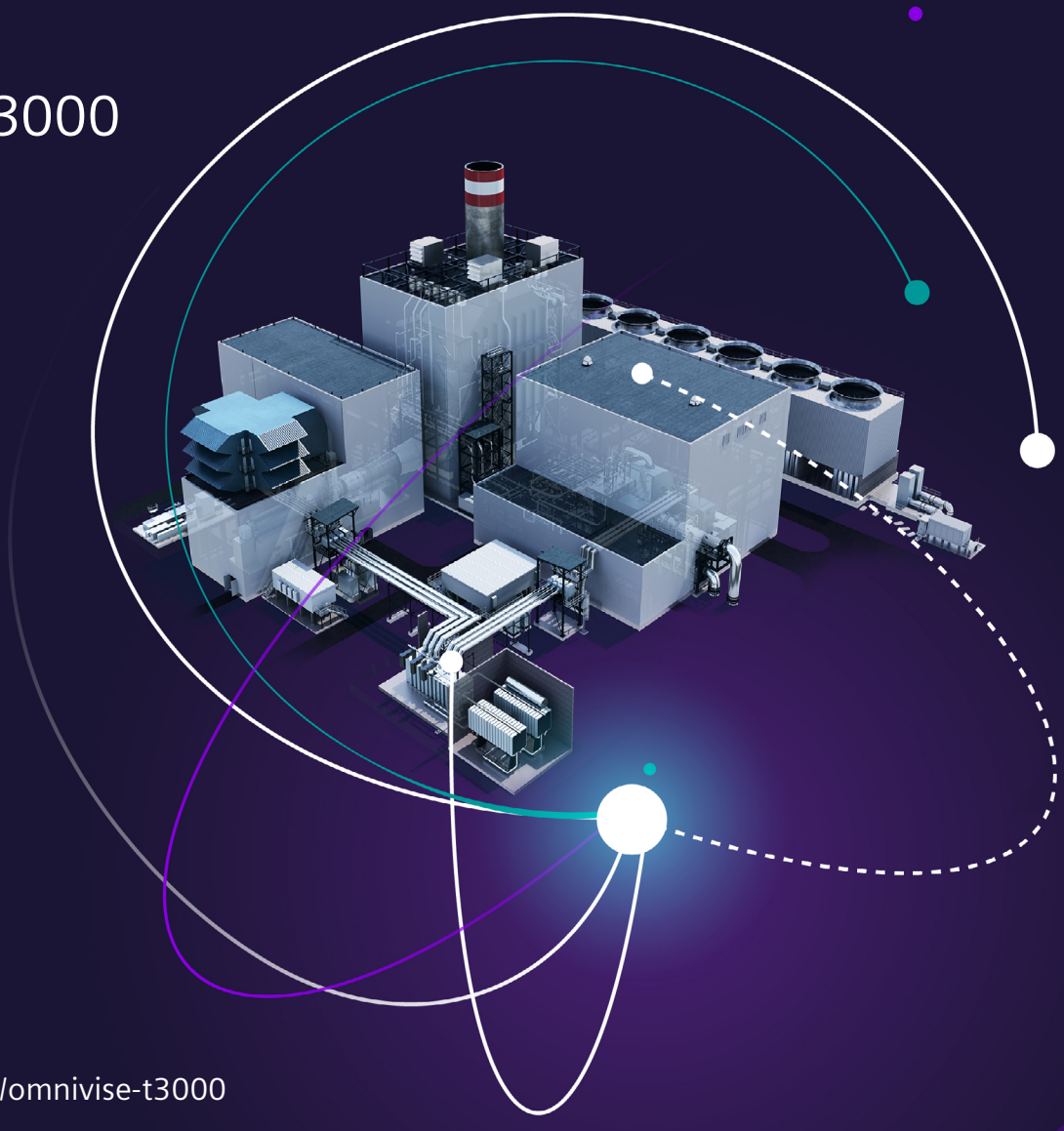
SIEMENS energy

Protect your power plant with continuous security

Omnivise T3000



siemens-energy.com/omnivise-t3000

Value & Benefits

Minimum Risk

Extensive Experience

- Omnivise T3000 in use in over 3,500 units worldwide

Global experts

- Presence in 190 countries
- Comprehensive knowledge of particular markets and their special requirements

Continuous investments in R&D

- Continuously innovating to allow you to be ready, flexible and resilient today and in the future
- Comprehensive knowledge of particular markets and their special requirements

Reliable Day-To-Day Operation

Tried and Tested Technology

- Clear and intuitive operation
- First rate alarm handling for quick reaction in critical situations
- One click access to root cause analysis
- Clear instructions and transparency of potential upcoming issues
- Integrated workflows, integrated Alarm Management & Analysis
- User friendly engineering

Investment Protection

Long Term Supported Release:

- Includes long term support for min. 8 years of lifecycle protection
- Online installation of patches and updates for uninterrupted availability
- Additional powerful security capabilities for compliance with challenging requirements
- Innovated hard- and software for flexibility in automation and communication performance
- Small size DCS for efficient and reliable operation of remote and distributed units and plant auxiliaries

Keeping Your System Secure

A secure system must always be kept up to date to reduce vulnerability

Every change you make could impact connected components, while vulnerabilities in one place may lead to problems across the system. The optimal way to manage security effectively is through integrated services: That is exactly what T3000 offers.

- We understand the power generation OT landscape better than a pure IT company.
- We are engineers, manufacturers and power generation asset managers, with profound OT know-how.
- We understand that patching and upgrading OT components is different than IT patches.
- The risks are greater, the potential for operational impact is higher and the need for specialized knowledge and skills is more urgent.
- We also understand the balance between stringent IT security and the need for physical security within a power plant.

Continuous development of cyber security features contributes to maintaining high plant security level for the entire lifecycle of your asset

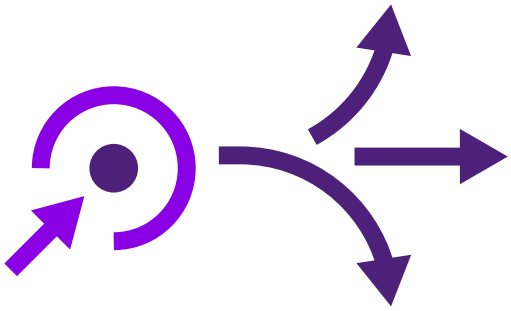
- Security features
- Security processes
- Handling of vulnerabilities
- Security consciousness
- Security Zone Architecture driven by NERC CIP V5, VGB-S-175 and IEC 62443-3-3 / IEC 62443-4-1
- Enhanced Security Testing

Cyber Security features of T3000, e. g.:

- Centralized Online Security Patch Management
- Malware Protection Solution
- Security Information and Event Management (SIEM)
- Configuration Change Monitoring
- Application Whitelisting
- Network Intrusion Detection System (NIDS)
- System Hardening
- Secure Remote Access
- Secure Data Gateway
- Active Directory
- Centralized Backup and Restore

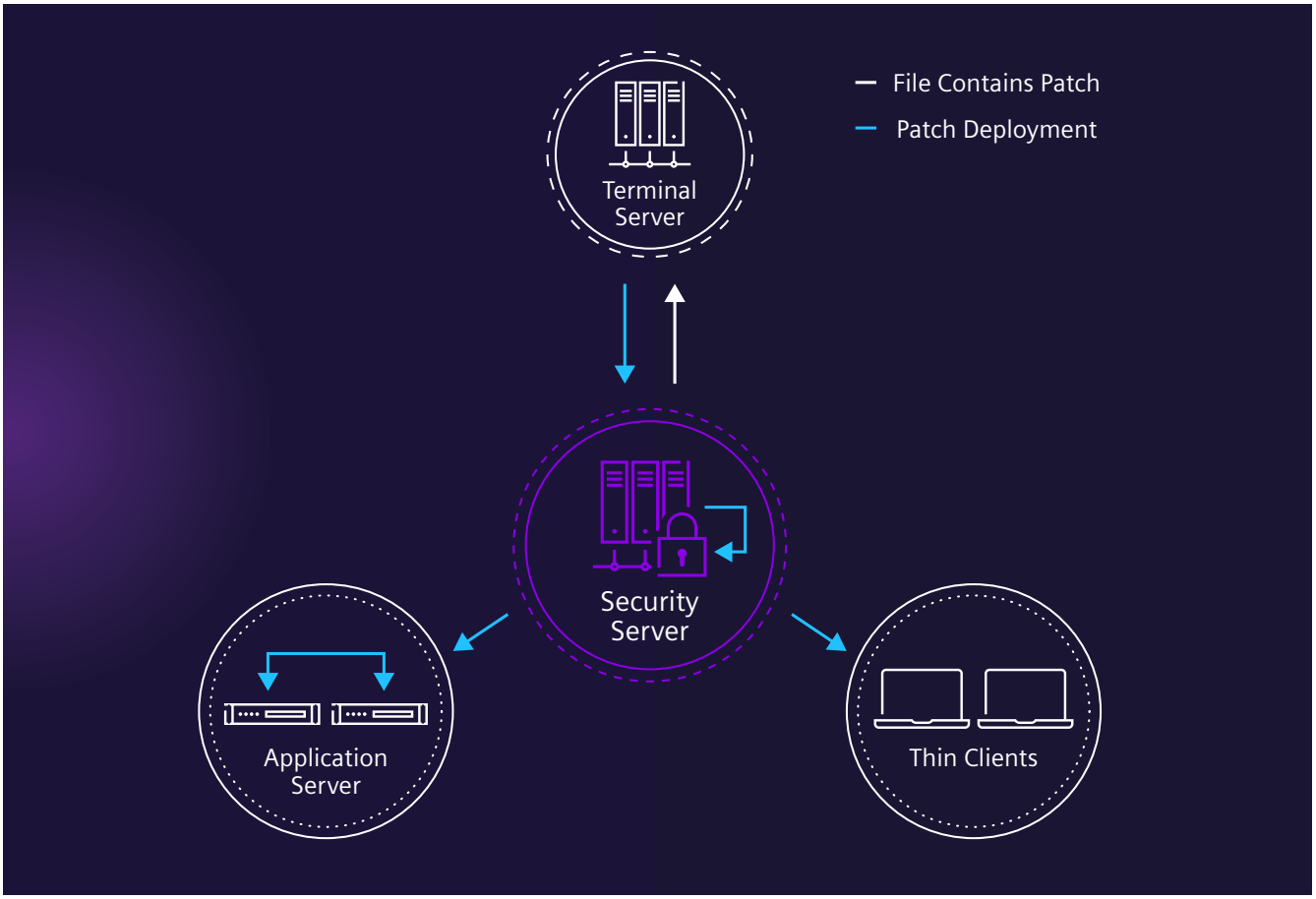
Simple, Secure Patch & Update Process

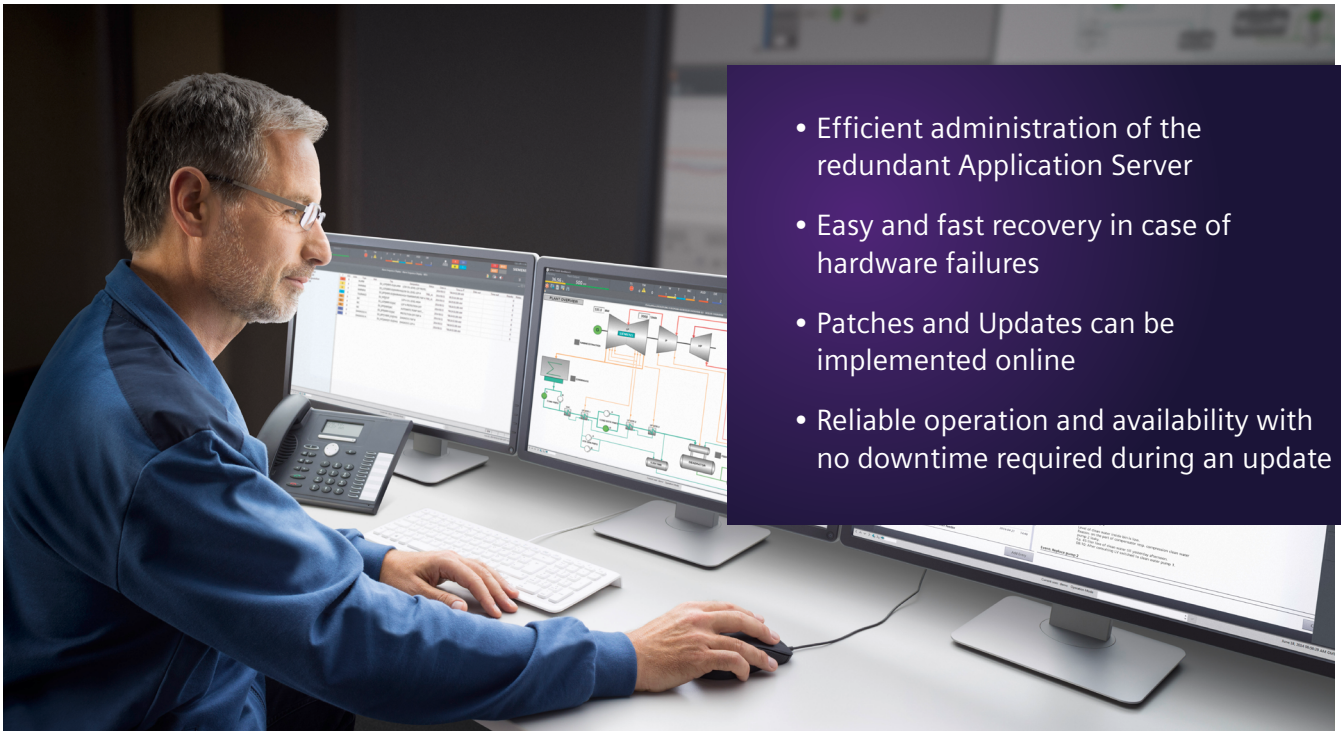
Centralized Deployment for efficient secure patch implementation



- User friendly via central deployment
- Flawless patch installation through control, monitoring and visibility from a single device
- Lower potential for security gaps resulting from un-patched components
- Transparency of the software status of the relevant components

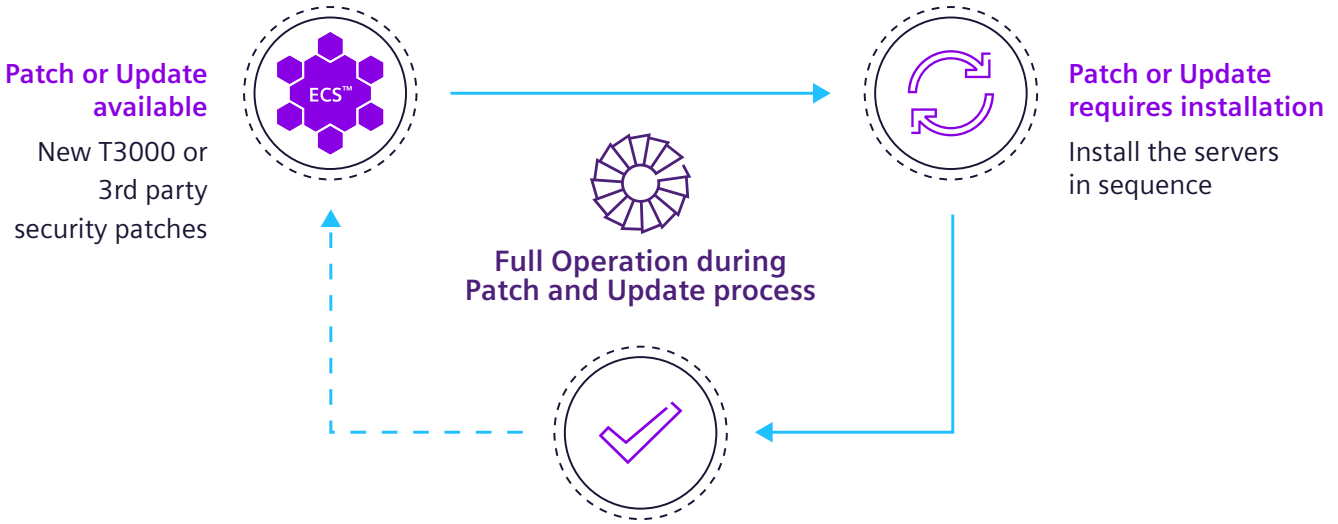
Security Server deploys security patches and virus patterns from a central point





- Efficient administration of the redundant Application Server
- Easy and fast recovery in case of hardware failures
- Patches and Updates can be implemented online
- Reliable operation and availability with no downtime required during an update

Online Patch and Update capability of the Application Server based on system integrated redundancy



Only a continuously maintained installation can be optimally kept “up to date” and secured

Vulnerability Management

The operational technology (OT) environment and landscape is constantly evolving, so vulnerability management is more important than ever before. Organizations need a modern, comprehensive strategy to quickly and accurately identify vulnerabilities and misconfigurations and remediate them, tailored to your standard installed T3000 plant. Siemens Energy T3000 provides a comprehensive strategy to quickly and precisely identify vulnerabilities and operational risks so they can be mitigated and remediated immediately, to avoid any potential for harm. This approach is customized for your T3000 plant.

The Challenge

Many software and hardware vulnerabilities may have operational consequences. These vulnerabilities can range from affecting physical devices, to modifying underlying execution procedures, to leaving security information exposed. Typically, operational technologies are actively scanned for vulnerabilities, but only during shutdown. Given the understandable reluctance to shut down a plant, this means fewer opportunities exist to scan for vulnerabilities. Even on rare occasions when a system network is analyzed, plant operators struggle to actively prioritize and schedule remediation. The plant's operational network remains unsecure.

Solution

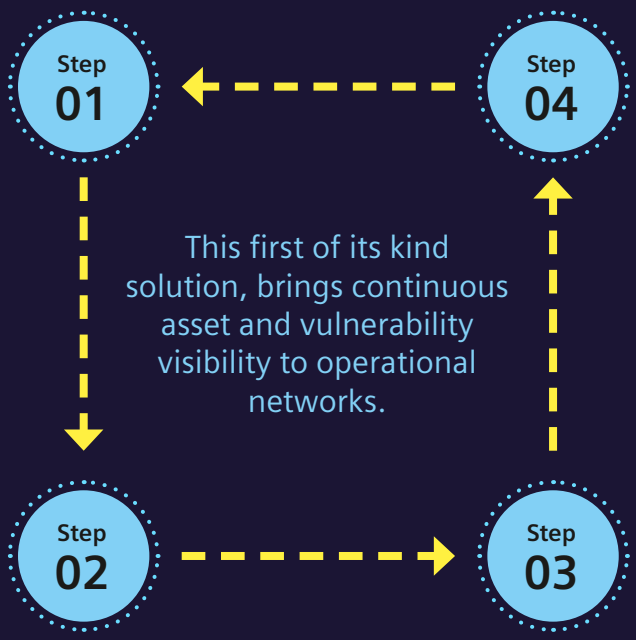
Considering the importance of having a well defined strategy for vulnerability management, we have developed a comprehensive srategy, which accurately identifies vulnerabilities and misconfigurations and remediates them, specifically for your standard installed T3000 plant.
We frequently issue security advisories to communicate any affected vulnerability, via our I&C Customer Portal.

Step 1

- Active and continuous scanning of all standard HW / SW / Firmware release products
- R&D notification of the vulnerabilities in real time

Step 2

Evaluation of vulnerabilities and T3000 specific risk assessment tailored to your power plant installed standard (given that you follow our standard release asset list) including affected compo-nents, probability, priority, impact and exploitability published regularly in the Customer Portal Security Announcement



Step 3

Remediation plan for every single vulnerability, communicated through the Customer Portal Security Announcement

Step 4

- Remote Service of regular inspection to identify, investigate, prioritize and remediate vulnerabilities as well as possible misconfiguration in the entire environment of standard delivered T3000
- Our service does not need active scanning and thanks to our state of the art online patching solution, can be done also online
- Service can be ordered on demand or on regular basis (per month, quarterly, annually)

What's Coming Next?

The next developments will introduce new security mechanisms to further enhance the communication security and operation of the system.

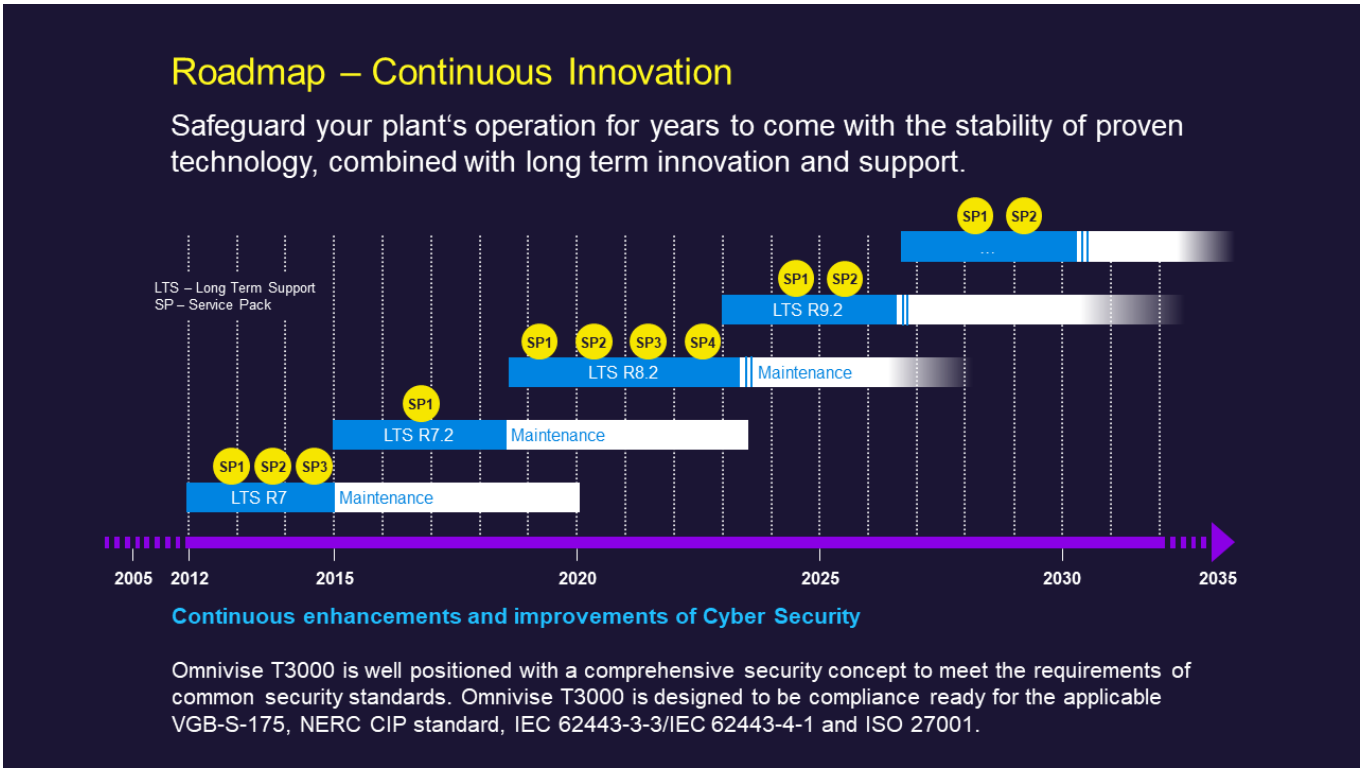
For example:

- Enhanced T3000 Hardening based on CIS bench-mark
- Improvement of communication security by extension of input validation
- Two-factor authentification for cRSP
- Full integration of Unidirectional Gateway (UDG)

Beyond T3000 itself, we can also offer services to help protect your investment:

- Service contract 24/7 availability of system experts
- Remote proactive services to detect potential issues before they escalate
- I&C Monitors & Advisors implement digitalization into the traditional DCS service
- Software or System Maintenance Agreement – we keep your software "up to date" and secure

For additional information or questions, please contact your local sales representative.



Published by and copyright © 2022

Siemens Energy Global GmbH & Co. KG
Otto-Hahn-Ring 6
81739 Munich, Germany

For more information, please visit our website:
www.siemens-energy.com/omnivise-t3000