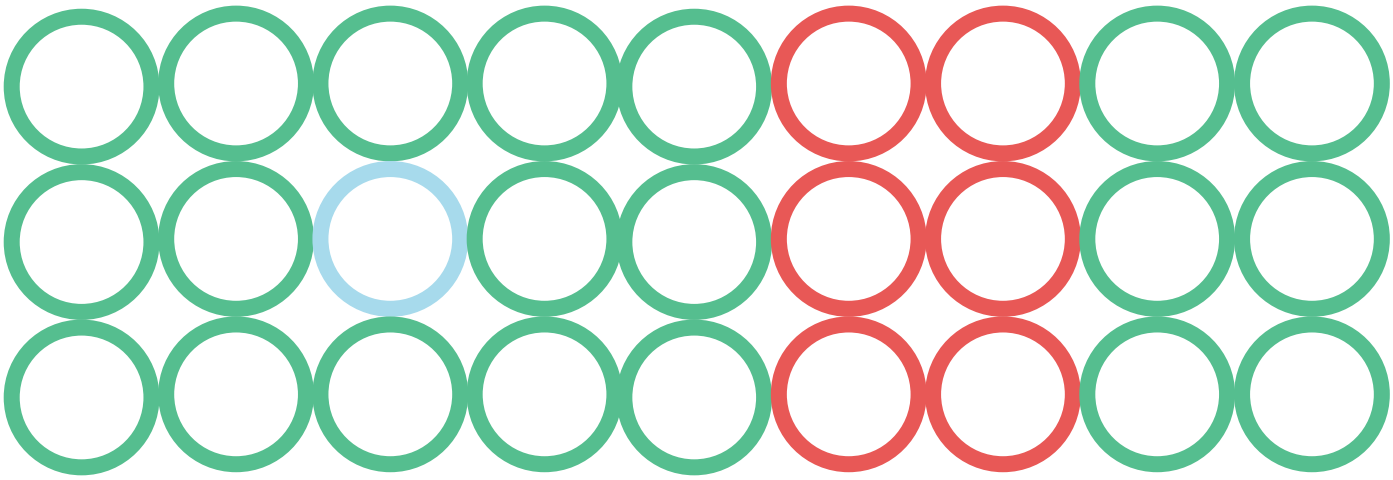
Cybersecurity Features

Delivering vertically integrated and secure IIoT solutions



November 2020

Contents

“

World-class security is the foundation upon which all our products and services rest.

SPENCER CRAMER, CEO, ei3

Secure by Design

Manufacturers cite cybersecurity as one of their most important considerations when choosing a supplier of cloud services. This is particularly important in Industrial IoT because of the critical nature of the connected devices and the value of the data they produce. As a result, savvy manufacturers go to great lengths to assess the experience, capabilities, product features and skills of any company they are considering to use for delivering a solution.

ei3, a leading supplier of Industrial IoT for manufacturing, has taken extraordinary steps to ensure the quality and excellence of everything ei3 does - and this naturally includes a close focus on cybersecurity.

The purpose of this document is to provide an overview of ei3's security and cybersecurity features to help the reader assess the benefits and risk reduction of using ei3.

Evaluating a company's cybersecurity strength is more than a review of certifications, questionnaires and feature lists. Done right, cybersecurity is inculcated in an organization's culture and manifest in everything an organization does. "Secure by Design" is what we call the plans, actions and responses that ei3 takes to promote robust cybersecurity throughout all aspects of its offerings and operations.

Rooted in Experience

Since 1999, ei3 has delivered thousands of secure connections to industrial equipment, machines, process lines, buildings, and transportation systems. Leading companies use ei3 to provide critical IoT services to their most important assets. ei3 has connected to the machines and lines that make products in a wide range of industries including: Chemicals, Food, Metal Parts, Packaging, Paper, Plastics, Printing and others.

In most cases, ei3's IoT solution works by connecting to and gathering data from the existing heterogeneous automation systems already running on the shop floor. ei3's solution is compatible with automation solutions from B&R, Beckhoff, Bosch, Rockwell, Schneider, Siemens, and many others. From this base of experience, ei3 is ready to tackle the largest and toughest enterprise Industrial IoT challenges.

Delivered as an Integrated Solution

One thing that sets ei3 apart from other Industrial IoT solution providers is its fully vertically integrated solution. As a "one stop shop", ei3 provides everything needed to realize the value proposition of the Industrial IoT. This is an essential feature because Industrial IoT solutions are complex - and with complexity comes the possible introduction of vulnerabilities. It is difficult to safely take a piecemeal approach of sourcing from different vendors to integrate a patchwork solution. This is because the edge devices, networks, cloud and apps from different organizations will have complex aspects that must be perfectly synchronized - even with a growing list of IIoT standards. If everything is not set up correctly, there is the potential to introduce risky cybersecurity vulnerabilities.

Over time, devices and clouds need to evolve to meet changing business needs and react to new cyber threats; as they evolve at different speeds and potentially diverge, managing the overall security of such a diverse solution becomes increasingly difficult: An Industrial IoT solution is only as strong as its weakest link.

The ei3 vertically integrated solution ensures that the hardware and software of each layer is designed to work together to provide a holistic approach to the complexities of the Industrial Internet of Things.

Executed with Skill and Passion

ei3's obsession with providing a strong cybersecurity defense drives our exacting specifications for everything we create. Product design at ei3 includes thorough exhaustive assessments of potential risks to inspire powerful mitigation strategies. Security measures are found in every layer of our full-stack delivery.

ei3 knows that the capabilities, commitment and passion of the team providing the IoT solution is a critical factor to security. A cybersecurity solution is only as strong as the people who stand behind it. Deeply rooted in ei3's company culture is the fundamental understanding that rigorous security practices promote trust from customers and business partners. This trust is evident by the continuous business growth that ei3 has experienced with its long-standing customers. The ethic of cybersecurity is most clearly manifested by ei3's inhouse developed and managed Information Security Management System, or ISMS. All employees are subject to the requirements of this extensive document which outlines all of the organizations standards, policies, rules and guidelines. The ei3 ISMS is aligned with ISO 27001 best practices and ei3's compliance to that standard is audited yearly by DEKRA, an internationally respected certifying body. This effort demonstrates ei3's commitment to security, a fact that is respected by ei3 users around the world.

ei3: Security Embedded

Systems engineers know that when every component of a solution is tightly integrated, the total solution becomes more secure. Each part of the full ei3 Industrial IoT stack has embedded features that work together to deliver a solution optimized for heightened cybersecurity defense. Some of these measures are described below.

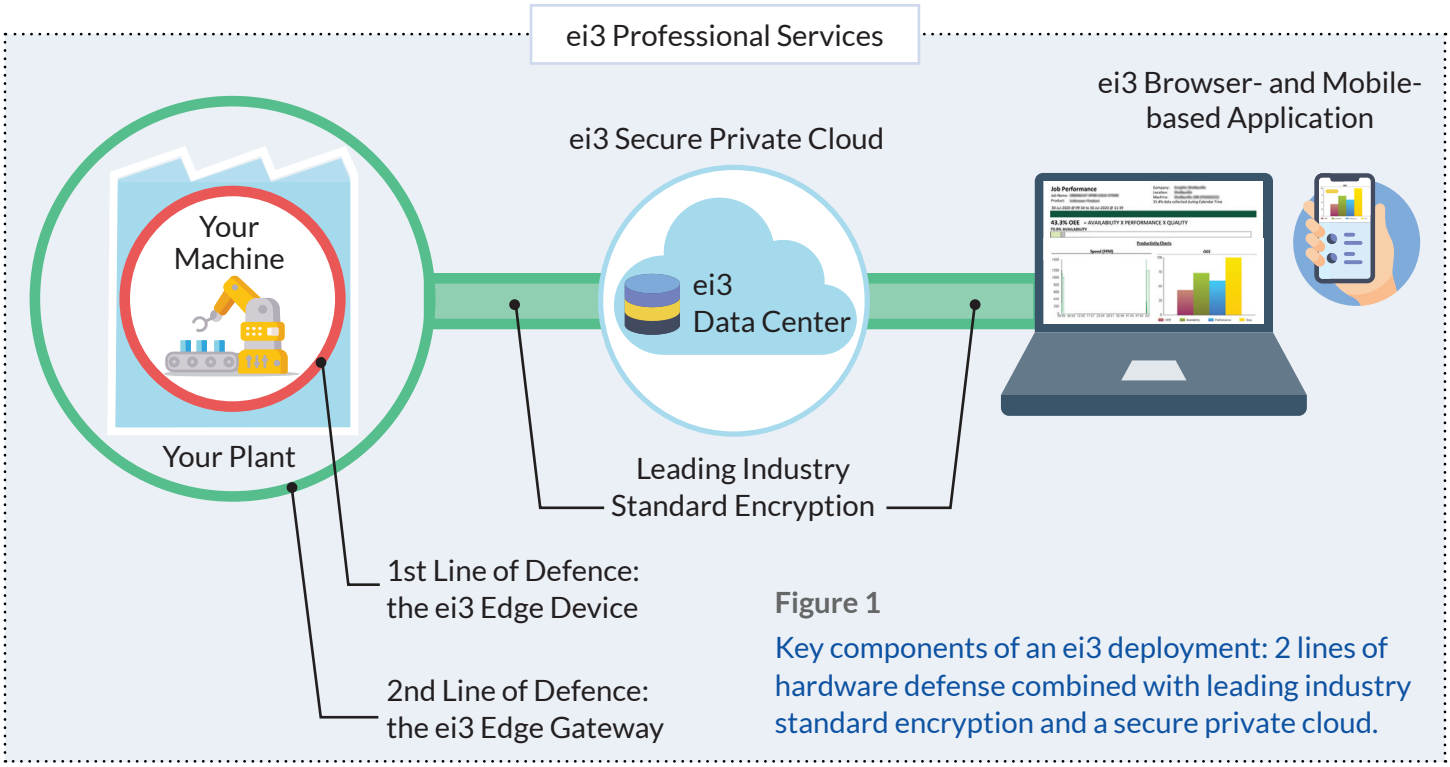


Figure 1

Key components of an ei3 deployment: 2 lines of hardware defense combined with leading industry standard encryption and a secure private cloud.

Hardware: The Amphion - your virtual fortress

The Amphion, ei3's edge device, is named after the Mythological Greek God who built the fortress at Thebes by moving stones with his lyre. Likewise, the ei3 Amphion builds a virtual fortress that can be visualized as defensive walls established around individual pieces of equipment inside a massive wall that protects the entire shop floor. ei3's Amphion creates these defensive walls in a practical, manageable and scalable framework. Some of the cybersecurity features of the Amphion are:

The Amphion only makes outbound connections to listed ei3 controlled destinations. This simple principle creates a high degree of cybersecurity because it means the Amphion will not respond to any inbound connection attempts.

The communication channels between the Amphion and its destination is always encrypted. A 2048 bit TLS encryption cipher is used to prevent third parties from intercepting data.

Amphion devices are configured online using the ei3 cloud. ei3 knows precisely how every device in service is set up, what data traffic is allowed, what ports are opened, and other details. Sophisticated AI algorithms inspect every configuration in real-time to validate and ensure no vulnerabilities are accidentally created.

Amphions are in constant contact with the ei3 cloud and are automatically updated with the latest security features. If a threat emerges, the ei3 operation team develop and dispatches updates right away.

The Amphion is an embedded Linux device built on a hardened linux kernel. This enables Amphion users to benefit from a broad professional community of security experts who maintain constant vigilance for emerging threats.

Edge device features are part of the Amphion. ei3 provides users with a docker container framework to provide a secure area for custom programs. Developers have a place to perform local Machine Learning and AI applications knowing their device and data are part of ei3's secure network.

IT professionals appreciate having a way to deploy edge devices and take advantage of powerful new features while being able to monitor and manage their security.

Managed Secure Network: safe passage for remote service

The SARS-COV-2 epidemic has driven Remote Access to the top of every manufacturer's list of priorities. Deciding how to respond to this acute need is complicated by many factors, but none is of greater importance than compliance with Enterprise cybersecurity policies. Connecting remote service technicians to equipment on a shop floor requires strict control over connectivity. Anything less creates unacceptable risk. This is why in the past so many organizations have simply made the decision to block all connections. But the reality of today's environment is causing more companies to rethink their approach and many see that ei3's Managed Secure Network holds the key to solve their dilemma.

Before discussing the cybersecurity benefits of ei3's Managed Secure Network, it is essential to realize that not all remote access methods are equal. In fact, there is a surprisingly wide range of technical differences that gives rise to an incredibly varied level of cybersecurity - a good reference is given at the OpX Leadership Network on secure remote access: ei3.com/the-remote-equipment-access-options-analysis

Secondly, it's important to stress that machine-mounted DIN rail VPN devices with "free" connectivity plans for remote access are not as free as you think. The landscape of threats on the internet is changing every day. Staying ahead of these changes means it is essential to monitor and upgrade every device that connects. This takes time and money, which if not done will undoubtedly result in creating vulnerabilities. For the safety and security of your company and its employees, you should always be wary of putting any device online that has a free or low-cost connectivity service at the core of its proposition.

ei3 delivers a practical solution with the highest degree of cybersecurity protection for connecting outside service providers to equipment on the shop floor. Software-defined access control and Zero Trust Networking are part of ei3's Managed Secure Network, and some of the security features are:

- All network connection points are monitored, to ensure that when the device connection is needed, it's there and ready for use. Every piece of equipment and device is constantly monitored for connectivity. Alarms are dispatched when connectivity breaks or shows abnormal behavior. Sophisticated log analyzers are used to monitor traffic to send alerts when abnormal behavior is detected.

- ei3 delivers a uniquely designed two-tier network where the secure internet gateway is isolated from the machine/equipment edge device with a customer-defined VLAN in between.

- An ei3 Gateway device is used to connect each manufacturing enterprise site. The device makes a secure outbound connection using TLS/SSL encryption with a 2048 bit cipher. A significant advantage is that there's only one point of contact for all machines/equipments/assets connected - regardless of vendor or control system type. By consolidating all connectivity through one device it becomes easier for IT to manage remote access to assets within the enterprise.

- A VLAN is used between the gateway device and the individual equipment. The data traffic on the VLAN is unencrypted. Unencrypted data traffic is compatible with the favorite monitoring tools used by company and enterprise IT professionals. They can monitor the ei3-created network to ensure proper use of their company IT infrastructure.

- A secondary ei3 Edge device is used to route data traffic between the machine control system and the shop floor VLAN. The router also performs two key functions:
  i) creating a subnet to micro-segment the machine network and
  ii) perform network address translation.

- The subnet or micro-segmentation of the machine control network creates a security wall around individual equipment, even parts of equipment. This enables the OT professionals on the shop floor to allow remote service access in a controlled, granular manner. It's a virtual function that is similar to what you would do when a technician visits a shop; they can only connect to the machine they came to work on.

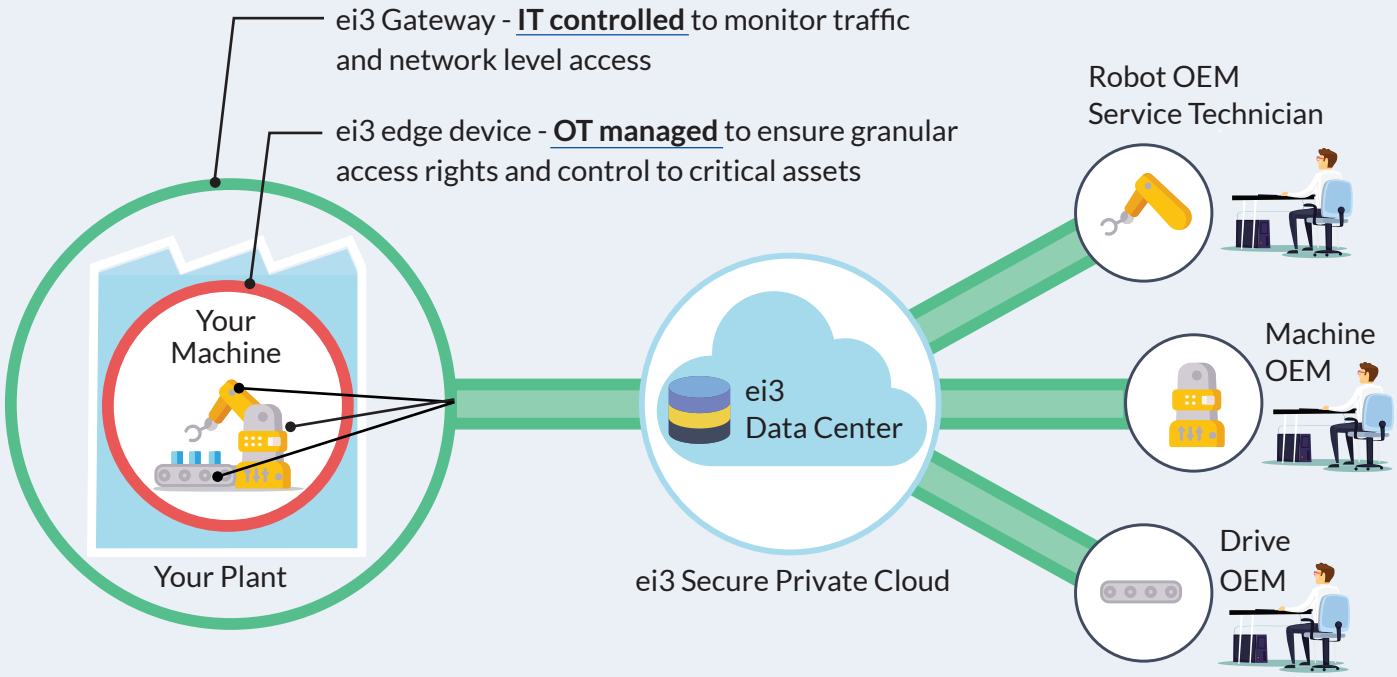
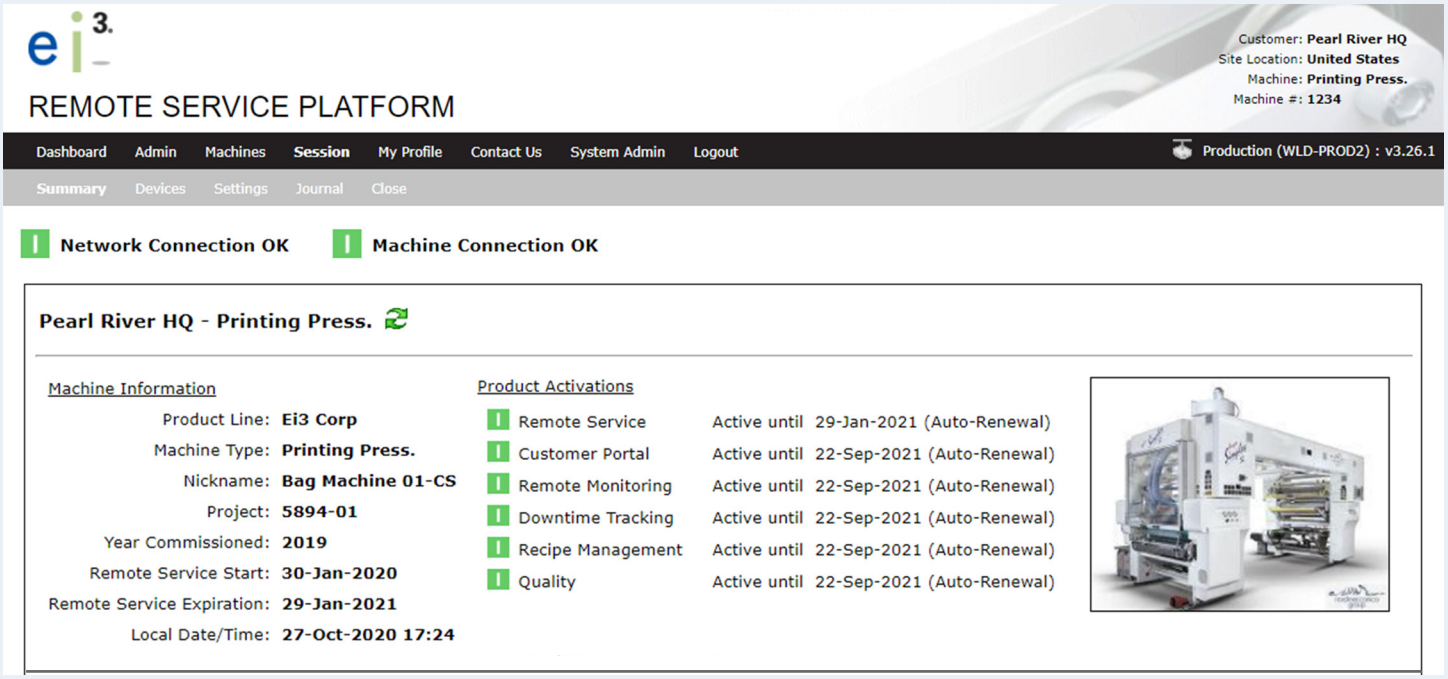


Figure 2

ei3's unique two-component architecture allows common machine access to multiple vendors - so each connect to their specific asset or system using a secure key. Each can access their respective data sets, or collaboarte in service sessions.

- The ei3 network is compatible with equipment from many vendors. Logic controllers, industrial computers, machine interface panels, robotic vision - anything that supports Ethernet for the programming port is compatible. This important feature enables the manufacturing enterprise to use ei3 to be the one remote service access method technical people use from many different OEMs, System Integrators and Consultants.

- ei3's Managed Secure Network comes with a full hierarchical active directory ready to manage a shop floor's complex organizational units with machines and lines from many OEMs and Integrators. This active directory provides one place of authentication for all third party users in a Zero Trust Remote Access environment. Connectors are available to link to enterprise Directory Services and domain federation is supported.



The ei3 Remote Service Platform provides control center for all access authorization

- OT personnel use secure web pages to invite authorized third parties by sending asset connection authorization keys by email. A second factor is provided through a different method to heighten security. The key is valid for a defined time and use is fully audited.

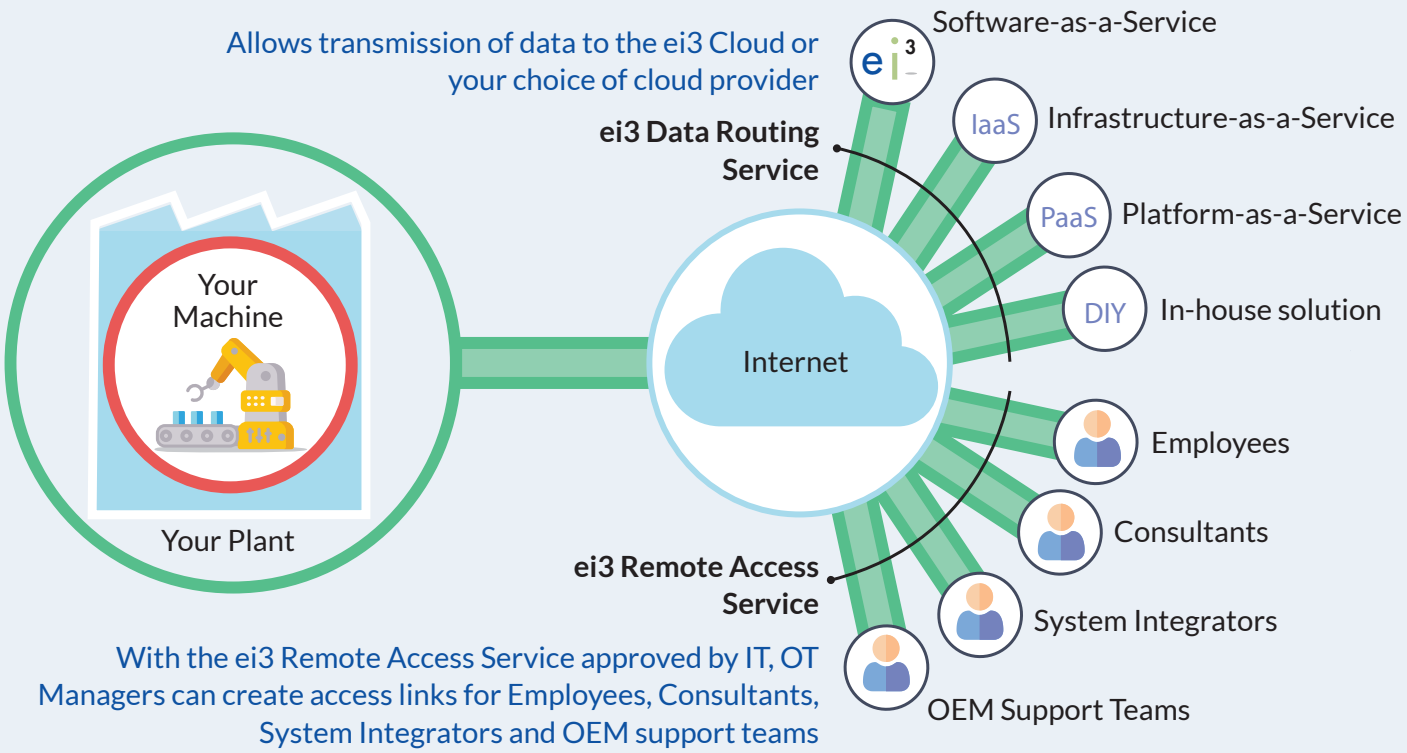
- Third parties who receive access permission are provided access solely to the assets which were explicitly defined when the access was defined. The third party is provided with an ei3 VPN client. This lightweight client is fully interoperable with VPN clients from all major connectivity suppliers. Once a connection is made, ei3 provides the service provider with a web page guided experience to help them understand and navigate the remote connectivity experience.

- Network administrators can use their in-house network analyzers to monitor the ei3 managed secure network traffic on their local VLAN. This feature assures that every byte of data communication is limited to only the intended devices within the specified sub-networks.

- Network configuration details are provided with full transparency. This offers further understanding and enhances security. Every important detail about the network and machine devices can be viewed, maintained and controlled by the ei3 cloud application. Rigid security rules are embedded into ei3 devices to prevent vulnerabilities from being introduced by mis-configuring a device.

- A final feature is that the managed secure network can be used for two purposes simultaneously. It can i) enable secure remote access to equipment and ii) serve as the transport for data collection. Transmitting data through a VPN increases security for the data being transmitted even if other protocols such as OPC-UA, MQTT or AMQP are used. Having only one network for these two features eliminates cost and complexity and increases security.

Figure 4



IT Approved, OT Managed

Many organizations struggle with deciding which technical team is responsible for assessing, managing and approving third party connections, especially those explicitly for remote technical support to equipment, machines and lines. The conundrum is that IT, or Information Technology professionals, have the skills to assess and choose cybersecurity solutions, while OT, or Operations Technology professionals are faced with urgent and important requirements for allowing connections to occur. This situation is compounded by the normal fact that both teams are exceptionally busy keeping up with their organization's requirements.

The design of ei3's unique solution accommodates the needs of both IT and OT. It works by putting a framework in place that can be understood, assessed and approved by IT professionals, and then managed on a daily basis by the OT professionals.

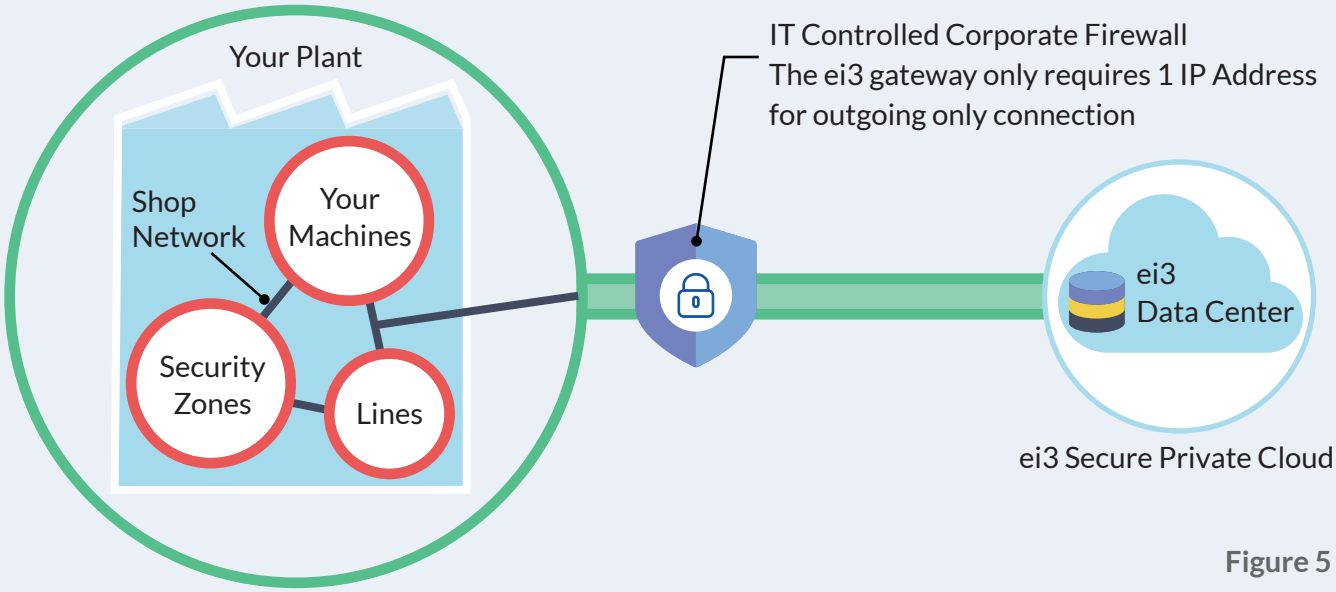


Figure 5

With ei³'s security and access architecture, IT regulates access into the corporate firewall and OT regulates internal access contol.

Once IT approves the solution then ei3 hardware is deployed to establish protection of the shop floor and each individual set of equipment. The ei3 devices are compatible with both existing networking equipment and most brands of machine controls thereby making it easy for organizations to adopt the solution by avoiding excessive costs for installing new managed (level 3) switches or expensive interface devices. To comply with IT security policies and standards data traffic on the Shop Floor network is monitored.

OT professionals know that Factory floors are dynamic with new equipment being installed and changes being made all the time. It's difficult for IT to keep up with these details about machines, their controllers and access requirements on the ever-evolving shop floor. This is why OT engineers are given the ability to add and modify the ei3 devices to allow connections to be established to their equipment. The OT team is also in charge of deciding who can access their machines and when. ei3's solution allows them to invite machine OEMs and other experts - which makes sense because OT professionals are the ones who need the support.

In addition to enabling IT and OT teams to work together, ei3 has an active role in maintaining security. From a global operations center, ei3 watches for threatening abnormal use and provides all devices with an automatic patching service to keep them updated with the latest cybersecurity features.

The innovative design of ei3's Managed Secure Network promotes strong cybersecurity while providing a practical solution that can be approved by IT and managed by OT professionals.

Zero Trust Remote Access ™

The ei3 Zero Trust Remote Access (ZTRA™) is an extension of the proven Zero Trust security model. The Zero Trust security model was conceived years ago when IT and security professionals began to give up on the security perimeter concept. It was not feasible to simply build a barrier around a corporate network and then assume all the activity on the inside, especially the manufacturing networks, are trustworthy.

The practical application of ZTRA has become urgent because remote access to machines and automation systems is an essential part of running a manufacturing shop floor. The ei3 ZTRA solution goes beyond perimeter security to ensure that personnel safety and operational integrity are maintained by providing these added benefits:

1. Proper vetting that the remote support person is the correct resource
2. Validating that the correct machine or equipment is chosen and linked for remote access
3. Ensuring that the activity takes place in the correct window of time
4. Limiting access to only the assets requiring support
5. Locking all other devices from access without proper permission
6. Documenting any activity that takes place with a remote connection

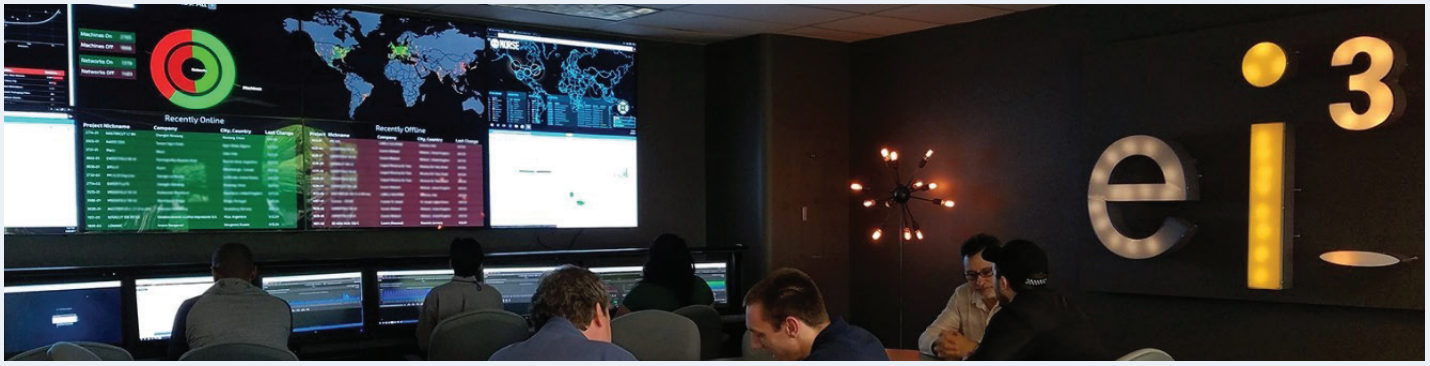
It is these enhanced capabilities that provide ei3 users with the confidence that will allow remote support that will increase responsiveness to equipment operations and potential failures as well as reduce the overall cost of maintaining these complex systems.

The ei3 Cloud: Purpose-built for secure Industrial IoT

Over the past decade, cloud technology has had a profound impact on the IT landscape in industry and manufacturing. Analysts agree that there is no one cloud architecture that fits all needs: private, public, or hybrid clouds all have their respective place for different applications.

ei3 has developed a cloud infrastructure that is scalable, high-performance, cost-effective, and has a proven track record with industry clients since 1999.

The ei3 cloud consists of a geographically diverse, highly fault-tolerant core of privately owned IT computing resources that is purpose-built for Industrial IoT. The ei3 cloud offers the benefits of on-demand scalability and interoperability with the most popular public clouds, including Google, AWS, and Azure. Some of the features of ei3's secure private cloud include the following:



ei3 Operation Center in New York is staffed with highly experienced network engineers to monitor ei3 data centers worldwide.

- Geographic locations are carefully chosen for ei3's cloud hosting centers. Before investing in a colocation contract, ei3 conducts an exhaustive detailed risk assessment of all factors related to a potential site. A primary decider is the degree of security that is provided by the colocation site host. The security factors assessed include physical security, personnel access, energy supply redundancy, internet access, networking and others. Considerations also include site stability, both geological and political.

- Once an ei3 site is chosen, ei3 builds a stadium of IT equipment. The ei3 stadium is a high availability triple-redundant modular hardware design that enables dynamic assignment of on-demand computing. Each ei3 stadium runs VMWare's V-Sphere to spin up and deploy the myriad of servers required to securely deliver a global Industrial IoT infrastructure. All physical equipment and virtual servers are subjected to ITIL processes for service availability, change control, patch and release management. These processes are rigorously monitored using automatic systems.

- Advanced log aggregation is performed including use of advanced analytical features that use Machine Learning methods to detect and alert when abnormal use events occur.

- The ei3 secure private cloud is protected by advanced firewalls that deploy an intrusion prevention system (IPS). This critical component delivers core security capabilities and protects against known threats and zero-day attacks such as malware and underlying vulnerabilities. Deployed inline as a bump in the wire, ei3's IPS solution performs deep packet inspection of traffic at wire speed, requiring high throughput and low latency.

- ei3 monitors the performance of all its data centers from a single network operations center, located in New York, which is staffed with experienced network engineers on a continuous basis. Any irregularity can be addressed immediately, and elaborate back-up plans are executed to ensure no customer data is affected.

Robust Suite of Apps: interface with your equipment securely and in real-time

ei3 provides users with a comprehensive suite of web-based applications and mobile apps that give users immediate access to the benefits of IoT. The method of subscribing to established internet applications, or apps, is commonly referred to as a Software-as-a-Service, abbreviated to "SaaS." Today many companies recognize that using a hosted SaaS saves them time and money while providing the benefit of always being up to date with the latest improvements.

ei3 applications are delivered using a software architecture called "Multi-tenant"meaning multiple organizations are using the same base of code, while data is kept securely apart. In a practical sense, this principle allows much more effort to be made towards application security than in a single-company case. As an analogy, consider the security features of a multi-family high rise apartment building versus a single home. The larger building can afford a higher degree of security than all but the richest of homeowners. Just like a multi-family apartment building has more protection, so does a multi-tenant application. ei3 delivers the security needed for the most stringent industrial requirements thereby providing a high level of clearance to meet the needs of most companies.

ei3's suite of easy-to-use apps to improve machine performance, improve quality and reduce energy:

All ei3 application pages are served to users using hypertext transfer protocol secure, "HTTPS." Transport Layer Security "TLS" is used to make the communication path between ei3's servers and the users - secure and protected against eavesdropping, forging of information and tampering with data. ei3 applications are compatible with all major web browsers. User authentication can be done using ei3's directory service or integrated with a customer-partner company active directory services.

ei3 applications are built around a flexible architecture that consists of a core database and admin tool and loosely coupled microservices. This method accommodates the rapid onboarding and scale-up of large fleets of machines. The reliability and speed of deployment is accomplished through the use of a standardized core database. The structure of the core has been carefully designed to meet the needs of most industrial application requirements. The flexibility and customization is accomplished by using loosely coupled micro-services.

These microservices can take many forms, including mobile apps, dashboards, reports, and integrations with ERP/MES systems. The microservices interact with the multi-tenant database providing a secure way to view and add data without interacting with the system core.

ei3 applications are served to authenticated users using an advanced multi-geolocated network of redundant java application servers configured for load sharing. Users are provided with a high performance and secure session experience because the application clusters are balanced and will share web requests across a common session. This clustered solution also enables most of the regular application upgrades to be done without interrupting user sessions.

ei3 developers work closely with the customer experience and customer support teams in an "agile" fashion to develop features and functions rooted in the practical realm, with software releases at least six times every year. A three-tier architecture of a complete environment for Dev, Test and Production is maintained to allow for thorough testing of the software before anything is released to production. Rigorous code control and automated deployment suites are used and managed by trusted system administrators to bring a heightened security level to the development environment.

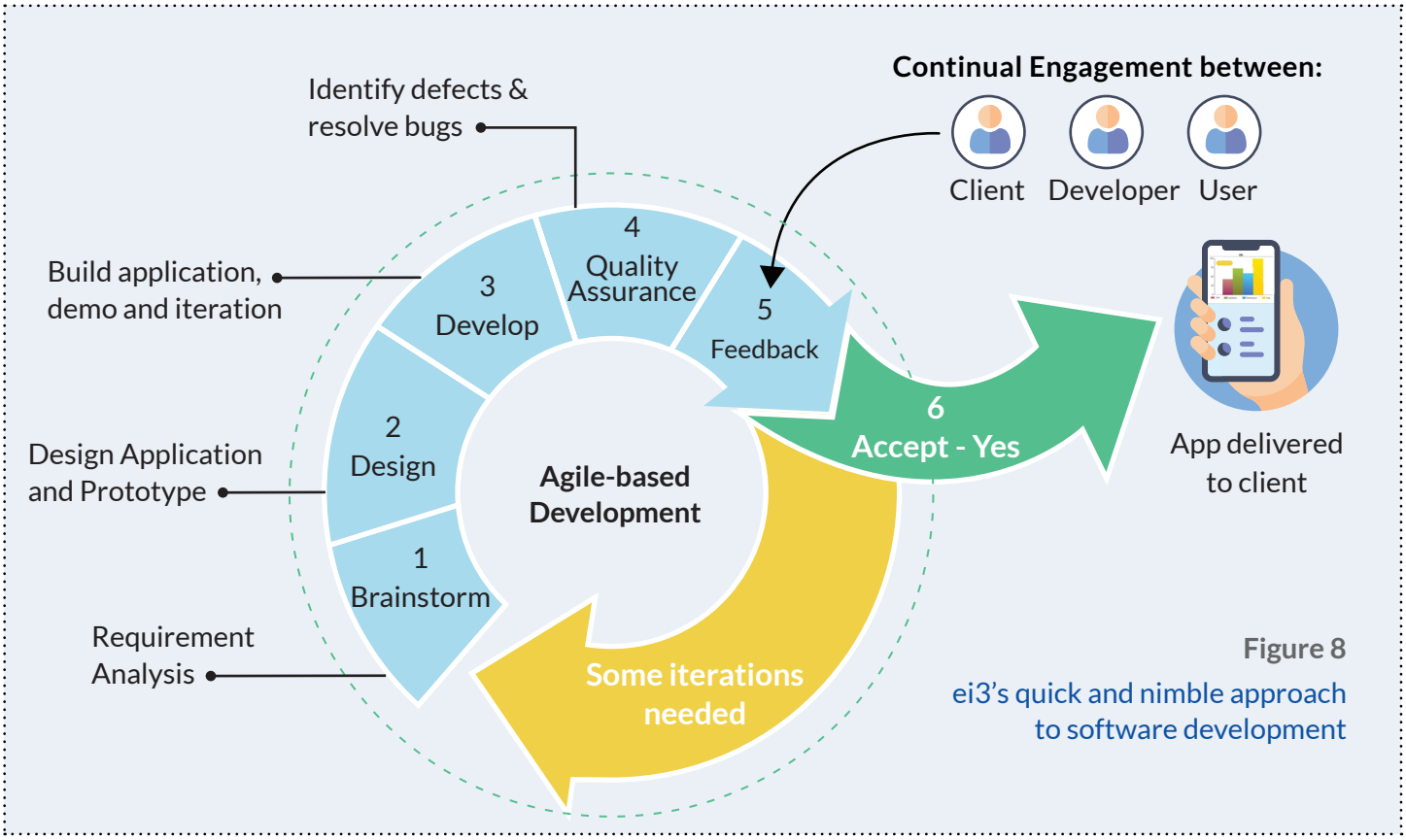


Figure 8
ei3's quick and nimble approach to software development

API and Enterprise Mirror

One of the most useful aspects of the ei3 flexible architecture is the Application Programming Interface, or "API." This powerful tool provides endless integration possibilities. The ei3 API uses Representational State Transfer, a.k.a REST, to retrieve and store data values from and to ei3. ei3's API provides a large number of integration capabilities with customers' back end data systems. For example, ei3's API can be used to integrate ei3 with ERP/MES systems sharing machine performance, quality and job data. REST APIs can be used to power up local machine dashboards or tie-ins to machine HMI computers. REST APIs can be used to put data from other sources into ei3, including on-shop floor acquisition systems based on Linux, PLC's even raspberry pi devices. The API is secure: calls may only send or receive data using HTTPS and each call requires a Globally Unique Identifier, "GUID," to be provided. The GUID provides robust granular control over the scope of the data fetched. Each GUID has the same degree of permissions as a user, thereby giving great control, flexibility and power over what can - and can not be provided by the API server.

While the ei3 API provides a powerful source of data, there are cases where a full replication is needed. For example, data replication might be required to comply with company policy or to allow third-party applications to perform independent queries and analysis. ei3 provides a solution for this with a secure and private data source called the "Enterprise Mirror." The Enterprise Mirror provides authorized company users with their own monitored ei3 data in a structured database of their choice that is completely isolated from the ei3 core database.This product increases ei3 security because it prevents any outside access to the ei3 core. This isolation follows the information security best practice of compartmentalization to avoid unintended access to ei3 data or resources.

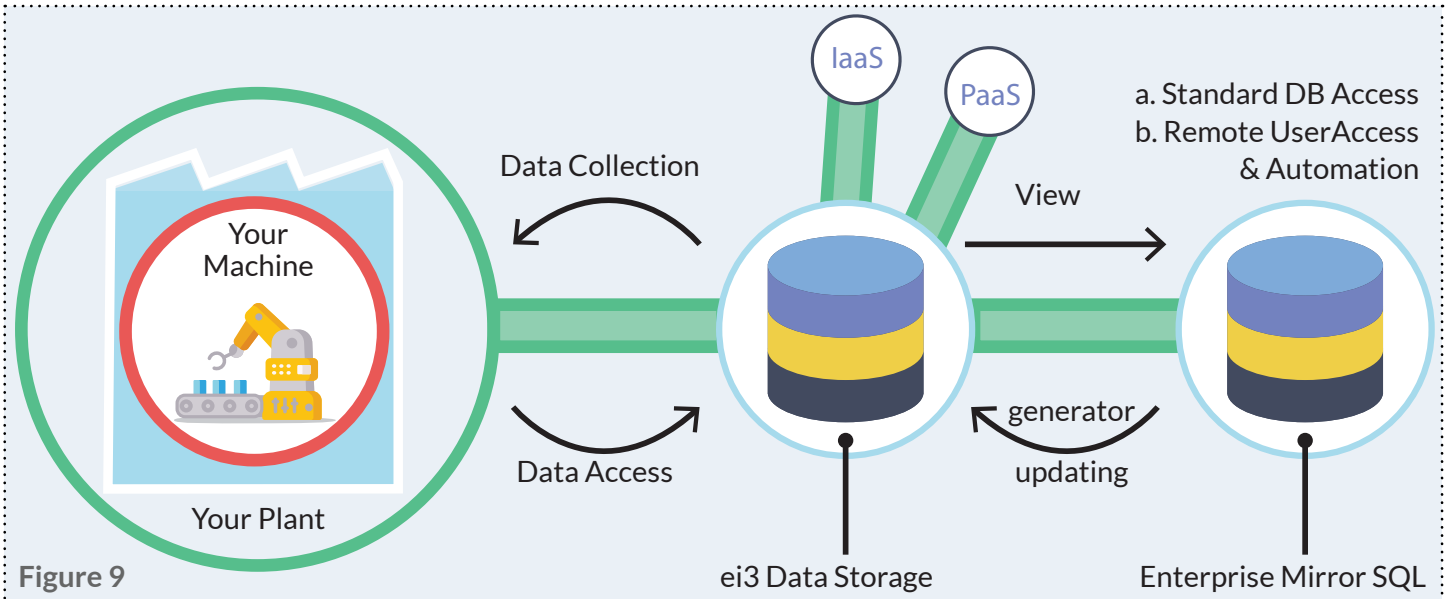


Figure 9

The Enterprise Mirror provides a copy of your IoT data

Standards and Best Practices

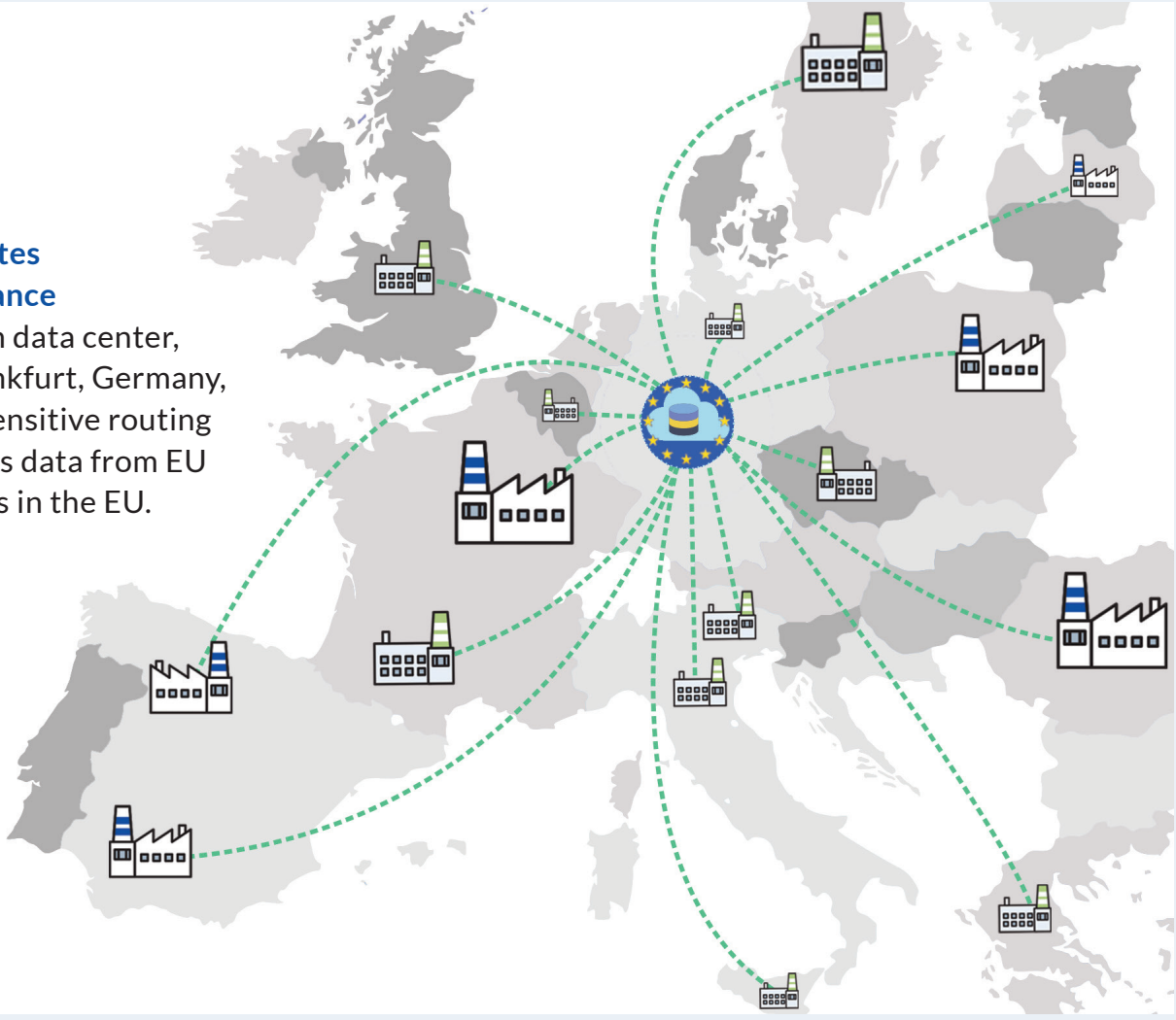
Compliance to **International Standard Organisation (ISO) 27001:2013, certified by DEKRA**

Following **The Information Technology Laboratory of the NIST Computer Security Resource Center Publication SP 800-82 rev 2**

ei3's Self Assessment to **the Cloud Security Alliance (CSA) Consensus Assessment Initiative Questionnaire (CAIQ v 3.1 is available to qualified organizations upon request**

ei³ demonstrates GDPR compliance

ei3's European data center, located in Frankfurt, Germany, enables geo-sensitive routing and guarantees data from EU machines stays in the EU.



Secure by Practice

Company culture is another cybersecurity factor of great importance. Company culture goes beyond having highly secure product features and compliance with known security standards. ei3's core values are excellence, dependability, and trustworthiness. Taken together, these core values define who we are.

The "e" in ei3 stands for excellence. We strive to deliver excellence in everything we do and seek business partners who share our passion and pursuit of excellence. Pursuit of our mission requires us to be dependable - we must reliably deliver secure solutions with completely trustworthy and transparent conduct. We are proud to be a leader in providing state-of-the-art, world-class security in Industrial Internet services, and we steadfastly conduct ourselves in an ethical and honorable manner.

One key action taken by ei3 to follow these core values is our use of (ISO)27001 as a specification for an information security management system (ISMS). The ei3 ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in ei3's information risk management processes. In a way, the ei3 ISMS defines who ei3 is from a cybersecurity perspective.

ei3 Corporation maintains a current certificate of compliance with International Standard Organization (ISO) 27001:2013 by DEKRA Certification B.V. The DEKRA audit validates ei3's commitment to the safety and privacy of client data, together with the integrity of ei3's IT infrastructure and business practices. ei3 set a benchmark by being the first company in the IIoT space in North America to have successfully attained the ISO 27001 compliance by DEKRA.

Ready for the Future

This document provides a small glimpse at the extraordinary efforts ei3 has made towards security. In addition to what you have just read, the cybersecurity practice at ei3 is constantly evolving and improving.

This happens continually because at the very foundation of a vigilant cybersecurity team is the recognition that threats are changing every day. Because of this it is not possible to deliver a comprehensive catalog of all the actions, designs, practices, standards and guidelines that are being pursued by ei3. Instead, this whitepaper aims to describe some of the high-level cybersecurity features of ei3 to convey the degree of importance placed on achieving world-class ability in this category. Hopefully, the reader now understands how ei3 sees its role and the seriousness it places on cybersecurity.

ei³ Corporation
Tel. +1 201 802 9080
E-mail: contact@ei3.com
Website: www.ei3.com

Contact us so we can help you as you develop your plans for digital transformation.

With over 20 years of experience, ei³ is in a unique position to provide a vendor-agnostic, scalable, and fully integrated solution that is IT approved and OT Managed — delivering the ROI of the Industrial IoT from day one.