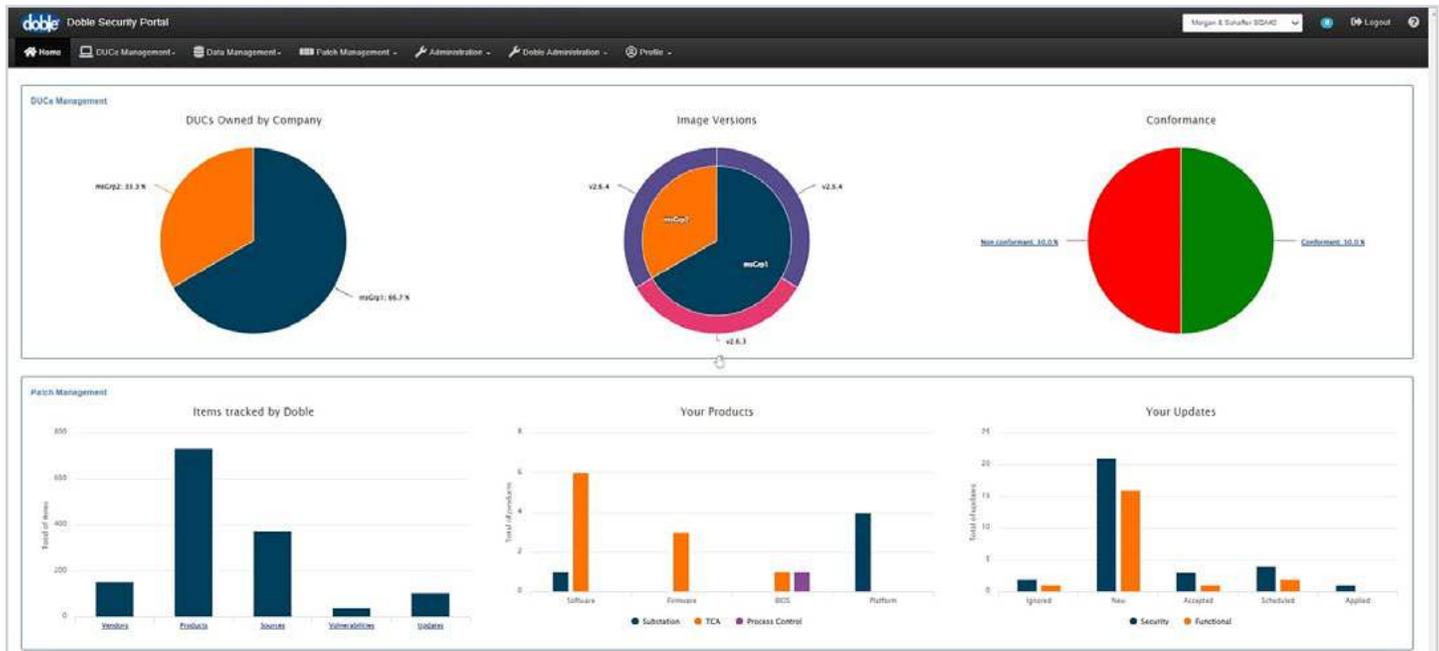


PatchAssure™

Managed Security Software Patching

CENTRAL UPDATE MANAGEMENT FROM A SECURE PORTAL



Doble PatchAssure™ is a portal-based management solution that ensures IT and Compliance teams meet NERC CIP security patch and software update requirements easily, efficiently and economically. Cybersecurity experts from Doble consult with you to identify which of your cyber system products to include in your profile, then they prepare your Doble Security Portal™ access where you can login to see your CIP-reportable elements, including your transient cyber asset (TCA) fleet, and make clear-headed decisions on matters requiring your attention. Recommendations from Doble help you know when patching deployments are critical and which devices they affect. Compliance evidence is at your fingertips!

FEATURES

- Covers all aspects of patch management, from discovery to delivery.
- Covers all types of cyber assets, including substation devices and transient cyber asset (TCA) field computers.
- Covers all types of product updates, including security and functional enhancements.
- Modern, easy-to-use Doble Security Portal™ with comprehensive management and reporting of fleet devices and updates.

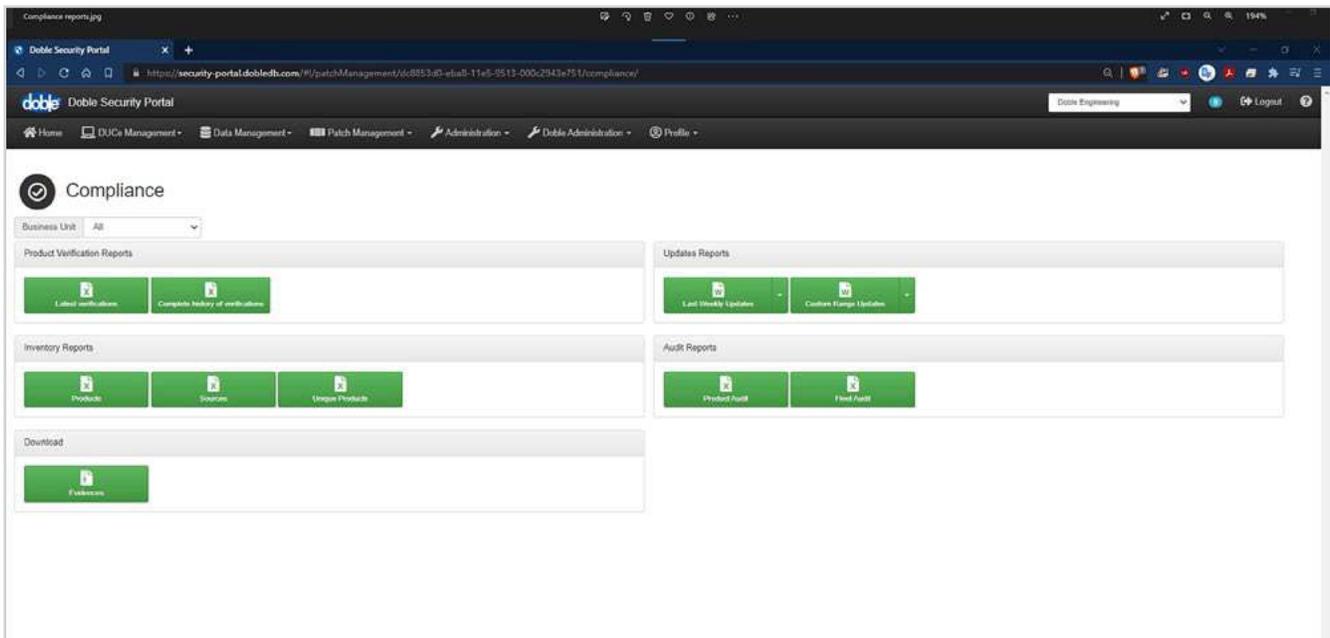
BENEFITS

- Considerable cost and resource savings compared to in-house programs.
- Quicker discovery of vulnerabilities, patches, and emerging information.
- High degree of traceability and efficiency.
- On-demand evidence for NERC CIP audits.
- Doble expertise and support every step of the way.



NERC CIP COMPLIANCE READINESS

Leverage the tracking and reporting tools that PatchAssure provides to improve your company's NERC CIP-7 and NERC CIP-10 compliance stance:



CIP-007-6 R2 - Security Patch Management

Patch sources being tracked must be documented; at least once every 35 days, patches must be evaluated for applicability; within 35 following evaluation, patches must either be applied, or create a dated mitigation plan, or revise an existing mitigation plan.

1. Patch sources are documented and also monitored for availability of patches.
2. Patches retrieved are analyzed for applicability and recommendations are given per classification criteria being met. Patch sources are checked weekly.

CIP-010-4 R1 1.6 - Configuration Change Management and Vulnerability Assessments

Software being patched must be verified for integrity and the source must be identified.

1. Patch integrity verifications are performed.
2. Patch sources are identified.
3. Details are provided in weekly reports.



Doble Engineering Company

Worldwide Headquarters
123 Felton Street, Marlborough, MA 01752 USA
tel +1 617 926 4900 | fax +1 617 926 0528
www.doble.com

Specifications are subject to change without notice.

Doble is an ISO 9001 & ISO/IEC 17025 & 17034 Certified Company.

Doble is an ESCO Technologies Company.

PUBLISHED: JUNE, 2024