TOSHIBA

Connect with Confidence

An overview of Toshiba IoT Solution Pack's robust security features.

IoT-connected water systems unlock tremendous business value by helping managers effectively visualize, analyze and optimize their operations. Yet, connected devices can also increase security risks through exposure to cybersecurity vulnerabilities and data breaches. Smaller systems in particular face budgetary challenges with maintaining an up to date IT environment capable of keeping ahead of these attacks.
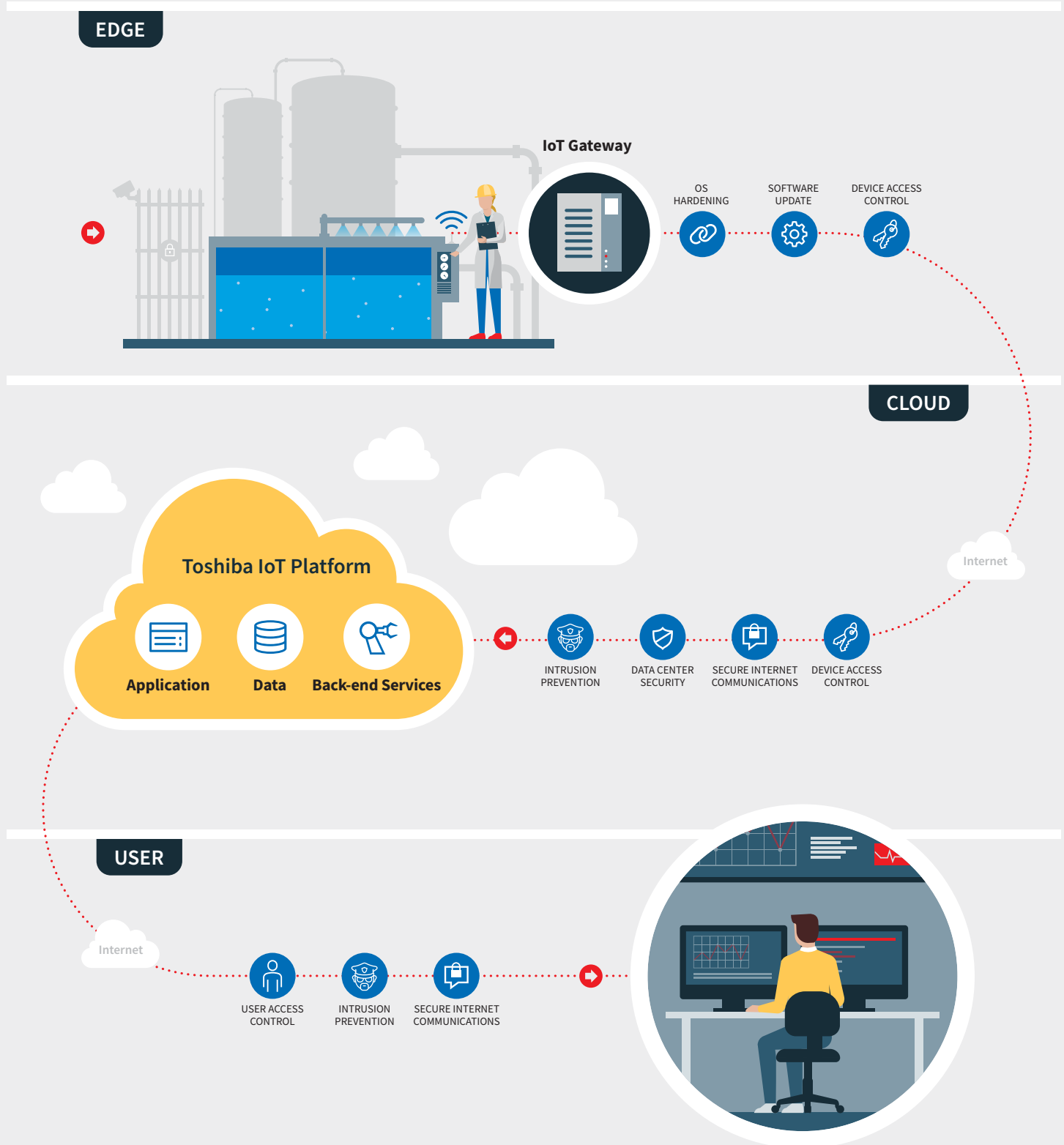
Many operations, particularly those that serve the public sector (e.g., water treatment plants), comprise essential community infrastructure and require reliable protection from an ever-growing list of cyberthreats.
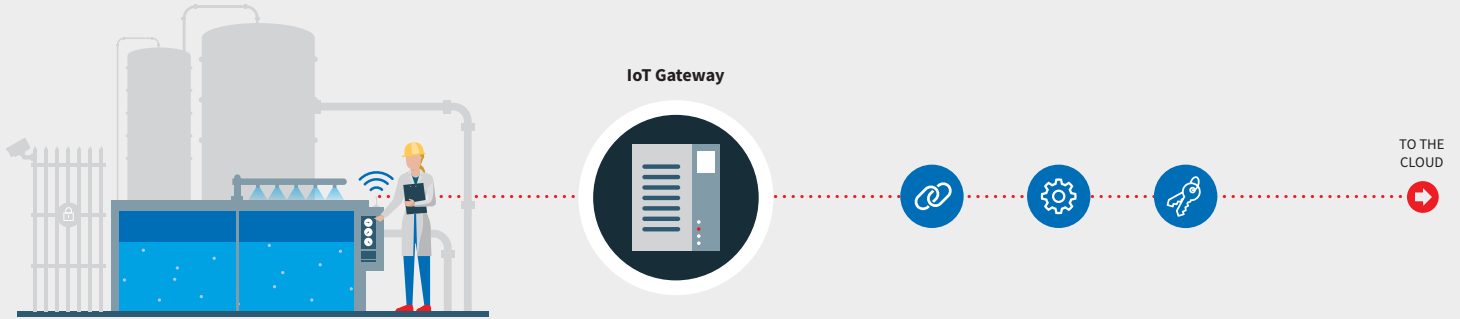
The Toshiba IoT Solution Pack application was built with customer security in mind, delivering the end-to-end protection that's vital to keeping your data, your operation and your mission secure.

A Multi-Layered Security Approach

Toshiba IoT Solution Pack bolsters overall network security by addressing key areas of vulnerability across the IoT infrastructure—at the Edge, in the Cloud and in the User environments.

EDGE

IoT Gateway

OS HARDENING

SOFTWARE UPDATE

DEVICE ACCESS CONTROL

CLOUD

Internet

Toshiba IoT Platform

Application

Data

Back-end Services

INTRUSION PREVENTION

DATA CENTER SECURITY

SECURE INTERNET COMMUNICATIONS

DEVICE ACCESS CONTROL

USER

Internet

USER ACCESS CONTROL

INTRUSION PREVENTION

SECURE INTERNET COMMUNICATIONS

**IoT Gateway**

TO THE
CLOUD

Security at the Source

Security requirements at the edge largely focus on protecting the physical environment—the connected assets that make up an operation. Depending on the industry, these could include pumps, fluid tanks, compressors, flow meters, and other devices. Most facilities surround their edge environment with some type of physical perimeter (e.g., wall or fence), which is secured and monitored by locks, access control systems and surveillance cameras. The IoT gateway located at the edge needs to be protected from unauthorized access like the other edge equipment.

The gateway device is the component that brings edge equipment and process data into the IoT application. Gateways integrate protocols for networking, help manage storage and edge analytics on the data, and facilitate the secure flow of data between edge devices and the cloud. Typically, the gateway is located in the edge environment. Therefore, it's important that the gateway be in a secure building with proper access control protection.

Toshiba's IoT Solution Pack provides the following security features in the gateway device at the edge:

Operating System (OS) Hardening – Unnecessary apps are uninstalled and the firewall is configured to limit access only to essential applications, thus helping minimize gateway OS exposure, preventing exploitation and external access to apps that aren't essential to the IoT infrastructure.

Secure Software Update – Software updates to the gateway are managed through a predefined server and are protected via a dedicated login credential. Updates can be initiated remotely or automatically.

Device Access Control – During the gateway software installation process, a unique certificate is installed in each IoT gateway. This certificate or key is used to verify the gateway before authenticating the device and allowing access to the cloud.

FROM THE
EDGE

Internet

Toshiba IoT Platform

Application   **Data**   **Back-end Services**
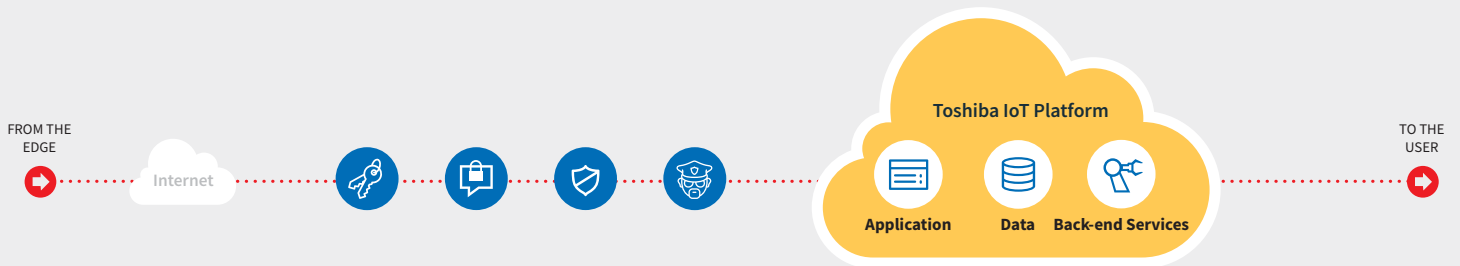
TO THE
USER

Security in the Cloud Environment

Most IoT networks connect and transport enormous amounts of data from edge devices to the cloud via the gateway. Because this data is the core of the IoT application, it's crucial that the cloud environment be highly secure to guard against today's rapidly evolving cyberthreats and help to keep your IoT infrastructure operation running smoothly.

In addition to providing device access control and secure communication to and from the gateway, Toshiba IoT Solution Pack is built on a highly secure cloud platform, providing protection to secure your IoT infrastructure and operational efficiency. You will benefit from having a secure datacenter with industry-leading operational practices making sure the cloud is protected.

Toshiba IoT Solution Pack provides the following security features in the cloud environment:

Secure Communication via TLS Encryption – Transport Layer Security (TLS) is the most current cryptographic protocol that provides end-to-end communication security of data transmitted over the internet, ensuring protection against breaches, eavesdropping, and malicious tampering or alteration of the content.

Datacenter Security – Toshiba IoT Solution Pack is backed by the most rigorous data center security and compliance standards in the world, ensuring your data stays safe and sound. Each year, independent audit reports (e.g. SSAE 18 SOC 1 and SOC 2) verify that the data center adheres to leading-edge security controls for data security, availability, processing integrity and confidentiality.

Intrusion Prevention – Because each gateway has a unique access control certificate, Toshiba IoT Solution Pack prevents cybercriminals from connecting a rogue or unauthorized IoT gateway and gaining access to the cloud as a trusted gateway device.

User Access Control – Different user accounts can be created—assigning unique access rights to different features and functions, based on user roles. Additional software features include user authentication and ID management through strong password policies, expiration timeframes and reset protocols in cases of suspected theft of user credentials.

FROM THE
CLOUD

Internet
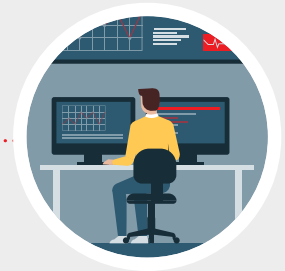
Security in the User Environment

The user environment is simply the location where the operation is being monitored and managed by a team of operators and administrators who access, visualize and respond to the flow of data from connected edge devices to the user interface. Typically, users log into their interface via the Internet, which can present cybersecurity risks, underscoring the need for strong security protocols designed to ensure proper access rights and protection from unauthorized actors.

Toshiba IoT Solution Pack provides the following security features in the user environment:

Web Application Firewall (WAF) for Intrusion Prevention – Web applications are increasingly targeted by malicious attacks such as SQL injection, cross-site scripting attacks and session hijacking. Preventing such attacks is challenging yet preventable—requiring rigorous maintenance, patching and monitoring at multiple layers. The WAF makes security management at this level much simpler by providing centralized protection of your web applications from common exploits and vulnerabilities.

TLS Encryption for Secure Communication – TLS is more efficient and secure than its predecessor Secure Socket Layer (SSL) as it has stronger message authentication, key-material generation and other encryption algorithms. The TLS protocol defines two layers: The TLS record protocol provides connection security, and the TLS handshake protocol enables the client and server to authenticate each other and to negotiate security keys before any data is transmitted.

A Rock-Solid Cloud Platform for Best-in-Class Security and Reliability

Toshiba IoT Solution Pack ensures maximum protection and availability of your data in and through the cloud. It not only delivers a consistent, reliable flow of information, but the peace of mind that comes with knowing your IoT infrastructure is secure and productive. Best-in class security in the cloud includes:

- State-of-the-art physical security at all data centers from perimeter to datacenter floor
- A wide range of threat protection technologies, including DDoS (Distributed Denial of Service) attacks
- Extensive regulatory compliance documentation

CATEGORY	COUNTERPLAN	DETAILS
Confidentiality	Physical	• 24H, 365D monitoring by camera • Motion sensor • Entry access management by biometric authentication • Alarm when security boundary breach
	Cyber	• Quarterly audit • 9 layer network security protection
	Inormation Leak	• Support/Service member authentication by Secure ID card or RSH Secure ID token • Data encryption by 128bit key/Communication encryption by HTTPS
Integrity	Data Loss	• 3 copies
Availablity	Physical	• Multiple power generator • Multiple power plant and two feeder • Duplicated power supply for rack • Battery backup • Computerized air conditioning
	Network	• Redundancy, failover
Operation	Compliance	• ISO27001 • SSAE 18 SOC 1 and SOC 2

Peace of Mind with End-to-End Security Features from Toshiba IoT Solution Pack

Connecting your operations with IoT technology is a smart way to collect data from throughout your facility, delivering near real-time visibility into your processes and enabling faster decision-making and problem-solving. Not to mention efficiencies and cost savings. However, more connections can mean more security risk—so you need a solution with security at the core. Toshiba's IoT Solution Pack delivers the efficiency you want, plus the security you need.

About Toshiba

A world-class technology leader, Toshiba brings decades of manufacturing experience plus a deep knowledge of using big data to solve real-world industrial challenges. We offer the partnerships, flexibility and field-tested insights for highly effective co-creation, plus a full range of Toshiba-developed IoT components—databases, sensors, gateways and agents.

Explore what's possible with a digital transformation. Learn more about Toshiba IoT Solution Pack today.

TOSHIBA

Visit https://www.toshiba.com/tic/other-products/iot-solution-pack | **Write** TIC-IoTsp@toshiba.com