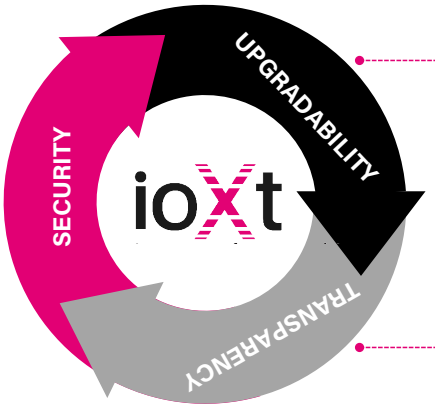
A manufacturer is encouraged to register every version of firmware with the ioXt Alliance such that security researchers can continuously evaluate the security of the device and provide feedback when issues are found. The manufacturer may use a mix of lab and/or bonded certification methods.

Because security never stands still, the ioXt compliance program is a continuous and living process in which threats are continuously evaluated, and manufacturers are informed about them, before they can impact the entire IoT ecosystem.

For more information, please visit ioXtAlliance.org

SECURITY

- No Universal Passwords
- Secured Interfaces
- Proven Cryptography
- Security by Default



UPGRADABILITY

- Automatic Security Updates
- Verified Software

TRANSPARENCY

- Security Expiration Date
- Vulnerability Reporting Program

ioXt alliance