HACH®

Be Right™

Water Intelligence

Security by Design, Efficiency by Nature

Claros is Water Intelligence. Designed by Hach, the Claros suite of solutions combines instrument, data, and process management to offer a comprehensive solution that can be tailored to your operations. Secure by Design, Claros uses premier security features so that organizations in the water sector can transform lab and process data into insights and optimization, while also reducing overall risk.

Built on the five key principles explained inside, Claros is Security by Design.

1

Not Just Any Cloud

Hach uses **Microsoft Azure**, the same **cloud trusted by the largest enterprises** to run secure applications and store the most sensitive data. We picked Azure because Microsoft has built it to be enterprise-grade and compliance-ready, and Microsoft reports that it has averaged over $1B spent every year improving and upgrading Azure's security. All data in Azure is automatically encrypted at rest and in transit, and automated smart traffic monitoring and profiling identifies threats before breakout events. Azure was the first cloud to support Trusted Execution Environments (TEEs) to ensure that data is safe from unauthorized access and tampering. It has built in Antimalware and Antivirus defenses and firewalls, which we take advantage of to provide additional layers of security for all Claros customers.

Hach uses Azure because we believe utilities and water treatment facilities deserve enterprise-grade protection. According to Microsoft's official reporting, Azure invests more, encrypts more, and monitors more than any private or public organization's IT team. See **Microsoft's Azure Trust Center** for more information about compliance and certifications.

2

Industry Best Practices

Our choice of cloud is just the beginning. Because we believe the best defense is multi-layered, Hach follows certain established **best practices** across the industry. As such we work to reduce the risks with any attack vector, and endeavor to ensure that that data stays secure and recoverable in the unlikely event of any breach.

Four Layers of Protection

Data Safe Encryption

99.9% Server Uptime

Regular Backups

Redundant data distribution

To that end, Claros operates from four key practices:

- All sensitive Data is stored in a “data safe,” encrypted at rest using AES-256-bit encryption and encrypted in transit using Secure Hash Algorithm 2 or AES algorithms, keeping data unrecognizable even in the event of a breach.
- We have a 99.9% uptime for all server-side activity, ensuring that operations aren’t compromised by DDoS or other service interruption attacks.
- We conduct regular backup snapshots, to enable a smooth and up-to-date recovery in the event of any compromised system.
- Data is distributed across multiple systems, to prevent a single source of failure and mitigate the risk of exposure.

In other words, from storage to access, from uptime to recovery time, Claros is built around certain industry-established **best practices** and certifications.

3

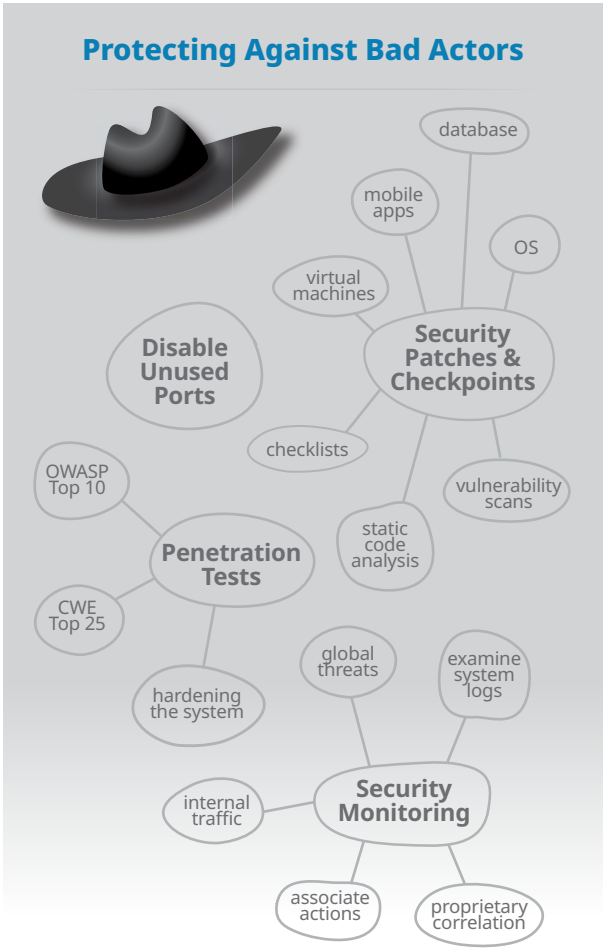
Comprehensive Risk Reduction

When it comes to water safety, risk is endemic. These are high value, critical systems, and mistakes can have consequences. As with any system, there are two main risk vectors: **bad actors** and **human error**. Hach's Security by Design offers a comprehensive solution to both.

Bad Actors

When it comes to **bad actors**, Hach uses a variety of techniques to curtail their ability to gain entry or do damage.

- All ports and services on any server that are not required for the operation of Claros are disabled, eliminating many opportunities for external intrusion, and reducing the number of ports that need to be monitored.
- Security patches are applied to all components of Claros, including the operating system, databases, virtual machines, and mobile applications, following strict policies and procedures. All software development and related patches follow IEC62443-4-1 Secure Product Development Lifecycle requirements. This process embraces the addition of well-defined security checkpoints and deliverables to each phase of product development, including security checklists, vulnerability scans, and static code analysis.
- To stay ahead of threats, Hach conducts frequent vulnerability assessment scans and penetration tests. This includes assessments using the OWASP Top10, a list that represents the broad consensus about the most critical current security risks, and the CWE Top 25, a list of the most frequent risks and errors. In addition, Claros Development Operations closely inspects the entire deployed solution to "harden the system" by identifying any unnecessary



services and removing or disabling those capabilities that might result in increased vulnerability.

- Hach has a real time 360-degree view of threats. Hach's security monitoring program analyzes information gathered from internal network traffic, associate actions on systems, and outside knowledge of vulnerabilities. At multiple points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using a combination of open source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Hach technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as unexpected activity in former associates' accounts or attempted access of customer data.

Human Error

There is, however, the other vector for risk: **human error**. Human error happens when someone leaves a password on a post-it note or picks a password subject to intuitive guessing or a brute force attack. It happens when someone engages with a system they don't understand, with permissions they shouldn't have. Human error can result in bad readings of data and actions that reduce efficiency, or in some cases, actions that can pose dangerous risks for water safety. The benefit of using the Claros Water Intelligence System is that it can reduce these errors as well, resulting in a more comprehensive reduction in risk profile.

To help solve for human error, Hach deploys additional security procedures to supplement instrument automation and data collection:

- Hach's policy is to log administrative access to every Hach production system and all data. These logs are reviewable by Hach Security as needed, and auditable should something go awry.
- When passwords or passphrases are required for access, Hach enforces strict policies, including password expiration, restrictions on password reuse, and sufficiency of password strength. We use two-factor authentication (2FA) for all access to production environments and resources. As a result of these efforts, human error and phishing risk is radically reduced.
- Hach also helps reduces exposure with strict permission controls. Operational access to Claros is limited to a restricted group of Hach Development Operations employees, controlled via the corporate network, and every activity is logged for auditability, to help ensure nothing happens out of sight.

Avoiding Human Error

4

Secured at the Source

Securing a system requires the right policies and technology. Feeling like a system is secure also requires trust in the people implementing those policies and deploying the technology. Hach has worked to ensure that we earn that trust.

Hach's Claros platform is certified as ISO 27001 compliant, a widely known set of standards for managing sensitive data and developing applications in a secure environment. Hach employees with authorization to access Claros undergo regular training that keeps them compliant with all Hach corporate security policies. This includes technical support and service staff, as well as operations staff and anyone that might handle sensitive customer data and information. Training includes compliance, secure coding training, and security awareness training, so that all operatives are aware of relevant and emerging threats before they become a problem. Hach also runs a DevOps department explicitly dedicated to the operation and maintenance of Claros.

Certification Process

1. Preliminary Audit
   Inventory including document review verifying completeness and compliance with standards.
2. Certification Audit
   Stage 1: Verification of ISMS documentation
   Stage 2: Confirmation of ISMS efficacy
3. Report
   Audit documentation including evaluation of the management system
4. Certification
   Proof of successful certification with a maximum duration of 3 years

AFTER 1 YEAR

5. First monitoring audit
   Auditing of ISMS implementation

AFTER 2 YEARS

6. Secondary monitoring audit
   Repeated auditing of ISMS implementation
7. Recertification
   Repeat steps 3 to 7 to extend for another 3 years

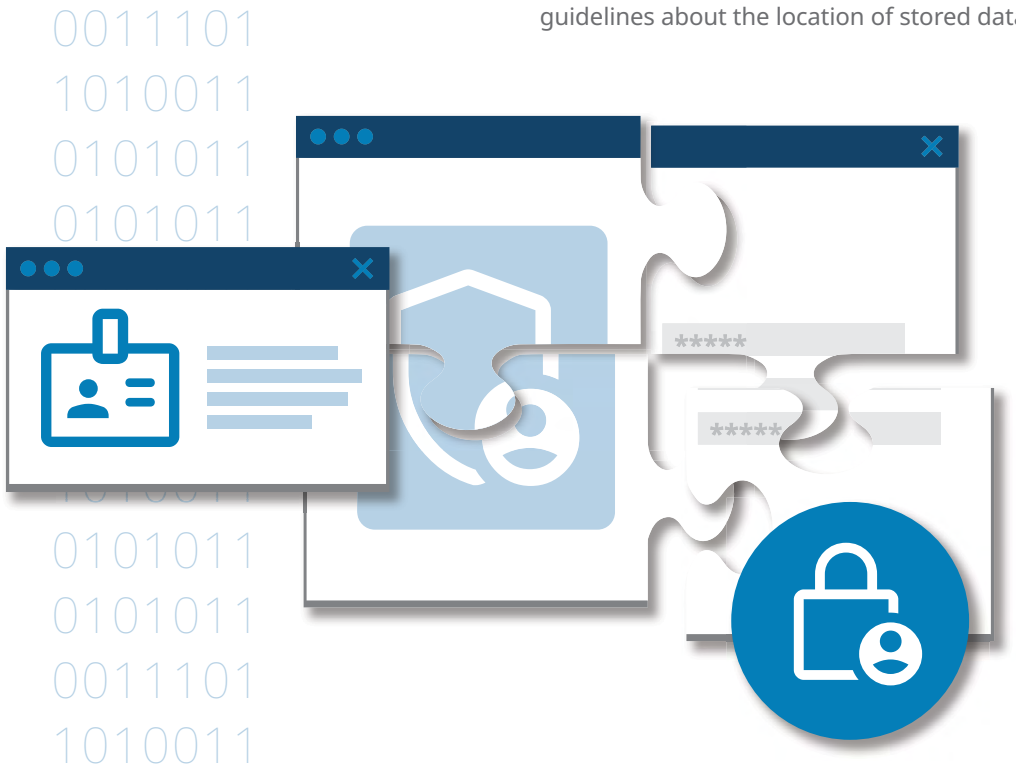
5

Privacy and Regulatory Compliance

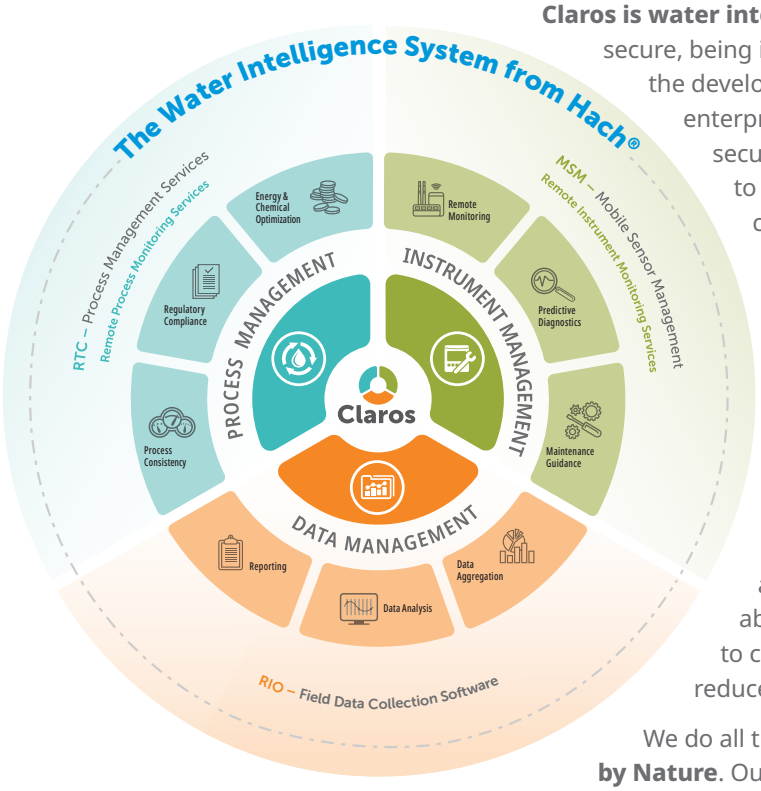
Finally, Hach is committed to a simple principle: your data is your data. Claros only collects data pertinent to the Claros platform—for example, measurement data, parameters, and device ID—and information needed for effective communication and coordination, including facility name, customer email, and usernames. Data remains the property of each customer, and Hach never sells PII or customer data to third-parties. We ensure this with yearly compliance assessments according to the General Data Protection Regulation, or GDPR.

Hach works under the assumption that your data is in fact your data, so that you can put the data to work running the plant without fear or doubt.

A big part of that puzzle is compliance. Along with following strict security procedures as outlined by the above third-party certification, Hach has made a series of decisions to help ensure that compliance and security go hand-in-hand. One of the benefits of Azure, for example, is that its servers are available in 140 countries, which means both that Hach can service more customers around the globe, but also that those customers can comply with national guidelines about the location of stored data.



Be Safer and Smarter with Security by Design



Claros is water intelligence, and a key part of being smart is being secure, being informed about threats, baking those threats into the development process, picking a cloud environment with enterprise-grade security, establishing robust, multi-tiered security frameworks, and training internal security teams to coordinate at every step of the way to keep customer, critical data, and product secure.

When we talk about **Security by Design**, we're talking about implementing best practices and security procedures that help mitigate risk both from the bad actors everyone is worried about and the human error that a customer might otherwise fail to see coming. We're also talking about continuing evolution of security protocols: updating vulnerability testing as new threats arise, evolving perimeter network defenses, regular penetrating testing, and improved administrative controls and backups. We're also talking about hosting a team of security experts who can talk to customers, help drive more secure outcomes, and help reduce the overall risk.

We do all this because **Security by Design enables Efficiency by Nature**. Our customers are improving the world's water supply, enabling clean water for drinking, manufacturing, and more. They deserve the efficiency and monitoring that can make their job easier, require less chemicals, and produce optimal outcomes. We do security best practices so that our customers can do their best work, without fear, without distraction.

That's water intelligence. That's Claros.

World Headquarters: Loveland, Colorado USA | hach.com

United States	**800-227-4224**	fax: 970-669-2932	email: orders@hach.com
Outside United States	**970-669-3050**	fax: 970-461-3939	email: int@hach.com

DOC063.53.30755