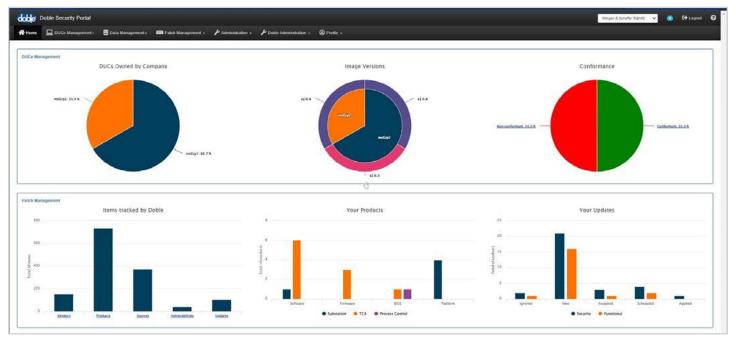
DOBLE CYBERSECURITY SOLUTIONS PatchAssureTM

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 deployments are critical and which devices they affect. Workflow and compliance evidence are 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.



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

- Regular intervals of patch checking for asset inventory
- Software functional update availability for applications
- Advisories concerning patches and updates

deble Online Seconda Postal			14.	and Highware and the	
Characteristics					
	Materialism Protots Advantary Additional Inf				
O Updates	Name Refused Date				
C chuaces	Latterin 1421 Physical General System (BCB 119 B	H118-2026			
+ Add interes Arrest and in the later	Texas	Security	Q\	Date: Dr. Bar marries	
News	Swirts	08.4	United and Links		
and the	Update Divery	Ogtal Synatore	Thrms-Saul-		
	140000 (42); (424,7434,00000); 11.2 eve	235, Latitude 2222 Flagged Calance Psychol (202) 1 112 (195)			
Ind Recommendings of Community, South 2018, 1987-291	Hank Type	Hands Type Automatically Consumed Halls		# A	11
Date (HD) Grannes (Door VIT H) 100.0126, 609	aveau controlmente controlmente			HIRPH AND A	
	Wendow Really	Heads Check (Optional upload heads check proof)			
state de trojad	EXECUTION NUMBER OF A DAMAGE PERSON AND A DAMA	100			
	Enable accountedly (souther) heat				
9192 & 2019	The lash worthin with the percentil class family. Coverball UK			1	
Lations 7424 Property Street System (1999) 1 710	Maps of Average 712,211007022004.11.40.49, 5222,5423,74	https://distroconfindiment/0200000000000000000000000000000000000			-
	Overlytter	Deschiller			
ACCOMPTANTS, 1	This spatie include seture boy and improvement. This spaties editories the total Technical Advance (NTEL TV-00001 and		in	a	
Supplicat (11)	And beauty Alexandra Mills, Sciences (Mills, Sciences), and S	Max Decade Advances WITEL ST-00016, WITEL GI-000191, and WITEL GI-00000.			
Supervised V/10 Y					10
Support and a S. S.		X Core			-
Superline of \$7.	billion from the second		-	1	

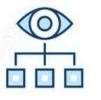
QUESTIONS TO ASK

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



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.



VISIBILITY

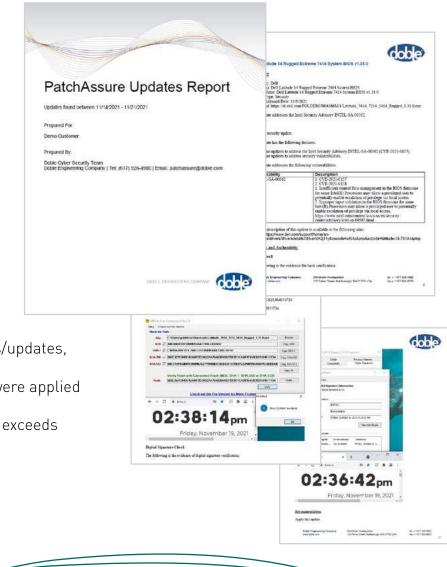
- Individual decisions on patching/updating and timelines
- Lifecycle of patches and updates New, Accepted, Scheduled, etc.
- History of patches and updates by product



TRACKING

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

diale Done :	Security Portal								frides (high-sering	4		Die stande 11
1		Data Management +	100 Pakit Materier	e Planate	- Finishingan - Citatio -				- 7-u	- 1		
🖸 Wee	kly Source C	heck	==							very diffee	at land t	M Amerikan OS Roserana Os konsepted Same
Smaller -	Finished -	Fristan Type -	Latest Version	Nalagan Late	Searce -	Local	Last Cliei And /	Nerdiec State		w Update	i	
Merraelf.	NET Formwork 8 Deer Profes	Dree			Tiga Trave streads and a wire a second contraction		Aquit 21, 2022	0	0 - 0	~ 0	p	8
Microsoft	JRT Formatik 4 Entertied	Subrans			that there involves the solar defined as Pre-		August 21, 2022	•	0 - 0	- 0	0	8
Record	NET Framework & Math. Torquelling	Schore			the interning only a last house of a		August 25, 2022	0	0 0	- 0	D.	0
Manaelt	NET Planaurank 4.5 Utan-Tergelling	Silver			High lines minimal contribution (NOvoil) alline .		Aspet25 2022	0	0-0	~ 0	ø	
Mariant	AET Promovale AEL1 Math-Tempeting	Solution			tiga loos minut and a last to barre to		August 24, 2022	•	0- 0	- 0	p	
Herrard	XET Transont 451 XXX	Schow			the loss stand and a sharehowing an		Page#28 202	•	0 - 0	~ 0	P	8
Nace mag cod	1-Value Delvan	Driver	- 435	28nary 1, 1998	ingle linear work throught a more produce that		August /0.2022	0	0 - 0	~ 0	φ.	8
Arlobar Systeme	19930	Firmum			The two at the contractory observable (CO)		Alty 27, 2012	0	0- 0	-	ρ	
Dailt Poet	COUR Report Applices	Ferman	8077.20.01 Guilet 8901.072631	February 4, 2023	The importants declarate processes to		August 24 2022		0 - 0	~ 0	p.	0
Streets Date:	140CP112128	/music			The market of the second s		Agirlis 201	•	0 - 0	~ 0	D	8
		10.1									-	1.00 (ME] 10





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

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:

Coble Security Portal					
😤 Home 📃 DUCe Management - 🛢 Data Management - 💷 Patch Management - 🗡 Adminis	ration - 🅜 Doble Administration - 🛞 Profile -				
Compliance Business Unit All ~					
Product Verification Reports	Updates Reports				
Latest verifications	Last Weekly Updates Custom Range	Updalm			
Inventory Reports	Audit Reports				
Perduchs Example Contracts	Product Austit Field				
Download					
Evidences					
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.	 Patch sources are documented and also monitored for availability of patches. Patches retrieved are analyzed for applicability and recommendations are given per classification criteria being met. Patch sources are checked weekly. 				
CIP-010-3 R1 1.6 - Configuration Change Management and Vulnerability Assessments Software being patched must be verified for integrity and the source must be identified.	 Patch integrity verifications are performed. Patch sources are identified. 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: JULY 2023