ICS PATCHING-AS-A-SERVICE:

Transforming Risk into Operational Resilience

DEXCENT.COM | (833) 482-4100 | SALES@DEXCENT.COM

INTRODUCTION:

The Unseen Battleground of Industrial Control Systems

In the intricate world of industrial operations, where uptime is paramount and every system underpins real-world processes, from power generation to manufacturing, patching is rarely just a technical task. It's a strategic decision fraught with consequences. These aren't just web servers or office desktops; they are control systems regulating pipelines, assembly lines, and electrical substations. For these environments, downtime isn't a nuisance; it's a significant cost, and mistakes can have far-reaching implications, impacting safety, compliance, and continuity.

Many operational teams, acutely aware of these stakes, approach patching with extreme caution, often delaying or avoiding it altogether. Over time, this caution can unfortunately morph into complacency. Months pass, vulnerabilities accumulate, and what was once a risk-managed delay becomes a systemic exposure.

Organizations caught in this dilemma often face familiar challenges: critical vulnerabilities remain unaddressed, auditors raise red flags during compliance reviews, and security teams struggle to align priorities with operational counterparts. Change control processes, if they exist, often slow everything down. It's not that industrial organizations don't care about patching; it's that traditional IT-centric approaches simply don't fit the unique realities of the operational world.

This is where **Patching-as-a-Service** from Dexcent emerges as a vital solution. This service offers a paradigm shift, introducing structure, reducing risk, and restoring control to a process that has historically been a source of immense burden and uncertainty. This ebook will explore the unique challenges of OT patching, demonstrate how Patching-as-a-Service successfully addresses them through real-world examples, and outline what to look for in a trusted partner like Dexcent to guide your journey toward operational resilience.

CHAPTER 1

The High-Stakes Reality of OT Patching

Operational Technology (OT) environments present a unique and complex set of challenges when it comes to patching. Unlike agile IT systems designed for frequent updates, OT systems are built for availability, stability, and longevity. Every change, no matter how small, can introduce instability or worse, directly impacting critical operations.

The key constraints in OT environments that elevate the stakes of patching include:

- **System Fragility:** Many industrial control systems were never designed with regular updates in mind. Applying untested patches in the OT environment can lead to critical SCADA and DCS applications failures, risking production halts or even safety incidents.
- **Legacy Technology:** Industrial environments often house systems that are decades old, running outdated or unsupported software. This makes them highly susceptible to modern cyber threats.
- **Availability-First Culture:** The core mandate of OT is continuous operation. Patching often requires taking systems offline, which is an unacceptable option for 24/7 operations without meticulously planned maintenance windows. The cost of unplanned downtime in industrial environments is significant (both financially and operationally), creating strong disincentives for preventive maintenance, even when it's necessary for long-term resilience.
- **Layered Networks:** Industrial networks are typically segmented into tightly controlled zones (e.g., Purdue Model), each with its own permissions, industrial communication protocols (like EthernetIP, MODBUS, DNP3), and security considerations. Patching across these segmented layers requires specialized control systems knowledge and careful coordination.
- **Limited Test Environments:** Unlike IT, many OT environments lack safe, mirrored test environments to validate patches before deployment to production. This absence of a sandbox for testing significantly increases the risk of unforeseen operational disruptions.

All these factors combine to create immense pressure to demonstrate due diligence in Cyber Security. Patching in OT is intrinsically linked to mitigating cyber risks, which ensures attack-resistant, safe operations and adherence to stringent regulatory compliance.

CHAPTER 2

Why Traditional Patching Fails Industrial Teams

The struggle with OT patching isn't due to a lack of care or understanding within industrial organizations. It's primarily because the traditional, often IT-driven approach to patch management is fundamentally overwhelming and ill-suited for the OT environment.

Common challenges that lead internal teams to struggle include:

- **Resource Constraints:** Patching in OT demands significant time, specialized tools, intricate coordination, and constant oversight, resources that many operational teams simply cannot afford. Teams are often stretched thin, focused on keeping systems running, supporting operators, maintaining uptime, and troubleshooting immediate issues. Patching, especially for undocumented or unsupported systems, often gets pushed to a lower priority.
- **Fear of Unintended Consequences:** Applying a patch without a comprehensive understanding of its full impact can lead to system failures, loss of process visibility, or even production outages. This inherent risk creates a strong disincentive for teams to perform updates, leading to a backlog of vulnerabilities.
- **Lack of Specialized Tooling:** Many ICS environments lack the dedicated patch automation or inventory systems found in IT. Teams often rely on manual processes, spreadsheets, or "tribal knowledge," making the process inefficient, error-prone, and difficult to scale.
- **Organizational Silos and Disconnection:** Engineering, Operations, Cyber Security, and Compliance teams often have different views of risk and distinct priorities. This lack of alignment can slow down or halt patching initiatives, as each function grapples with its own concerns without a unified strategy.

In this context, patching becomes a liability, a source of stress, and a task that is frequently deferred because the perceived risks of performing it seem as high as the risks of neglecting it. This "wait-and-see" approach only works until it doesn't, leaving organizations increasingly vulnerable.

CHAPTER 3

Patching-as-a-Service:

The Path to Predictable Protection

FORTUNATELY, PATCHING DOESN'T HAVE TO BE A CHAOTIC BURDEN.

It doesn't have to feel like an intrusion or a scramble. When managed deliberately, within a structured process that aligns with operational realities, patching transforms into something else entirely: a visible sign of control, a system of record, and a confidence-building measure that demonstrates risk is being actively addressed, not ignored.

DEFINING PATCHING-AS-A-SERVICE IN INDUSTRIAL CONTEXTS

Dexcent's Patching-as-a-Service offers a paradigm shift from reactive, manual patching to proactive, automated vulnerability remediation specifically tailored for Industrial Control Systems (ICS) and OT environments. Unlike traditional IT patch management, OT-focused patch management integrates specialized workflows for:

- **Legacy Equipment:** Addressing the unique needs of older systems.
- **Safety System Validation:** Ensuring updates do not compromise critical safety functions (often adding 14-21 days to typical patch cycles).
- **Maintenance Window Optimization:** Strategically planning deployments to align with planned operational downtime.

The service encompasses end-to-end processes, from vulnerability detection through patch deployment verification, combining cutting-edge software automation with industrial Cyber Security expertise. This specialization helps reduce the likelihood of unplanned downtime by introducing structure, consistency, and repeatability - key elements that manual and ad hoc methods often lack. It allows industrial organizations to better align cyber security requirements with the realities of operational continuity.

The shift to Patching-as-a-Service changes the equation by introducing a rhythm and a cadence. Instead of one-off, reactive cycles driven by emergencies or compliance deadlines, organizations can operate with a predictable patching plan, one built around their schedule, their people, and their unique industrial environment. This approach provides a process designed to fit alongside the customer's existing change control and documentation standards, enhancing them rather than replacing them. Where documentation is incomplete or out of date, Patching-as-a-Service brings much-needed structure.

Ultimately, what organizations gain isn't just patched systems; it's peace of mind. They gain the ability to speak with clarity during audits, significantly reduce the risk of silent vulnerabilities accumulating in their environments, and bring operations, engineering, and Cyber Security teams into alignment around a shared, manageable process. In complex environments where the stakes are high, this clarity is invaluable.

CHAPTER 4

Real-World Impact:

Case Studies in Patching-as-a-Service Success

THE TRUE VALUE OF ICS PATCHING-AS-A-SERVICE EMERGES WHEN APPLIED IN MISSION-CRITICAL, REAL-WORLD OT ENVIRONMENTS.

Dexcent's recent work with two major oil and gas pipeline operators illustrates how structured patching programs deliver measurable improvements in compliance, coordination, and operational confidence.

CASE STUDY 1:

CANADIAN PIPELINE OPERATOR GAINS CONTROL OVER SCADA PATCH CYCLES

Context: A Canadian operator required cyclical patching of SCADA systems to meet internal risk and compliance requirements. However, patching windows were frequently overrun, and internal SCADA support resources were burdened with competing operational priorities.

Solution: Dexcent implemented a multi-phase patching program including environment onboarding, non-production validation, live production deployments, and cycle-close reporting. All patches were coordinated with the SCADA vendor's approval process, ensuring technical compatibility and operational continuity.

Outcome: Dexcent's involvement stabilized patching schedules, allowed internal teams to refocus on high-priority production support, and delivered each cycle at a predictable, fixed cost.

CASE STUDY 2:

NORTH AMERICAN PIPELINE OPERATOR ACHIEVES >95% PATCH COMPLIANCE

Context: In response to TSA requirements, the client needed to patch thousands of OT assets quarterly, within 70 days of patch release. Internal capacity and existing processes could not support the frequency, scale, or precision required.

Solution: Dexcent embedded within the client's infrastructure teams to develop standardized playbooks, enhance change control processes, and execute quarterly patch cycles. Microsoft MECM and scripting were used for automation, while white-glove patching was reserved for high-availability systems.

Outcomes: The client achieved patch compliance exceeding 95% each cycle. The program remains sustainable, auditable, and scalable across growing asset inventories and SCADA domains.

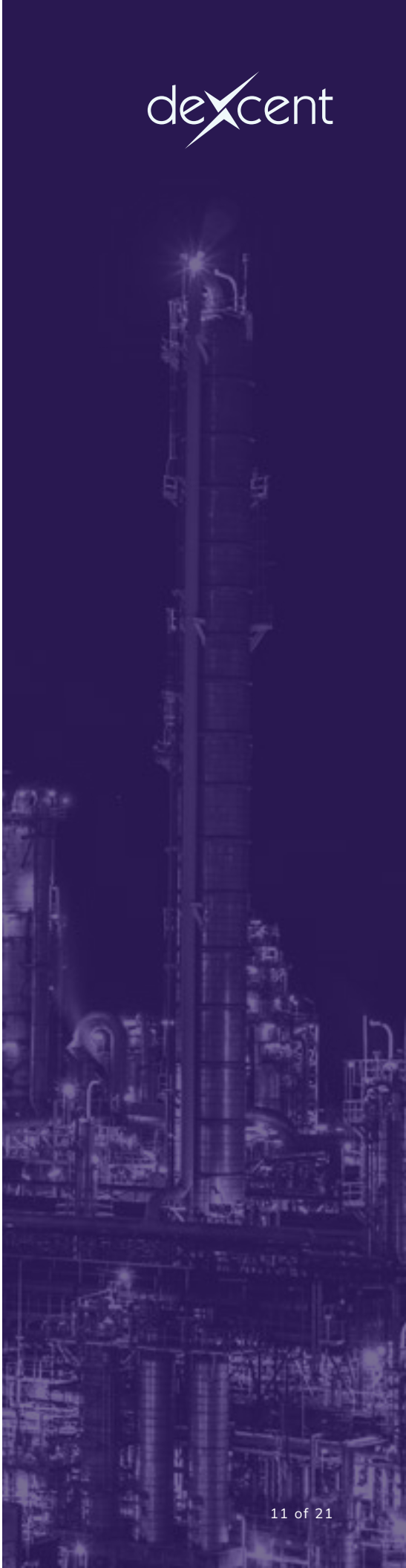
CROSS-CASE ANALYSIS:

KEY PATCHING-AS-A-SERVICE SUCCESS FACTORS

These case studies, and others, highlight several recurring success factors in industrial Patching-as-a-Service implementations:

1. **Operationally Aligned Planning:** Successful programs are built around the cadence of industrial operations. Rather than forcing IT-centric patch cycles, Patching-as-a-Service adapts to operational rhythms, respecting production windows, integrating with SCADA vendor certification cycles, and aligning with Management of Change (MOC) processes.
2. **Structured, Phased Methodology:** Predictable results come from repeatable structure. Each Dexcent engagement follows a multi-phase approach, beginning with planning and validation in non-production domains, progressing to carefully coordinated production rollouts, and concluding with post-patch reporting and lessons learned. This phased discipline ensures consistency across cycles and facilities.
3. **Integrated Validation and Rollback:** A patch is only as successful as its post-deployment behaviour. Dexcent engagements emphasize thorough pre- and post-patch validation at the system and service levels. Where high availability is required, rollback protocols are pre-established, ensuring minimal risk to live operations.
4. **Automation Where Appropriate, Expertise Where Essential:** Automation accelerates coverage, but it doesn't replace judgment. Dexcent uses tools like Microsoft MECM and custom scripting to manage scale, while applying hands-on expertise for environments where automation is either unfeasible or unwise, such as legacy systems or high-availability clusters.
5. **Clear Ownership and Accountability:** A key to Dexcent's success is defining responsibility across stakeholders. Daily standups, patch window coordination, and centralized documentation allow both Dexcent and client teams to work in lockstep, minimizing ambiguity and maximizing accountability.
6. **Strategic Resource Relief:** By handling the end-to-end patching lifecycle, Dexcent relieves internal OT teams from the operational drain of planning, executing, and validating each cycle. This allows in-house experts to focus on high-priority production support and longer-term infrastructure projects.

These examples underscore how Patching-as-a-Service provides a structured, predictable, and highly effective solution for industrial organizations seeking to fortify their Cyber Security defenses while maintaining uncompromised operational excellence.



CHAPTER 5

Choosing Your Partner:

What to Look for in a Patching-as-a-Service Provider

DEXCENT.COM | (833) 482-4100 | SALES@DEXCENT.COM

GIVEN THE UNIQUE SENSITIVITIES OF OT ENVIRONMENTS, SELECTING THE RIGHT PATCHING-AS-A-SERVICE PARTNER IS CRITICAL.

Not all providers are equipped to navigate the complexities of industrial systems, and choosing the wrong one can actually increase risks rather than reduce them.

If your organization is considering a Patching-as-a-Service model, here are a few critical qualities to look for in a partner:

- **OT-Native Experience:** Does the provider truly understand the operational technology environment? ICS environments are not merely extensions of IT; they are purpose-built, often fragile, and demand an intimate understanding of safety, redundancy, and control mechanisms. Look for a partner with proven experience in industrial settings, not just IT.
- **Vendor-Agnostic Approach:** Your industrial environment likely comprises systems from multiple vendors, often layered with decades of customizations. A truly effective Patching-as-a-Service provider should focus on protecting your existing architecture, rather than pushing proprietary solutions or trying to force a "one-size-fits-all" approach that disrupts your established systems.
- **Structured Change Management:** A reliable partner respects your internal processes. They should work within your existing change control systems, build in robust rollback procedures, and never take shortcuts that could jeopardize operational stability. Transparent, meticulous documentation of every patch (what was changed, why, and how it was tested) is essential for security, operational integrity, and audit readiness.
- **Transparent Documentation:** Every patch applied should be tracked and documented meticulously. The provider should clearly outline what was changed, why it was changed, and how it was tested. This isn't just about security; it's about ensuring operational integrity and being fully audit-ready.
- **Collaborative Engagement Style:** The right partner doesn't just "perform a service." They build relationships, contribute valuable insights, and work as a seamless extension of your team. This collaborative approach fosters the kind of trust that is essential when dealing with systems of such critical importance.

CHAPTER 6

The Dexcent Advantage:

Your Trusted Guide to OT Security

DEXCENT.COM | (833) 482-4100 | SALES@DEXCENT.COM

At Dexcent, we understand that every industrial environment operates to its own rhythm, with unique constraints and complexities. Our role isn't to overwrite these critical operational realities; it's to integrate seamlessly within them. Our approach to Patching-as-a-Service is built on a fundamental principle:

MEET OPERATIONS WHERE THEY ARE, BUILD TRUST, AND DELIVER SECURE, REPEATABLE RESULTS.

ALIGNED, NOT IMPOSED

Dexcent doesn't bring a rigid "one-size-fits-all" process. Instead, we begin by thoroughly learning how your systems are structured, how your teams operate, and how changes are currently managed. From there, we work within your existing framework, integrating with your schedules, your approval workflows, and your internal stakeholders.

Where your processes are already well-defined, we follow them, adding our experience and oversight to ensure they are maintained and continuously improved. Where gaps exist, we help fill them, leveraging our extensive experience to identify friction points, offer improvements, and introduce efficiencies that increase confidence and control over time.

PHASED AND PREDICTABLE

Our ICS Patching-as-a-Service engagement follows a structured, phased approach, ensuring predictability and minimizing disruption. Each engagement includes:

1. **ASSESSMENT AND PLANNING:**
    a. **Asset and Inventory Analysis:** Comprehensive discovery and baseline of in-scope OT operating system-based assets (Microsoft and/or Linux). This ensures a complete and accurate understanding of your environment.
    b. **Vulnerability Triage and Prioritization:** Cross-referencing asset data with the National Vulnerability Database (NVD) and OEM advisories to identify vulnerabilities. We then prioritize patches based on risk and impact, weighting operational impact higher than IT systems.
    c. **Risk-Based Patch Planning:** Development of a detailed, risk-based patch plan tailored to your specific environment and operational constraints.
2. **TESTING AND VALIDATION:**
    a. **System Environment Staging:** Preparation of mirrored or alternate test environments for "Test, Development, Decision Support, Production" that accurately replicate production systems. This is where patches are rigorously tested to validate functionality and ensure they do not disrupt ICS operations.
    b. **Patch Testing and Approval:** Validation of patches in the controlled test environment, followed by obtaining all necessary Management of Change (MOC) approvals from the customer before deployment.
3. **DEPLOYMENT AND VERIFICATION:**
    a. **Scheduled Deployment:** Implementation of patches according to the agreed-upon deployment schedule and MOC processes, typically starting with non-production environments before moving to production systems (Primary and Secondary).
    b. **Post-Deployment Verification:** Meticulous verification of successful patch installation and functionality of critical applications on each patched system.
    c. **Monitoring and Reporting:** Continuous monitoring of systems for 24 hours post-deployment for any issues, and generation of regular reports on patch status and compliance.
4. **DOCUMENTATION AND COMPLIANCE:**
    a. **Comprehensive Reporting:** Generation of detailed reports and audit trails that meet regulatory requirements and evidence requirements, which significantly cut compliance preparation time.
    b. **Process Enhancement:** Identification and updates to existing Patch Process Procedure documentation and the customer's ICS patch management plan to incorporate new procedures and environmental changes.

This transparent, deliberate process is driven by a cadence that respects both the urgency of cyber security and the realities of production.

BUILT FOR TRUST

Dexcent's clients operate in high-stakes industries, from Tier 1 operators with complex redundancy schemes to mid-sized companies implementing basic governance. Our teams deeply understand what it means to earn trust over time. We invest in improving what's already working, helping clients enhance their documentation, closing process gaps, and increasing readiness for audits and incidents alike. Our experienced patching service analysts apply lessons learned across multiple customer environments, ensuring focused expertise and consistent outcomes.

CHAPTER 7

Taking the First Step:

A Clear Path Forward

DEXCENT.COM | (833) 482-4100 | SALES@DEXCENT.COM

The first step toward transforming your OT patching from a burden into a source of confidence isn't about jumping into immediate action; **it's about building clarity.**

When you engage with Dexcent for ICS Patching-as-a-Service, we begin with a structured, yet low-risk discovery phase designed to comprehensively map out your environment, understand your specific goals, and identify precisely what's needed to move forward confidently.

WHAT YOU CAN EXPECT DURING THE DISCOVERY PHASE:

- **Introductory Alignment Session:** A foundational meeting to align objectives, expectations, and the overall scope of the engagement.
- **Asset Inventory Review:** A collaborative assessment of your existing OT asset inventory to identify all in-scope cyber assets and their characteristics.
- **Vulnerability Snapshot:** A high-level overview of current vulnerabilities within your environment, providing a preliminary understanding of critical areas.
- **Change Control Process Review:** An examination of your current change control procedures to ensure seamless integration and adherence to your operational standards.
- **Preliminary Roadmap:** Development of an initial plan outlining recommended next steps and a strategic direction for your patching program.

SAMPLE DELIVERABLES FROM THE DISCOVERY PHASE:

- **Simplified Asset Map with Patch Status Indicators:** A clear visual representation of your key OT assets, highlighting their current patch status.
- **Prioritization Matrix for High-Risk Systems:** A preliminary framework to identify and prioritize patching efforts based on the criticality and risk profile of your systems.
- **Summary Report outlining next-step recommendations:** A concise report detailing the findings of the discovery phase and actionable recommendations for your tailored Patching-as-a-Service journey.

This initial phase is your opportunity to clarify the scope, reduce unknowns, and build a shared foundation for action, whether you choose to move forward immediately or plan for a later date.

CONCLUSION

Securing Tomorrow's Industrial Landscape Today

DEXCENT.COM | (833) 482-4100 | SALES@DEXCENT.COM

IN OPERATIONAL ENVIRONMENTS, UNPREDICTABILITY TRULY IS THE ENEMY.

Every hour lost to downtime, every patch delayed by uncertainty, and every vulnerability left unresolved adds unacceptable risk to safety, to compliance, and to continuity.

Patching doesn't have to be chaotic. It doesn't have to feel like an intrusion or a scramble. When managed through a deliberate, structured approach, it becomes an integrated part of a resilient operation. That's what Patching-as-a-Service is ultimately about. It's not just about keeping systems updated; it's about reducing uncertainty, creating repeatable rhythms, and aligning operational excellence with security best practices, all in a way that profoundly respects your environment, the people who operate it, and the high standards they uphold.

Whether you're leading an operations team, overseeing critical infrastructure, or managing enterprise risk, the goal remains the same: to protect what matters most without disrupting it. If patching has become a burden in your organization, or if it has fallen behind despite your best intentions, there is a clear path forward. One that's steady, measured, and grounded in extensive experience.

And it begins with a conversation.

Partner with Dexcent today to secure your OT systems and ensure smooth, confident operations.

dexcent

(833) 482-4100 | DEXCENT.COM | SALES@DEXCENT.COM