electric imp™

ImpSecure™

Managed silicon-to-cloud IoT security

"Security is only as good as your weakest link" is especially true in commercial and industrial IoT security.

In most traditional IoT approaches, disparate components from different vendors need to be integrated, tested, and maintained for years, protecting against yet unknown threats. It becomes particularly difficult when viewed from the edge -- which could be a single sensor or a gateway of multiple points -- as data and controls are processed and integrated on through the cloud.

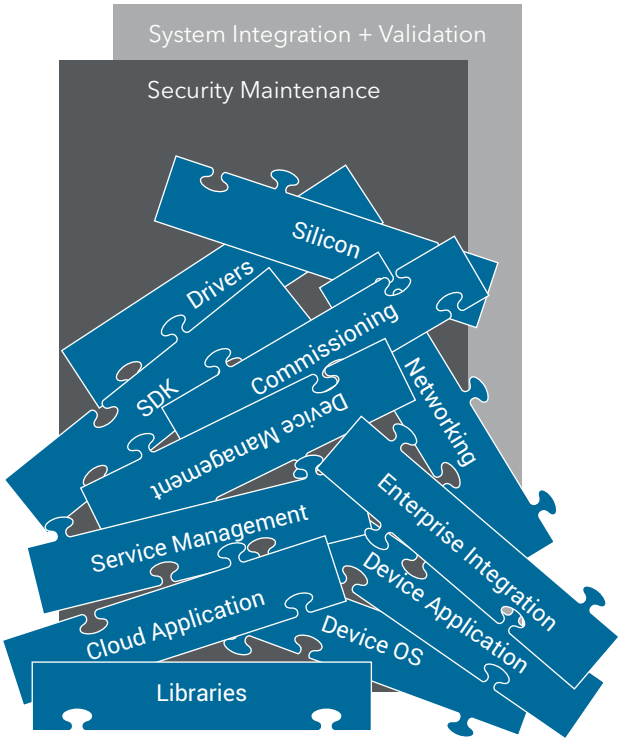
Electric Imp ImpSecure Managed Security is a security-first design. Our impSecure combines a comprehensive set of security frameworks, patented components, capabilities, & managed services integrated into the Electric Imp Connectivity Platform.

ImpSecure delivers multi-level defense-in-depth, silicon-to-cloud security technologies and managed services for constant resilience against security breaches and threats unique to complex commercial and industrial IoT.

Traditional IoT Security vs impSecure Managed Security

Traditional IoT Approach

Complex multi-vendor integration

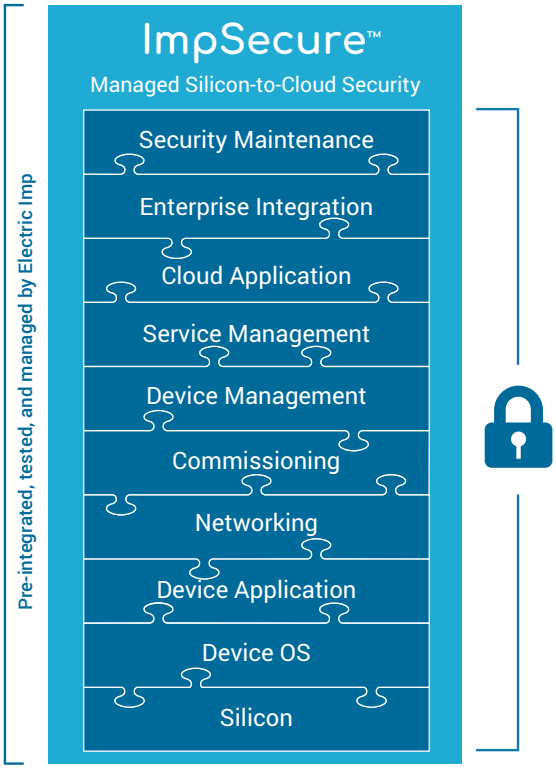


Unproven: likelihood of gaps and weak links

Electric Imp

ImpSecure™ Architecture

All components designed, integrated, and managed together



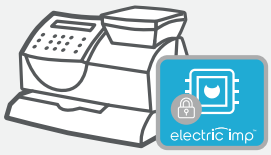
Certified secure silicon-to-cloud: no gaps, no weak links

To schedule a briefing email us at sales@electricimp.com

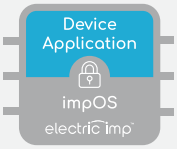
© Electric Imp 2018

The **ImpSecure Managed Security** tightly integrates edge device software and security functionality with Electric Imp's cloud-based managed services to deliver industry-leading, out-of-the-box silicon-to-cloud security, from POC to EOL. ImpSecure encompasses 7 different layers in one fully integrated offering:

01 Edge Device with Secure Silicon



02 Managed impOS and Isolated Application

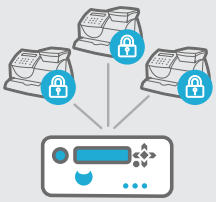


03 Secure Communication via Managed Tunnel

04 Protected Public & Private Cloud

05 Secure Cloud & Application Integration

06 Trusted Manufacturing



07 Full Lifecycle Managed Services

Tested & Approved

As insiders and inadvertent actors are responsible for up to 60 percent of IoT security attacks* to date, it's important that the underlying IoT security platform protects product teams from creating security vulnerabilities during product development, support or operation. ImpSecure provides a robust barrier against not only external malicious attempts but also against user errors and misconfigurations which could result in insecure operations.

ImpSecure has been audited, tested, and approved by security-conscious customers, such as Pitney Bowes and General Electric, and is proven for scalable, demanding IoT solutions act more than 100 customers around the world.

WORLD'S FIRST IOT PLATFORM

UL® 2900-2-2 Certified

1. Edge Device Security

Security starts at the device hardware. Each customer's IoT edge device is built around imp-authorized silicon modules, which have been co-designed by Electric Imp, and are uniquely provisioned by Electric Imp servers during their production process. These modules are cost efficient and highly integrated with an application processor, network interfaces, security features embedded in the silicon, and the integrated system software, impOS™.

Each device runs the customer's application in a tiny virtual machine (VM) sandbox, thus assuring maximum security and portability.
All critical software and security aspects of the edge device are monitored and managed by an Electric Imp-run cloud, either shared (public cloud) or for a single tenant (private cloud), enabling both the edge device application as well as system software and keys to be updated independently & at any time.

Edge Device Security feature short-list

- HSM-protected signing keys
- Secure boot
- Debug interfaces disabled
- Processing is module-internal — no external snooping
- Unique per-device keys
- AES-GCM+AEAD encryption
- Application sandbox
- Protection against unauthorized code execution

2. Data Protection

It should be self-evident that data privacy, integrity, and confidentiality are critical to any IoT solution. **ImpSecure** protects data throughout the platform, from the device into the cloud, with multi-level authentication and authorization of all parts of the system (devices, applications, and users), reliable transmission and processing of data, and advanced encryption from the silicon through to the cloud application.

Data Protection feature short-list

- All off-module storage is encrypted
- Data in transit is encrypted from silicon to application endpoint in cloud
- Authorized data access only, programmatic integrity checks and data resilience
- Electric Imp cloud does not store or introspect data

3. Trusted Commissioning

Device commissioning consists of three core phases: device manufacturing, device provisioning, and device activation (enrollment). All three phases must be implemented reliably and at scale to ensure a successful and secure IoT deployment. Electric Imp does all three starting with **ImpFactory**™ connected manufacturing process to ensure reliable, trackable, and highly scalable production of IoT devices (even in insecure factories). Device provisioning and activation uses patented **BlinkUp**™ to transmit provisioning information to devices and kicks off the activation and enrollment process in a simple and secure fashion. All software commissioning to devices is performed in a secure, scalable, and fail-safe manner.

Trusted Commissioning feature short-list

- ImpFactory device manufacturing without IP exposure
- BlinkUp optical provisioning, device activation/enrollment via replay-proof challenge-response
- Securely managed in-field updates of impOS, applications, and secrets

4. Secure Communications and Networking

ImpSecure assumes all networks are insecure and implements a managed, secure IP-based tunnel between the edge device and the **ImpCloud**™ on top of the existing communications network. This network tunnel uses mutually authenticated industrial-grade TLS 1.2 encrypted links and advanced security features, as well as the ability to update all security aspects in the field to address possible future (and yet unknown) vulnerabilities.

Networks supported include WiFi, Ethernet, and Cellular (early 2017).

Secure Networking feature short-list

- Communications management
- Industrial-grade TLS 1.2 link with forward secrecy
- Mutual authentication via RSA
- Non-impersonation via ECC challenge
- AES-128 encryption (AES-256 as a future option)
- Minimal attack surface; and random link traffic

5. Protected Public & Private Cloud

ImpCloud covers all aspects of end-to-end device security and connectivity, from initial device provisioning in the factory, device authentication, activation and enrollment, management and remote updates of device software and secrets, to in-field device monitoring. The ImpCloud is offered in two versions: a public cloud service and a single-tenant private cloud service using the customer's private cloud service managed by Electric Imp.

6. Secure Cloud Application Integration

To extract the most value from data, it needs to be integrated with analytics and enterprise applications. impSecure enables enterprise-grade cloud-to-cloud connections based on industry best practices. Secure integrations are assured using off-the-shelf, drop-in libraries for the most demanded cloud services, such as Amazon Web Services, Autodesk Fusion Connect, Microsoft Azure, and more than 25 others. **ImpCloud** APIs and cloud programmability are also available to rapidly address custom integration needs.

7. Full Lifecycle Managed Services

Security is not a feature, it is an ongoing process. As such, a system that is secure today may be insecure tomorrow . Industrial and commercial IoT products require ongoing expertise, monitoring, support, and updates to keep running smoothly, securely, and reliably for years to come.

impSecure by Electric Imp provides these Managed Services, ranging from SLAs, real-time support and expert consulting to ongoing maintenance and improvements to keep the Platform secure to cloud and device software updates and more.

Protected Cloud feature short-list

- Industry-best security practices, VPC architecture, bastion hosts, security policies, access control, device communication links terminated at application in cloud
- No device keys stored in cloud
- Automated cloud monitoring and management
- Device monitoring and security alerts

Application Integration feature short-list

- Industrial-strength cloud security
- Latest PKI and full chain validation
- HTTPS and secure AMQP (more protocols coming)
- Cloud application container
- Integration libraries
- Ability to implement custom application-level security

Managed Services feature short-list

- Ongoing platform maintenance and security updates (both cloud and devices)
- Rapid turnaround on security issues
- Near instantaneous over-the-air (OTA) in-field device updates
- Highly-experienced security experts working on your behalf

impSecure™ Managed Security

ImpSecure At-A-Glance

- Provides the trusted security you need to deliver full lifecycle IoT business value, from POC to EOL.
- Electric Imp developed the integrated, secure silicon-to-cloud connectivity platform so you don't have to.
- We constantly update, secure and monitor your products in the field for as long as you need them.
- Our staff of experts augment your own teams so you take advantage every day of increasingly rare resources without adding them to your payroll.
- Electric Imp is the trusted supplier for over 100 customers and their complex, demanding IoT products.

electric imp™

5150 El Camino Real Ste. C31, Los Altos, CA 94022 | electricimp.com | 1 650 383 7143

To schedule a briefing email us at sales@electricimp.com