NIS2 Directive: new organizational requirements

Risk Management

To comply with the new Directive, organizations must take measures to minimize cyber risks. These measures include incident management, stronger supply chain security, enhanced network security, better access control, and encryption.

Corporate Accountability

NIS2 requires corporate management to oversee, approve, and be trained on the entity's cybersecurity measures and to address cyber risks. Breaches may result in penalties for management, including liability and a potential temporary ban from management roles.

Reporting Obligations

Essential and important entities must have processes in place for prompt reporting of security incidents with significant impact on their service provision or recipients. NIS2 sets specific notification deadlines, such as a 24-hour "early warning".

Business Continuity

Organizations must plan for how they intend to ensure business continuity in the case of major cyber incidents. This plan should include considerations about system recovery, emergency procedures, and setting up a crisis response team.

Stratus

Resilience is not an easy task to accomplish

Who are we at Stratus?

We are '**The Experts in Uptime**'

We do one thing very well.

We have been doing it for over four decades.

We do it better than anyone else.

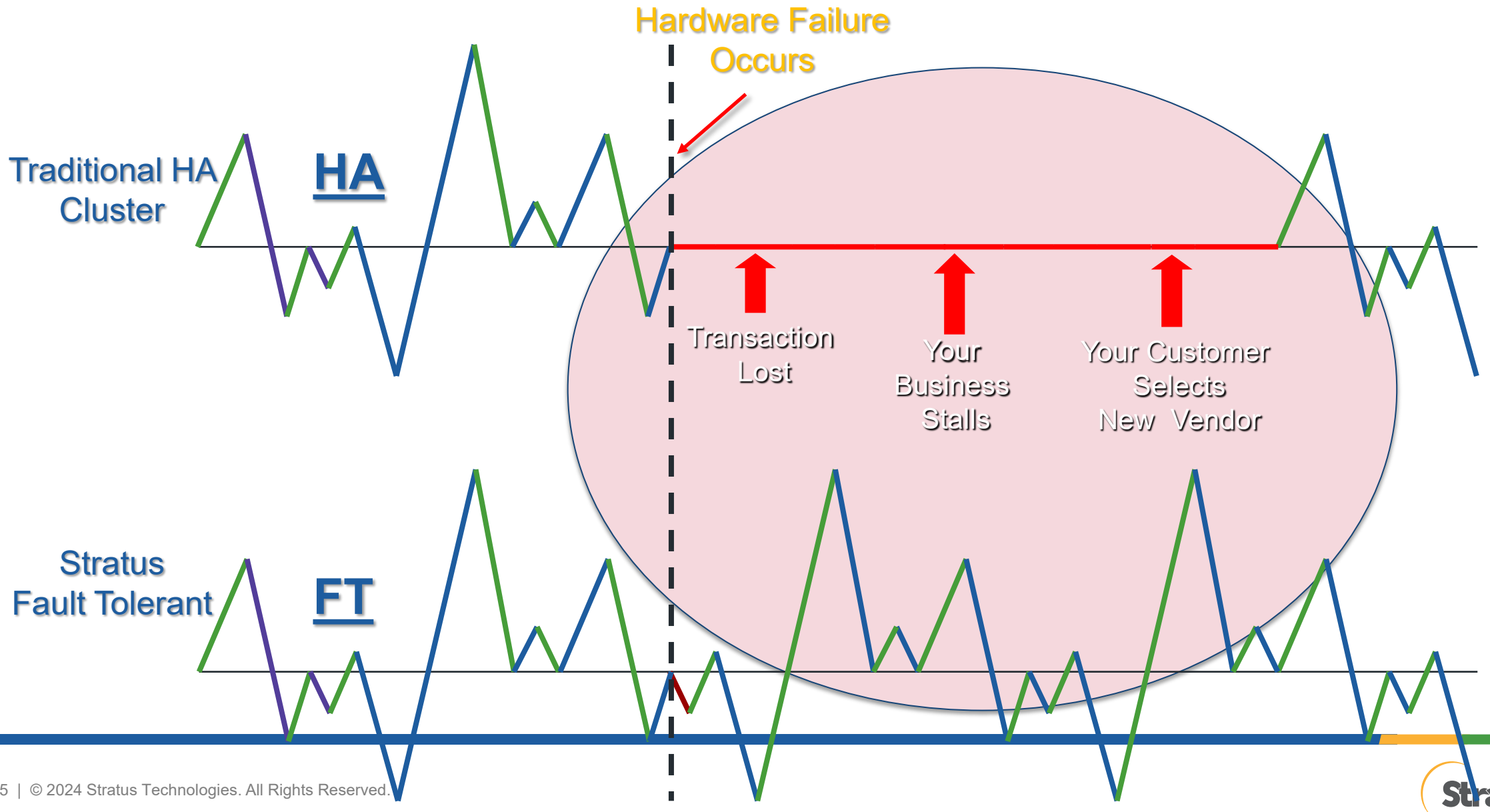
UPTIME

Stratus®

A PENGUIN SOLUTIONS™ BRAND

Standing out from the crowd

High Availability vs Continuous Availability explained



What We Do ?

Deliver zero-touch computing for continuous availability of mission / business - critical applications

Simple

Easy to install and manage
Highly interoperable
Manageable by IT or OT

Protected

Fault tolerant
Self-monitoring and healing
Secure

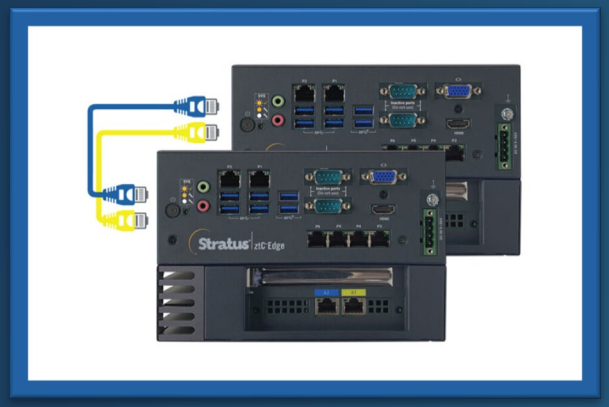
Autonomous

Seamless failover & redundancy
Automated replacement
Remote management

Meet the ztC's

Scalable from Edge to Data Center

Stratus ztC Edge

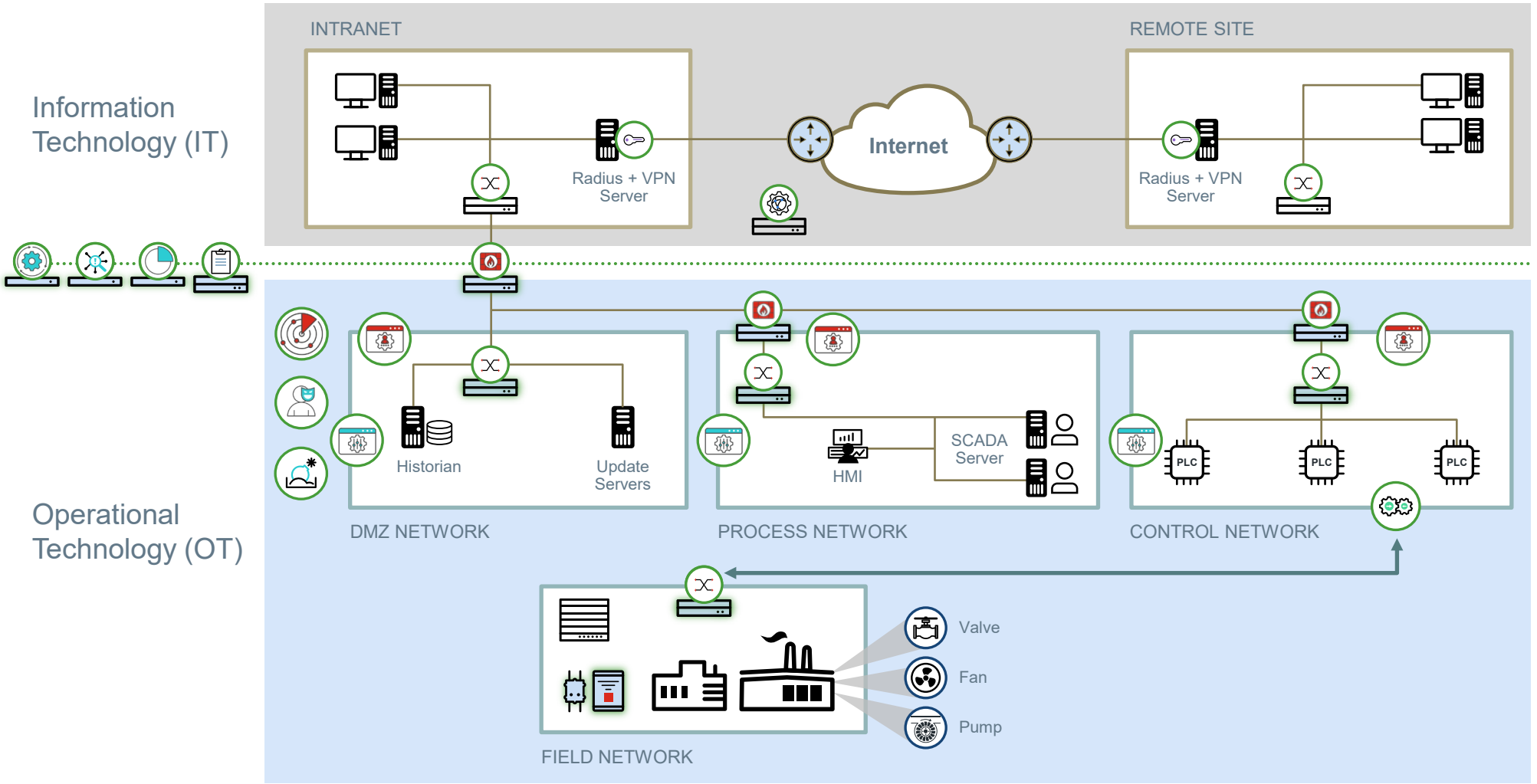


Zero-touch, secure, and highly-automated platform purpose-built for OT edge environments

Stratus ztC Endurance

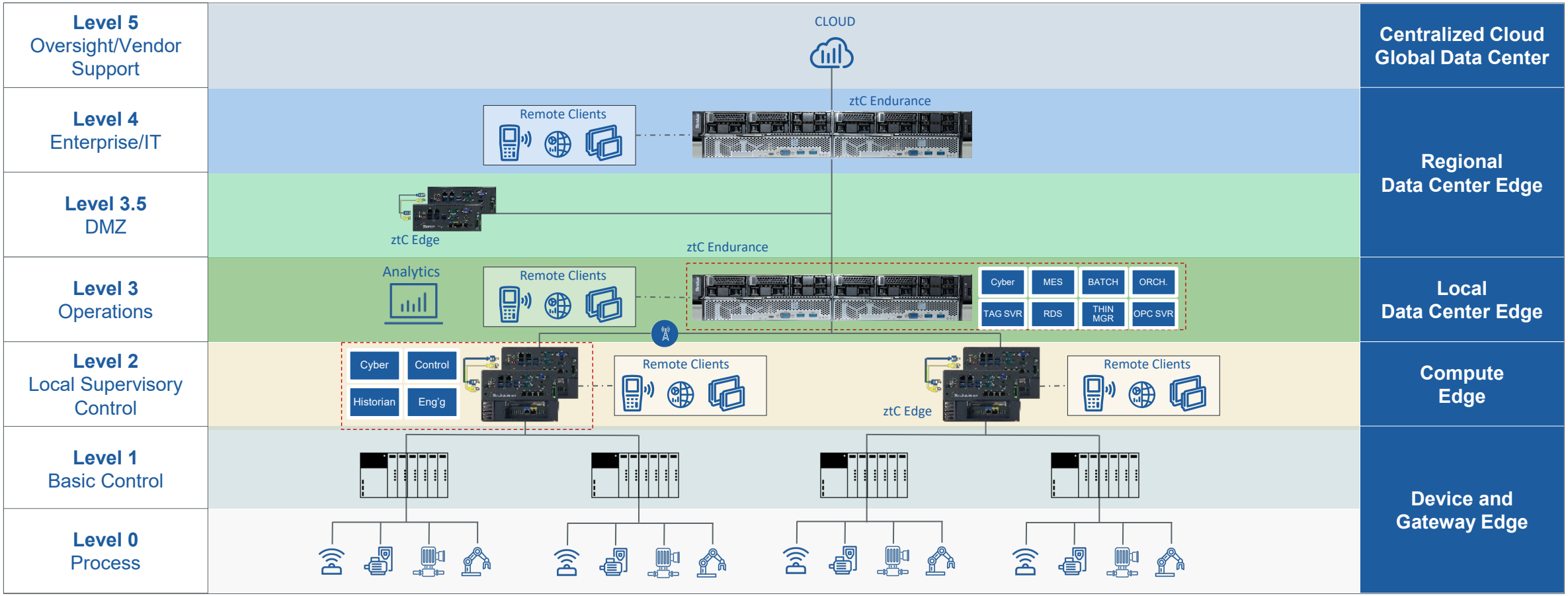
Intelligent, predictive fault tolerance delivering 99.99999% availability for next-generation, sustainable operations

Addressing Critical Controls Integrating OT and IT



- Zones and Conduits
- Secure Remote Connectivity
- OT Visibility
- Endpoint Security
- Security Monitoring
- Advanced Threat Detection

Purdue and Gartner Model Architecture - Industrial



in summary

- ✓continuous execution of software and protection of in-flight data
- ✓seamlessly integration into both IT and OT architectures with minimal support effort.
- ✓pre-validate cybersecurity solutions
- ✓consolidation of IT and OT workloads in a single Stratus compute platform backed by fault tolerance.

The importance of our Stratus Support Services

Our Customers / Personas

Our Customers just want to

‘Set and Forget’

So they can get on and :

- build it
- bake it
- brew it
- bottle it
- bend it
- box it
- bank it

Contact Stratus, we'll be happy to help during your digital transformation journey

- Solution brief Cybersecurity
- Stratus / Palo Alto reference
- Stratus is a member of Universal Automation Org
- ztC Endurance web page
- ztC Endurance data sheet
- ztC Edge web page
- ztC Edge presentation video
- ztC Edge data sheet

Giacomo Ghidini
Country Manager for Italy
Stratus Technologies
giacomo.ghidini@stratus.com
+39 335 6267585


Stratus
A PENGUIN SOLUTIONS™ BRAND
Thank You