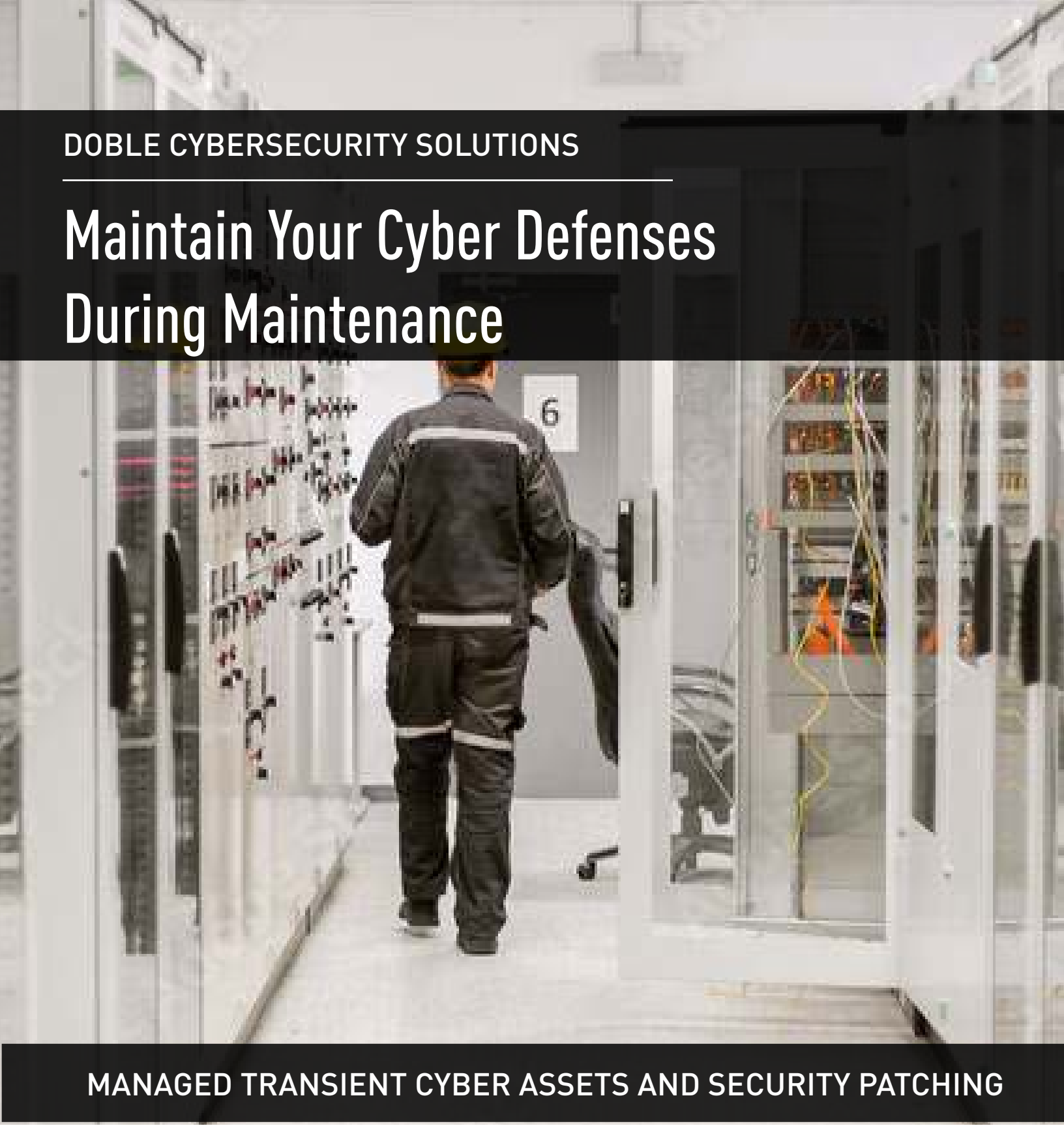
DOBLE CYBERSECURITY SOLUTIONS

Maintain Your Cyber Defenses During Maintenance



MANAGED TRANSIENT CYBER ASSETS AND SECURITY PATCHING

doble®

www.doble.com

SCAN FOR MORE INFORMATION ON DOBLE SECURITY & COMPLIANCE SOLUTIONS.

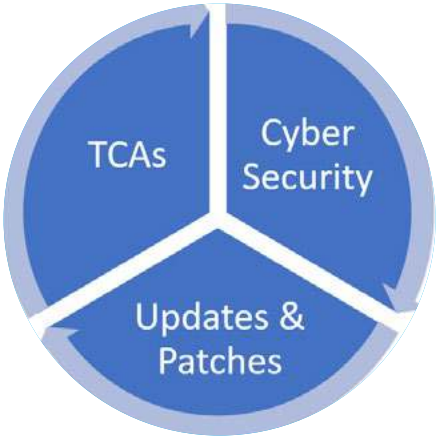
Ensuring Transient Cyber Assets are Managed Efficiently.

DOBLE CYBER SECURITY SOLUTIONS

Robust Defenses | Proactive Support | Efficient Processes

DEFENSE IS PARAMOUNT

Cyberattacks on critical infrastructures impact budgets and resources whether they succeed or not. Countering them requires advanced methods and technologies that can handle increasingly sophisticated and relentless threats. In this environment, robust cyber security is now as critical to electrical system reliability as routine testing and maintenance.



COMPLEX REQUIREMENTS

Laptops used for test and maintenance work in substations are potential cyber security risks. NERC classifies them as Transient Cyber Assets (TCAs) that:

- Must be tracked
- Must collect data safely and securely
- Must protect data even if laptop is stolen
- Must be scanned for malware at regular intervals
- Must only have authorized, scanned and verified software

UNRELENTING BURDEN

In-house TCA security management is difficult, costly and has its limits. IT teams must constantly monitor for security patches to retrieve, review, then apply to their company's TCAs. The updates must be timely to comply with NERC CIP mandates which can necessitate IT outsourcing to keep up with recurring updates that are regularly due on a fleet of TCAs.

Further, typical computer hardening can impede legitimate uses during work processes.

- How will you manage hundreds of field laptops?
- How will you securely transfer data?
- How will you ensure secure test equipment connectivity?
- How will you support latest and legacy software applications needed by test and maintenance workers in the field?
- How will you manage firmware updates, security updates, passwords and security patches?

Manage Security Vulnerabilities

DOBLE CYBER SECURITY SOLUTIONS

HELPING YOU GET AHEAD AND STAY AHEAD

The cyber security solutions from Doble give utilities a platform for field force automation that restores time in the day for professionals who would otherwise face significant operational process and technology challenges on their own.

Doble PatchAssure™ and the **Doble Transient Cyber Asset Program™** provide timely software functional updates and security patches for your applications in use in your fleet of transient cyber asset (TCA) computers. Both programs feature the **Doble Security Portal™** which gives a central location for TCA fleet management that includes administrative controls for reviewing, approving, deploying and reporting on all software or worker transactions affecting TCAs.

EFFICIENT FIELD TESTING

- Advanced hardening that allows support of all software applications and operating systems, new or old, needed for testing Bulk Electric System Cyber Assets (BCAs).
- Provides individual and groups of workers with the complete set of testing applications they need.
- Applications are guaranteed to run, even if requiring older operating systems like XP.
- Ensures consistency of testing applications and versions among users.

ROBUST CYBER SECURITY

- Cyber security that is transparent to the field worker.
- Provides central, efficient security patch, software update and TCA management.
- Secure controls for a least privilege approach providing defense-in-depth.
- Prohibits unauthorized network access.
- Enables quick malicious code detection and mitigation.

AUTOMATED DATA MANAGEMENT

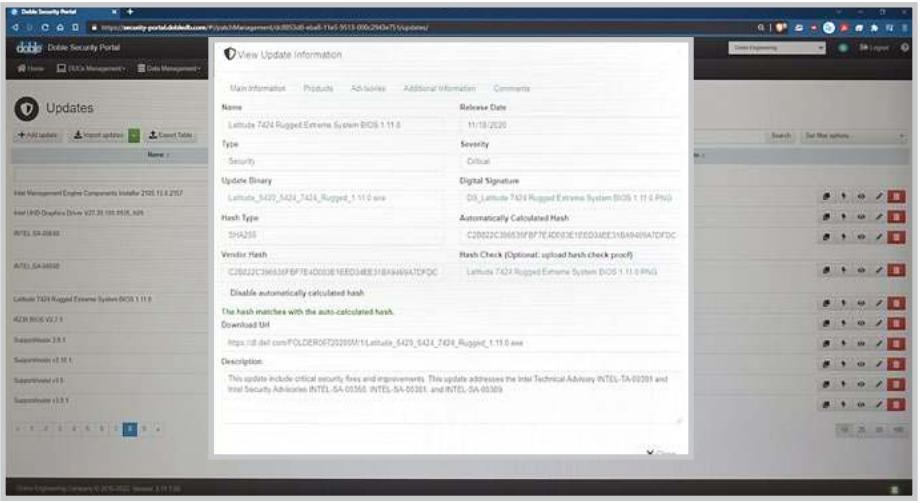
- Automatic compliance readiness - reports are in a central portal.
- Solid platform even as more and more data gets generated.
- Facilitates data in motion and data at rest security.
- Standardizes business processes.
- Uses dobleSYNC™ technologies for automating data transfers.

DOBLE PatchAssure™

PatchAssure is a "one-stop shop" portal-based solution for software version and security patch management. Experts from Doble monitor for the availability of updates from hundreds of sources and provide notice via the Doble Security Portal to utility administrators which includes analytics and recommendations. The multi-factor authentication the Doble Security Portal provides prevents unauthorized access to clients' CIP asset information.

MONITORING

- All asset inventory is checked for patches on a weekly basis
- Software functional update availability for applications
- Advisories concerning patches and updates



ANALYSIS

- Purpose and criticality of patches and updates
- Cyber security vulnerabilities addressed by patches and updates
- Validation of patch and update sources - URLs, RSS feeds, email lists, etc.

QUESTIONS TO ASK

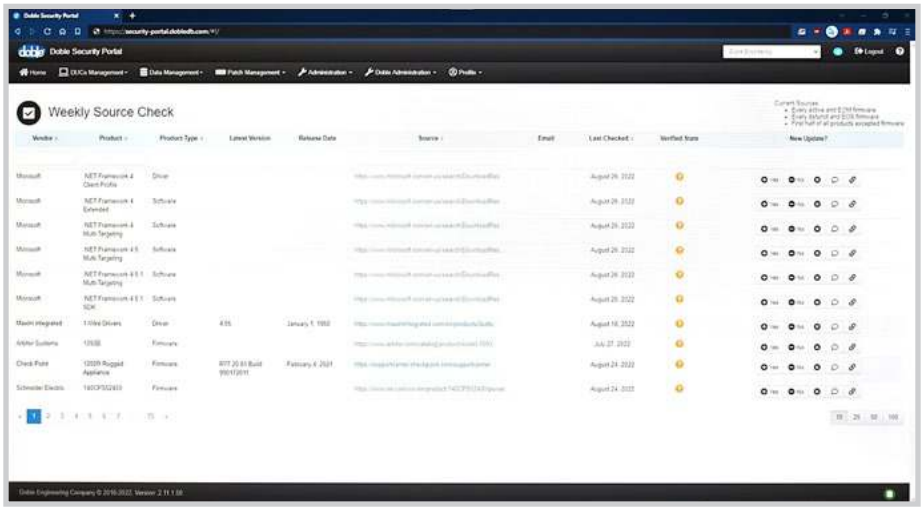
- Does the patch address a security vulnerability or weakness?
- Does the patch offer a new security feature or improved software performance?

VISIBILITY

- Individual decisions on patching/updating and timelines
- Lifecycle of patches and updates - New, Accepted, Scheduled, etc.
- History of patches and updates by product

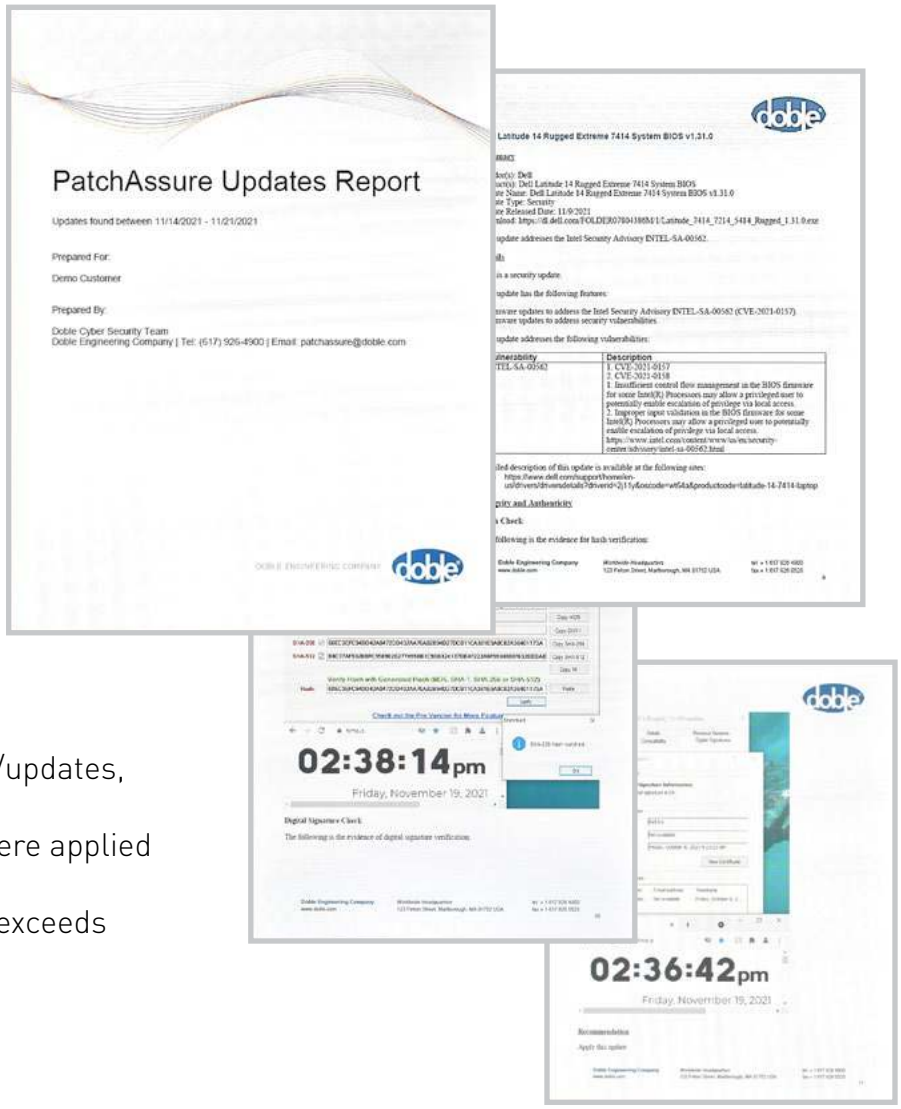
TRACKING

- On-demand access to patch, update, and TCA details
- Workflow actions regarding patches, updates and TCAs
- Management of users and notifications



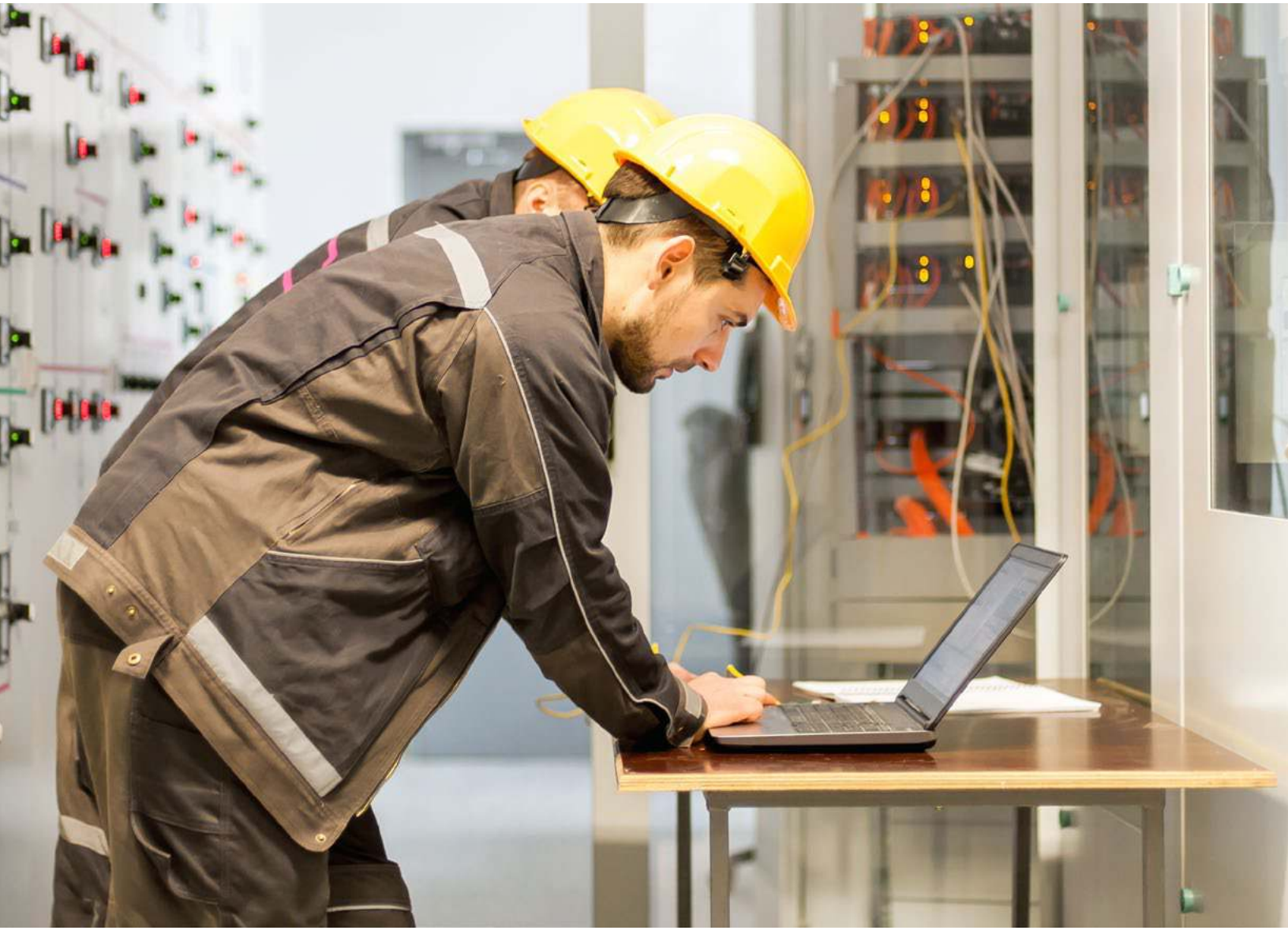
REPORTING

- Weekly report of relevant patches/updates, vulnerabilities, and advisories
- Proof that patches and updates were applied and sources were checked
- Auditable evidence that meets or exceeds NERC CIP requirements



THE DOBLE TRANSIENT CYBER ASSET PROGRAM™

The Doble Transient Cyber Asset Program takes the benefits of PatchAssure and the Doble Security Portal a step further with specially spec'd laptop computers that are ruggedized for field use. Doble TCAs feature cyber security hardening that meets or exceeds NERC standards for transient cyber assets.



Network Mode for secure upload/download operations and live support sessions.

Test Mode for interfacing with cyber devices like computerized protective relays during test and maintenance operations.

Customer Care for on-demand remote support.

DOBLE UNIVERSAL CONTROLLERS — ULTRA RUGGED TCA COMPUTERS

- Dedicated TCA that does not allow email or internet
- Non-disruptive to field workers — supports applications and performs transparent patching/updating
- Convenient app-style interface and custom data/results management
- Live assistance — users can interact with support personnel securely in live sessions
- Sealed doors and compression gasketing for superior device and data protection
- Independently tested to military standards and can withstand 6' drops
- Display is readable in sunlight and low light conditions and features resistive touch that works with gloves on
- Thermal management allows device to be operated in high temperatures
- Long battery life
- Designed to automaticaly work with Doble software products and user administration
- Universal — one device to operate all your test software and test equipment


DUCe Dashboard - DUCE-CJZGDD3
Running Processes
Windows Performance

DOBLE SECURITY PORTAL™

The Doble Security Portal gives administrators of PatchAssure and the Transient Cyber Asset Program accurate information about their TCA fleet and operations in real time. The modern interface provides aggregations of data surrounding the applications and users assigned to TCAs and simplifies software version update and security patch management. Critical details are organized into tabular views that are easy to navigate and comprehensive dashboards present important baseline analytics from the data being tracked.

Simplified TCA and Patch Management

Be confident in all aspects of your TCA program with up-to-the-moment information on the various field devices, images, software applications and versions in use. Be aware of notifications from Doble in real time regarding the integrity of your cyber security defenses so that appropriate interventions can be taken quickly if necessary. Have assurance that the TCAs in your fleet will be updated and patched non-disruptively.

Security Management

- Perform TCA assignments and authorizations
- Monitor unauthorized access
- Monitor security patch application

Data Management

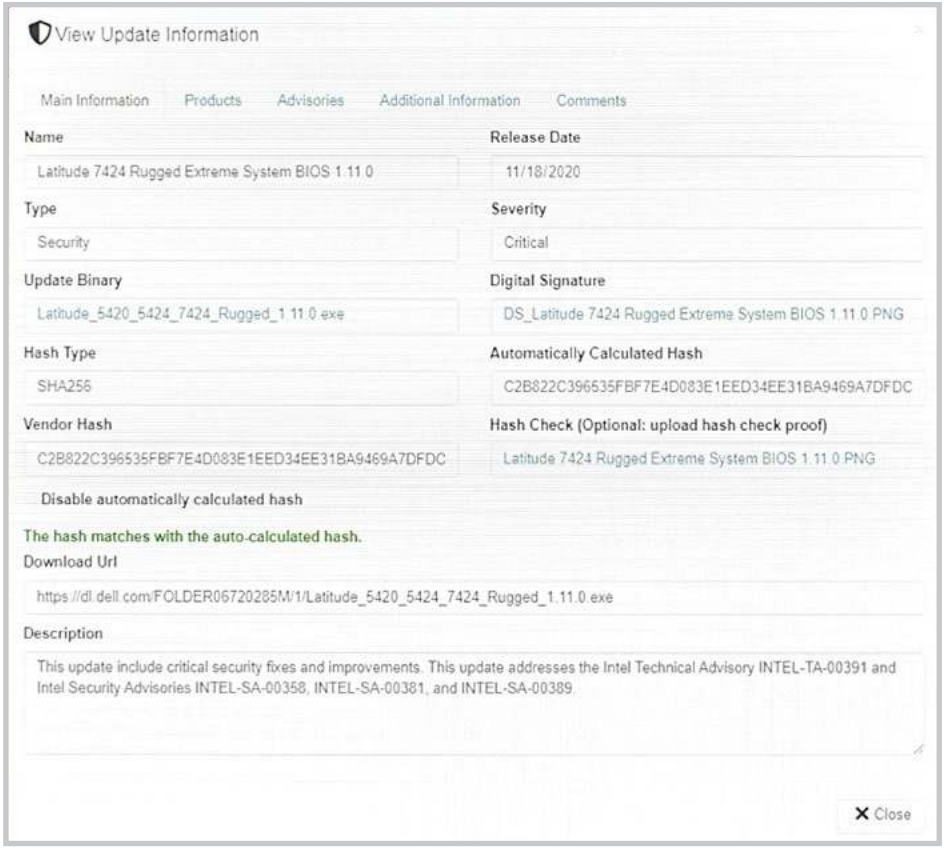
- Disseminate data to TCAs from the portal (e.g., test plans, SOP)
- Monitor data transfer between TCAs and repositories (e.g., settings, test results)

Compliance Management

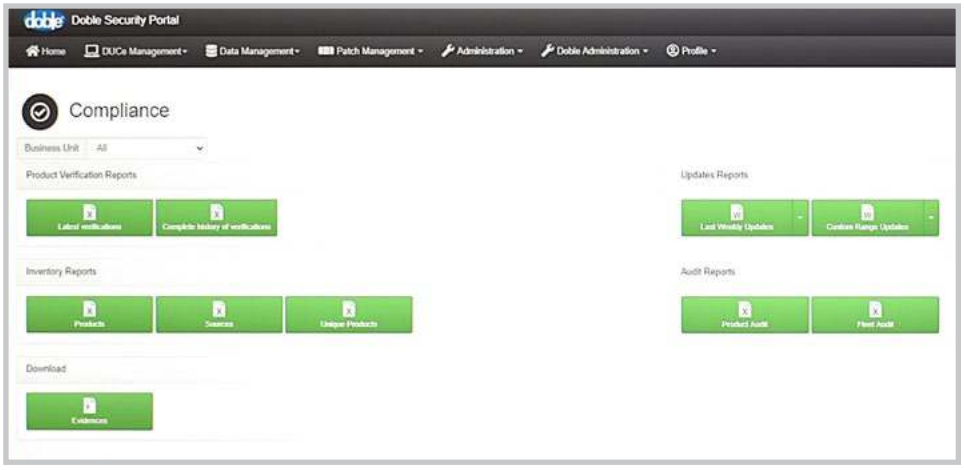
- Monitor software versions, image versions, and any departures from what was approved
- Monitor CIP compliance of individual units
- Obtain reports and evidence for audits

NERC CIP COMPLIANCE READINESS

Let PatchAssure and the Doble Transient Cyber Asset Program improve your compliance stance.



Have important details ready for compliance audits.



Quickly locate and provide required information.

DOBLE PatchAssure

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 TRANSIENT CYBER ASSET PROGRAM

CIP-010-4 R4 - Transient Cyber Assets And Removable Media
Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

1. Applicable only if customer uses removable media on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting.
2. Doble DUC is set up (if required otherwise disabled by default) to only allow or accept customer-verified and approved removable media devices to execute the functions listed above.

CIP-010-4 R4 1.1 - Transient Cyber Asset Management
TCAs must be managed in an ongoing manner to ensure compliance at all times, or in an on-demand manner before connection to BES Cyber Systems, or both.

1. Ongoing management with automated check-in for updates while Doble TCA in Network Mode.
2. On-demand management with procedure checklists when switching Doble TCA to Test Mode.
3. Gold Images are controlled to ensure all TCAs are consistent and compliant.

CIP-010-4 R4 1.2 - Transient Cyber Asset Authorization
Users of TCAs must be authorized individually or by group role; by location individually or by group; and must be limited to what is necessary to perform business functions.

1. Administrators can authorize individual TCA users and user groups as required using the TCA Portal.
2. User and user group locations are easily viewed and managed through the TCA Portal.
3. TCA device capabilities can be limited to only necessary business functions.

CIP-010-4 R4 1.3 - Software Vulnerability Mitigation
Software on TCAs must be up-to-date with latest-available security patches through manual or managed updating via read-only media, system hardening or other method(s).

1. Applies security patching through managed updates provided from a central service.
2. Operating system and software cannot be changed by the user.
3. System hardened by shutting down unnecessary ports and services.
4. TCA Portal shows which TCAs are due for software updates.

CIP-010-4 R4 1.4 - Introduction of Malicious Code Mitigation
Malicious code must be prevented from being introduced by TCAs into BES Cyber Systems by one or a combination of antivirus software, application whitelisting or other method(s).

1. Antivirus software provided which is kept up-to-date through remote updates.
2. Automatic antivirus date checks.
3. Centrally administered software applications.

CIP-010-4 R4 1.5 - Unauthorized Use Mitigation
Unauthorized users must be prevented from using TCAs by one or a combination of restricted physical access, full-disk encryption with authentication, multi-factor authentication or other method(s).

1. Physical access can be restricted through check-in/ check-out.
2. Full-disk encryption is implemented.

CIP-005-7 R1 - Electronic Security Perimeter
TCAs must be prevented from becoming an unauthorized ESP Access Point.

1. Doble TCA Test Mode disables all network communication interfaces for the duration of the test activity.
2. Test Mode and Network Mode are checked for integrity with baseline TCA configuration.

IMPLEMENTING DOBLE CYBER SECURITY SOLUTIONS

Doble manages a large catalog of industry software that continues to expand with each implementation of PatchAssure and the Doble Transient Cyber Asset Program. Any application and operating system, whether already tracked by Doble or not, can be supported within these managed programs.

Experts from Doble consult with your IT/OT team to identify the software applications in use by your company that need to be managed in PatchAssure or the Transient Cyber Asset Program. Every aspect is considered, like the makeup of your field force and the specific applications they require as individuals or as user groups. Your preferences for how you would like to receive patches are configured as well as your gold image.

1.TCA Controllers.
•Doble provided

2.Custom Gold Image:
•CIP security controls
•All the applications you need, configured the way you need it
•Customized to various work groups

3.Secure integration with your infrastructure and work processes.
•Ensure proper TCA interaction with all devices
•Support integration with your infrastructure
•Extensive training
•On-site and remote work with your users to ensure adoption

4.Ongoing Services:
•Project Management meetings
•Discovery, development, test and deployment of security updates every month
•SecOpsteam monitoring security vulnerabilities and updates
•Ongoing TCA training and support

5.Customer Care and 24/7 support

6.Doble Security Portal for management, compliance monitoring, and audit evidence

PatchAssure and the Transient Asset Program are backed by Doble's cross-functional team of security analysts, substation device engineers, network engineers, and protection engineers. Let their expertise and the community of **Security and Compliance User Group** participants help you implement and sustain robust cyber security over your software patches and TCAs in all facets and for any scenario.

DOBLE SECURITY VULNERABILITY ASSESSMENT PROGRAM

- Security best practices from several industry and regulatory standards.
- Frequently assessment by customers in accordance with the US Regulatory Standard NERC CIP 13 Cyber Security - Supply Chain Risk Management.
- Source code examinations using static code analysis tools, reviewed for correctness of function and implementation, and subjected to automated and manual penetration testing.
- Commercial vulnerability scanning tools to test source code and products.
- Doble application developers undergo comprehensive application security training covering OWASP Top 10 application security risks and SANS Top 25 software errors.

Doble Cyber Security Solutions

EXPLORE ALL THE WAYS DOBLE CAN HELP YOU WITH YOUR CYBER SECURITY PROGRAM

- Efficient Field Testing
- Robust Cyber Security
- Automated Data Management
- Compliance Tools
- Hardware
- Customer Service
- Fleet Managment

www.doble.com

Doble Engineering Company
Worldwide Headquarters | 123 Felton Street, Marlborough, MA 01752 USA