2025 WHITEPAPER

Transforming the energy industry’s critical processes through workflow automation

tines TRACE3

Contents

- Foreword
  — Executive summary

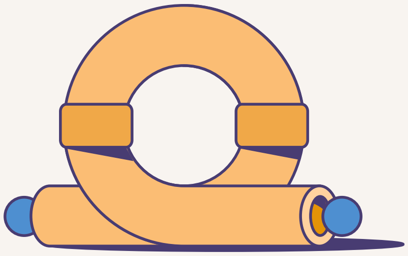
- Key challenges
  — Risks and impact

- Common challenges
  — Cyber security threats
  — Operational Technology (OT)
  — Supply chain security

- Benefits
  — Improved security posture
  — Increased operational efficiency
  — Compliance and regulatory assurance
  — Enhanced resilience and reliability
  — Choosing a workflow automation solution

- Use cases

- Conclusion



Introduction

“The risks are immense — a security breach can risk lives, cost millions, and disrupt critical infrastructure.

FOREWORD BY MICHAEL FARNUM ADVISORY CISO AT TRACE3

In 25+ years of helping organizations build robust cybersecurity programs, I’ve seen firsthand how high the stakes are in the energy sector. As an energy sector professional, you’re likely facing increasing pressure to maintain operational efficiency while safeguarding against ever-evolving security threats. The risks are immense — a security breach can risk lives, cost millions, and disrupt critical infrastructure.

Balancing operational efficiency with the ever-evolving landscape of cybersecurity threats demands vigilance and smart, scalable technology solutions. With the complexity of the energy industry’s IT, Security, and Operational Technology (OT) environments, leaders must ensure their systems are adaptable to present and future challenges.

That’s where workflow orchestration and automation enter. I’ve watched the right automation tools transform security processes, bridging the gaps between IT and OT and optimizing complex processes. Workflow automation doesn’t just address today’s threats - it lays the groundwork for ongoing resilience, enabling security teams to move from a reactive to a proactive approach.

Through Trace3’s partnership with Tines, we’ve shown how automation drives greater efficiency, security, and visibility in industries that rely on uptime and operational integrity. In the energy sector, where downtime and security breaches can have far-reaching consequences, the ability to orchestrate and automate isn’t just advantageous — it’s essential.

This white paper demonstrates the critical role workflow automation plays in enhancing your organization’s security posture, protecting your assets, optimizing your operations, and ensuring compliance with evolving regulations. It examines the unique challenges faced by the energy sector and explores specific use cases that offer practical solutions to those challenges.

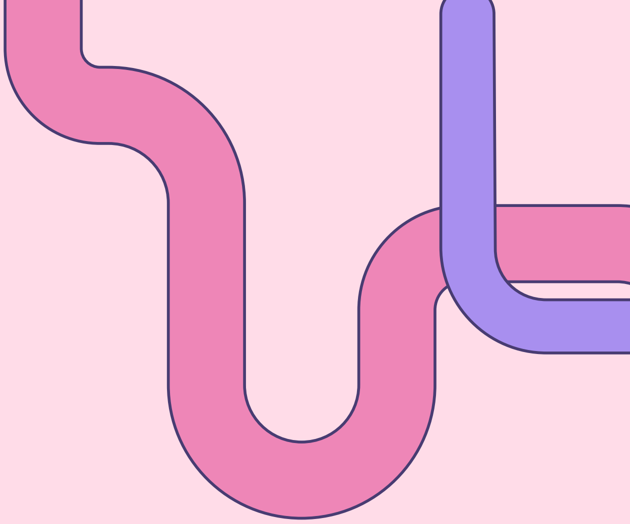
As the energy sector continues to evolve, embracing workflow orchestration and automation will be key to staying ahead of emerging risks and maintaining operational excellence. A robust automation program helps build resilience and reliability in a rapidly-changing landscape.

EXECUTIVE SUMMARY

The energy sector relies heavily on advanced systems for exploration, extraction, refining, and distribution processes. These systems are critical for ensuring safety, availability, and operational efficiency in highly complex and hazardous environments. However, they face unique challenges and risks that must be addressed to maintain seamless operations.

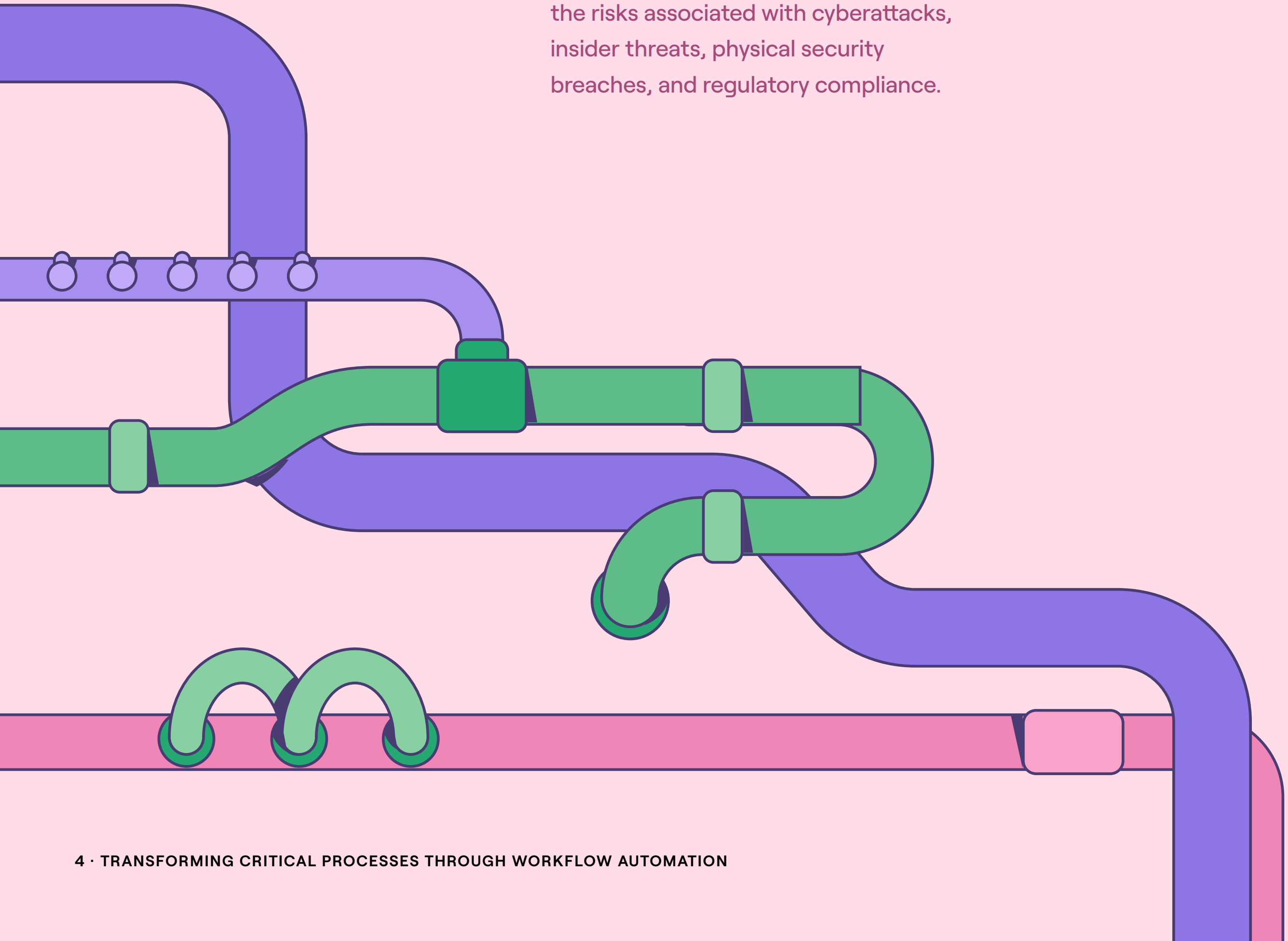
Workflow orchestration and automation offers robust solutions to mitigate these risks, enhance security, and optimize operational efficiency. This white paper outlines how the right workflow orchestration and automation solution can effectively address these pain points, ensuring safe, continuous, reliable, and secure operations.

Key challenges of the energy sector

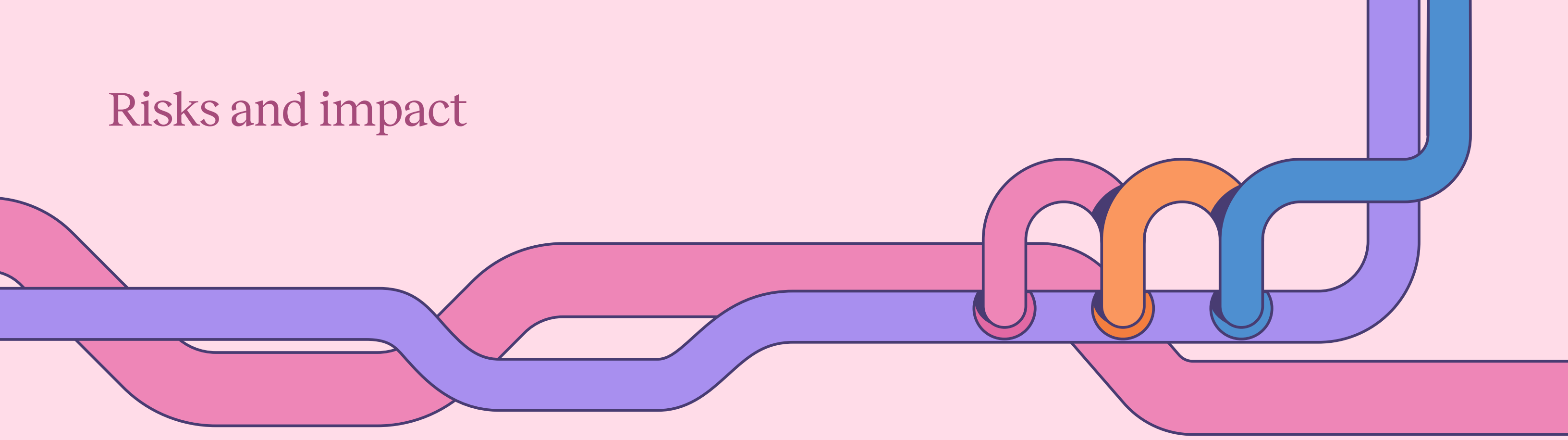


The energy sector, essential for controlling critical infrastructure and industrial operations, faces significant challenges due to its unique nature. These systems often run on legacy technology, are fragmented and complex, and require high availability, making them difficult to secure and manage. Additionally, the lack of visibility and interoperability, combined with a shortage of skilled professionals, exacerbates the risks associated with cyberattacks, insider threats, physical security breaches, and regulatory compliance.

The sector also faces specific challenges such as harsh operating conditions, remote locations, critical infrastructure vulnerability, and stringent regulatory compliance. Addressing these challenges is crucial for ensuring the security, efficiency, and reliability of operations.



Risks and impact



$4.72m

average cost of an incident for the energy sector

90%

of the worlds' top energy companies experienced a data breach in 2023

60%

of the breaches resulted from phishing attacks

FINANCIAL IMPACT

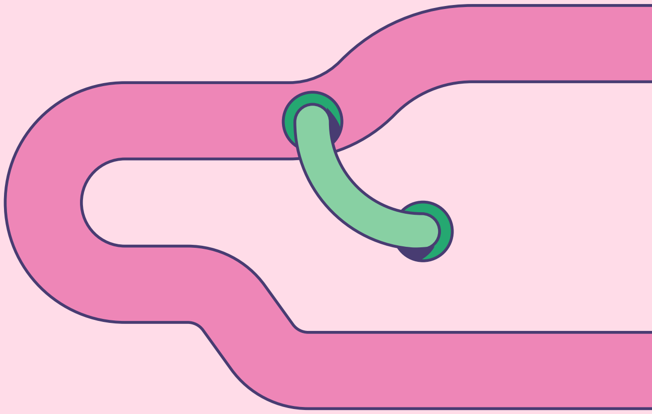
The energy sector faces an average cost of $4.72 million per cyber incident, which includes direct costs like hiring security experts and indirect costs such as reputational damage and lost revenue. (source: International Energy Agency)

HIGH INCIDENTS OF BREACHES

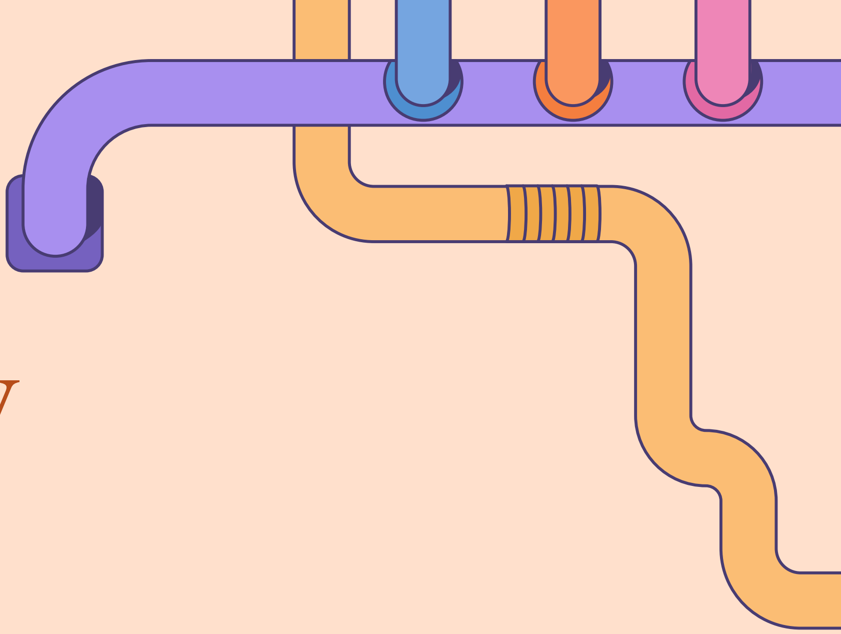
In 2023, 90% of the world's top energy companies experienced third-party data breaches. (source: IBM Security Intelligence)

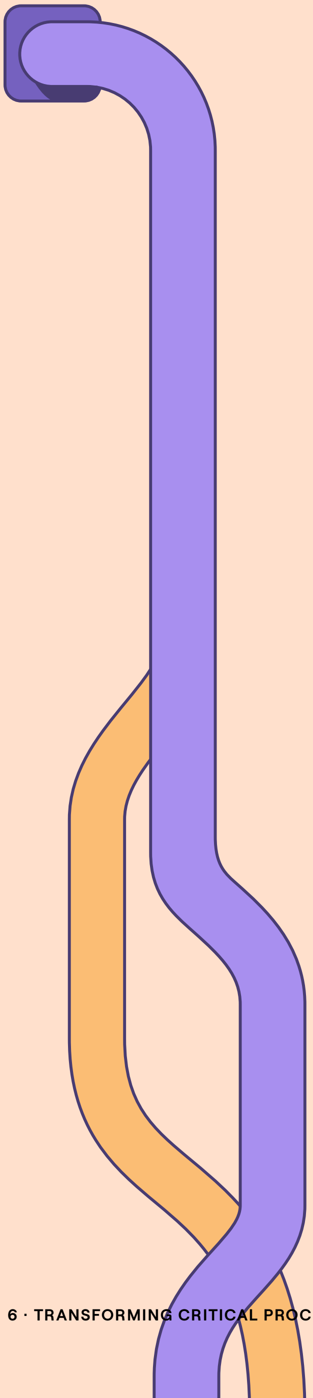
PHISHING ATTACKS

60% of energy sector data breaches result from phishing attacks. (source: Data Breach Investigations Report)



Common challenges in the energy sector





In addition to the inherent difficulties energy companies face in protecting their infrastructure and computing systems, these organizations must defend against a wide range of threats and organizational risks.

Besides the typical security concerns most companies face, energy companies must also protect their operational technology, comply with intensive regulations, and govern the security of their supply-chain partners.

RANSOMWARE ATTACKS

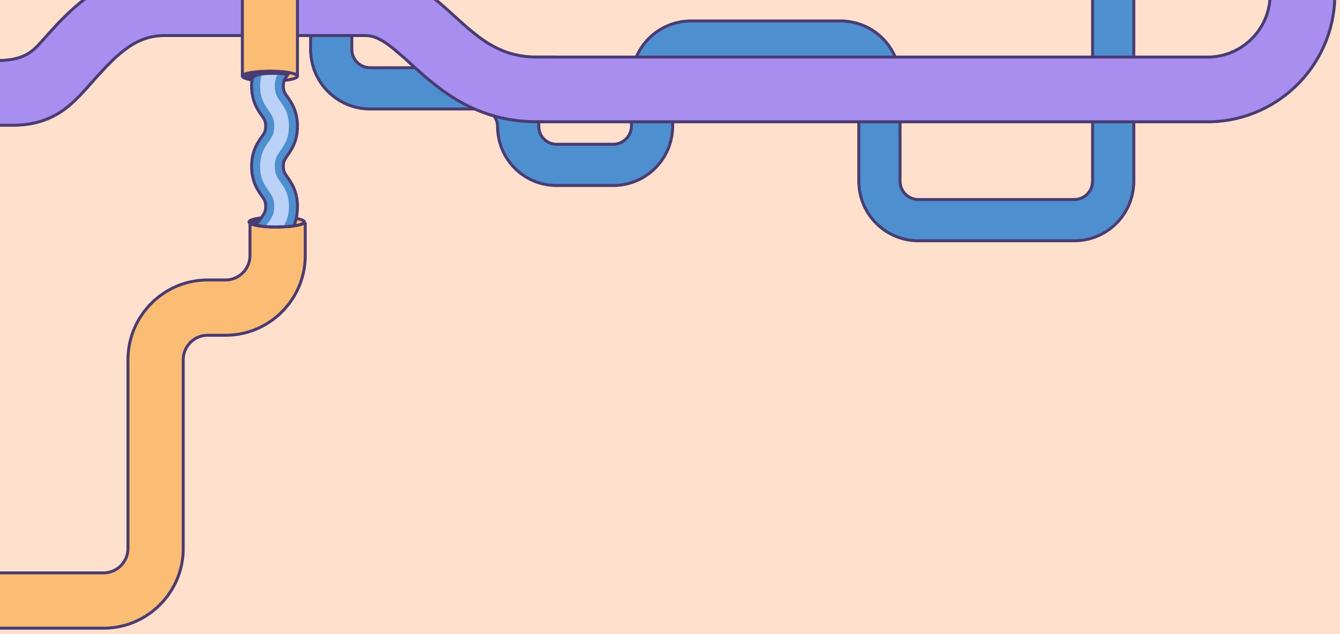
Energy companies are prime targets due to the critical nature of their operations. For example, the Colonial Pipeline attack in 2021 led to widespread fuel shortages.

ADVANCED PERSISTENT THREATS (APTS)

These are long-term, sophisticated attacks often conducted by state-sponsored actors. For instance, an APT might infiltrate a system to gather intelligence on energy production capabilities.

PHISHING AND SOCIAL ENGINEERING

These attacks trick employees into revealing sensitive information. A common scenario might involve an email impersonating a vendor requesting access to systems.



Operational Technology (OT) security

LEGACY SYSTEMS

Many energy infrastructures rely on outdated OT systems that lack modern security features. For example, a decades-old SCADA system controlling a power plant may not have built-in encryption and likely uses unsecure protocols such as Modbus, DNP3, and PROFINET.

IT-OT CONVERGENCE

As IT and OT systems become more interconnected, securing the interface between these two environments becomes crucial. A breach in IT systems, like a compromised employee email, could potentially allow access to critical OT systems controlling physical infrastructure through vulnerable communication protocols.

Regulatory and standards compliance

EVOLVING REGULATIONS

Security teams must stay abreast of and comply with a complex landscape of regulations. This might include standards like NERC CIP for electric utilities or API 1164 for pipeline cybersecurity.

COMPLEX STANDARDS

Compliance to standards such as IEC 62443 and NIST SP 800-82 provide comprehensive and practical guidelines for risk assessment, secure system design, and ongoing maintenance.

REPORTING AND AUDITING

Ensuring accurate reporting and undergoing regular audits to meet compliance requirements can be resource-intensive.

Supply chain security

THIRD-PARTY RISK

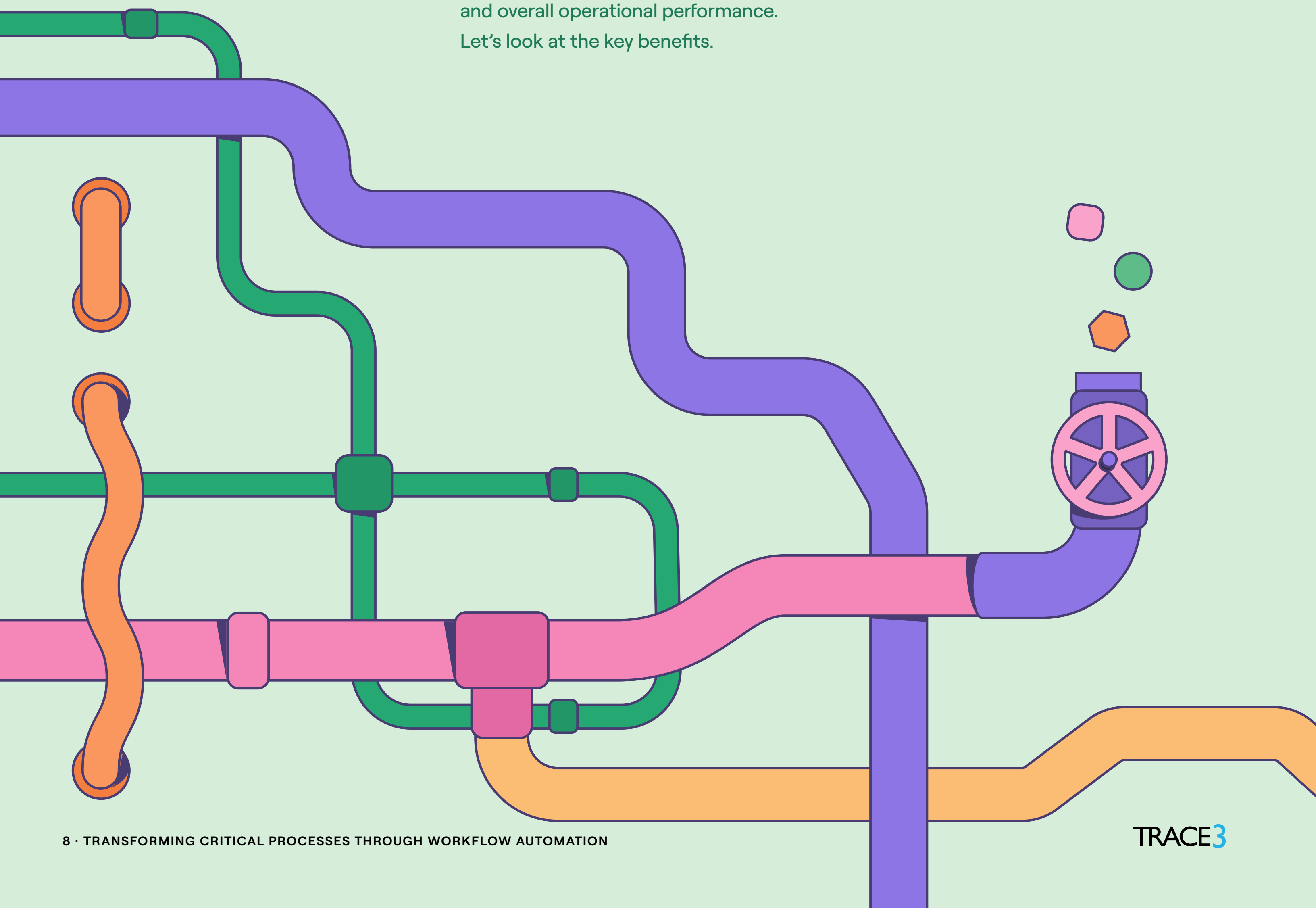
Energy companies often rely on a vast network of suppliers and contractors. Ensuring these third parties have adequate security measures in place is challenging but crucial.

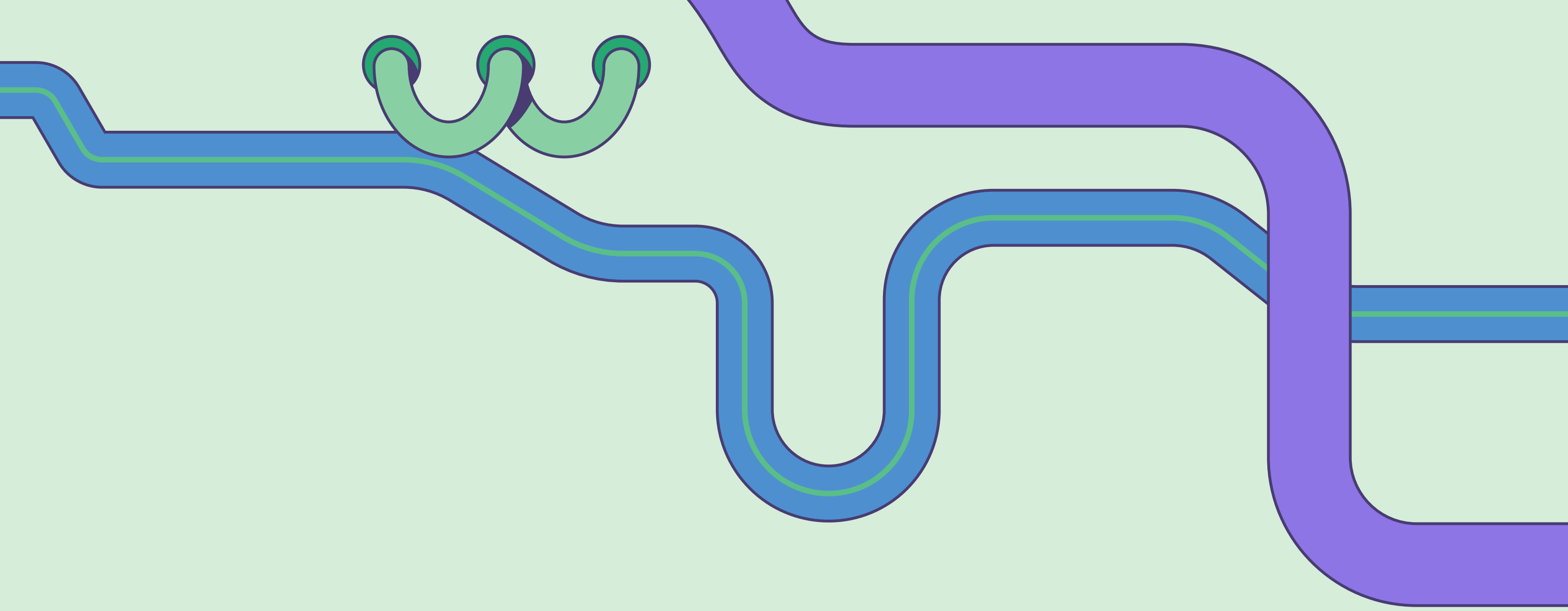
HARDWARE AND SOFTWARE INTEGRITY

Securing the supply chain to prevent the introduction of compromised hardware and software is critical, as these can be vectors for attacks.

Benefits of using workflow orchestration and automation for the energy sector

Addressing these challenges requires a multi-faceted approach, combining advanced technology, comprehensive training, and robust policies and procedures. Workflow orchestration and automation offer numerous benefits that enhance security, efficiency, and overall operational performance. Let's look at the key benefits.





Increased operational efficiency

REDUCED OPERATIONAL DOWNTIME

Automation of routine tasks and incident responses ensures minimal downtime. For example, patch management can be automated to occur during off-peak hours, reducing disruption to operations.

STREAMLINED WORKFLOWS

With the right solution, organizations can orchestrate and streamline complex workflows, reducing the manual workload on staff and allowing them to focus on higher-value tasks.

RESOURCE OPTIMIZATION

By automating repetitive and time-consuming tasks, organizations can optimize their resource allocation, making better use of skilled personnel and reducing operational costs.

Compliance and regulatory assurance

CONTINUOUS COMPLIANCE MONITORING

Workflow orchestration and automation helps maintain compliance with industry standards and regulatory requirements by automating the enforcement of security policies and generating audit-ready reports.

AUDIT TRAIL AND REPORTING

Automated reporting and comprehensive audit trails ensure organizations can easily demonstrate compliance during regulatory reviews and audits.

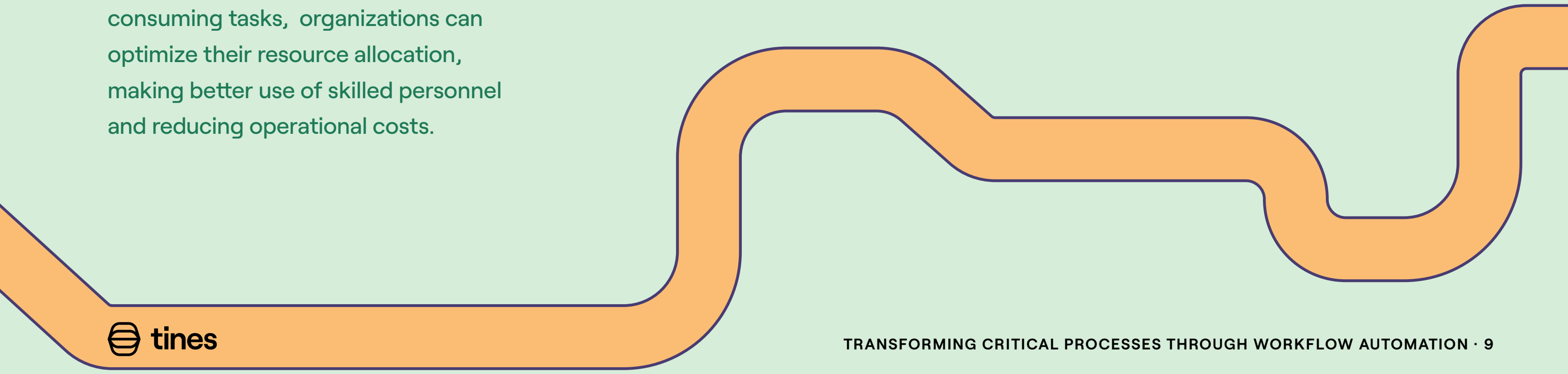
Enhanced resilience and reliability

HIGH AVAILABILITY

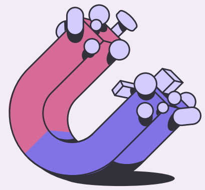
Workflow orchestration and automation ensures critical systems remain available and reliable, even during security incidents or other operational disruptions.

RESILIENT INFRASTRUCTURE

By automating security processes and incident responses, organizations can build a more resilient infrastructure capable of withstanding and recovering quickly from attacks.

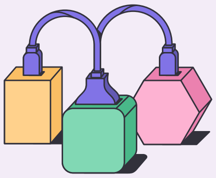


When selecting a workflow orchestration and automation solution for the energy sector, it's important to choose a product that can comfortably deliver all of the benefits previously outlined. The solution's success depends on satisfying the following critical criteria:



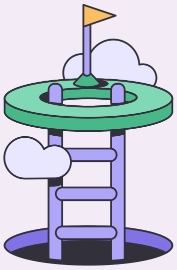
INTEGRATION WITH EXISTING SYSTEMS

The solution should seamlessly integrate with a variety of legacy and modern systems, providing a unified platform for security management without the need for extensive system overhauls.



ADAPTABLE SOLUTIONS

Your workflow orchestration and automation platform should offer scalable solutions that can grow with the organization, ensuring the system can adapt to evolving needs and requirements over time.



CUSTOMIZABLE AUTOMATIONS

Organizations should be able to tailor their solution's workflow automation and orchestration capabilities to their specific needs, ensuring it aligns perfectly with their unique operational processes.

When it comes to workflow orchestration and automation, customers and independent reviewers consistently highlight Tines' ability to deliver seamless integrations across diverse tech stacks. The platform's highly customizable nature allows organizations to build workflows tailored to their unique needs, while the platform's adaptability ensures it scales effortlessly as those needs evolve. Users also appreciate Tines' dedication to secure innovation. The platform's AI-powered features and AI chat interface Workbench are all designed with robust guardrails that maintain user control.

Common use cases

PHISHING RESPONSE

Identifies and mitigates phishing attacks targeting oil and gas personnel, protecting sensitive information, and maintaining operational integrity. For example, automatically analyze suspicious emails, quarantine threats, and alert security teams.

THREAT ENRICHMENT

Automatically gathers and analyzes threat intelligence to provide comprehensive insights into potential risks, enhancing proactive defense mechanisms.

RESOURCE OPTIMIZATION

Streamlines resource allocation and management, improving efficiency and reducing operational costs. This could involve automating the scheduling of maintenance tasks based on real-time equipment data.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Automates the management of user identities and access controls, guaranteeing only authorized personnel can access critical systems. This is particularly crucial for remote operations and third-party access management.

SECURE REMOTE ACCESS

Ensure secure remote access for employees and third parties by automating the management of VPNs, multi-factor authentication, and monitoring remote connections for suspicious activity. This is essential for maintaining security while enabling the flexibility needed in modern energy operations.

RISK PRIORITIZATION

Uses automation to assess and prioritize risks based on their potential impact on oil and gas operations, enabling more effective risk management.

DATA INTEGRATION, CORRELATION, AND ANALYSIS

Integrates and analyzes data from various sources to provide a unified view of operations, improving decision-making and operational efficiency.

DOCUMENTATION

Automatically generates and maintains comprehensive documentation of processes, incidents, and compliance activities, ensuring accuracy and ease of access.

SYSTEM INTEGRATION

Facilitates seamless integration of disparate systems, enhancing interoperability and coordination across energy operations.

AUTOMATED SCANNING AND PATCHING

Where safe and appropriate for OT environments, continuously scans for vulnerabilities and applies patches in real-time, solidifying the security and reliability of your systems.

AUTOMATED AUDITS AND COMPLIANCE CHECKS

Ensures ongoing compliance with industry regulations and standards by automating audit processes and compliance checks, reducing the risk of non-compliance.

INCIDENT RESPONSE

Automates detection and containment of security incidents, minimizing downtime and impact on critical energy operations.

Process OT detection alerts in Claroty and document in Jira

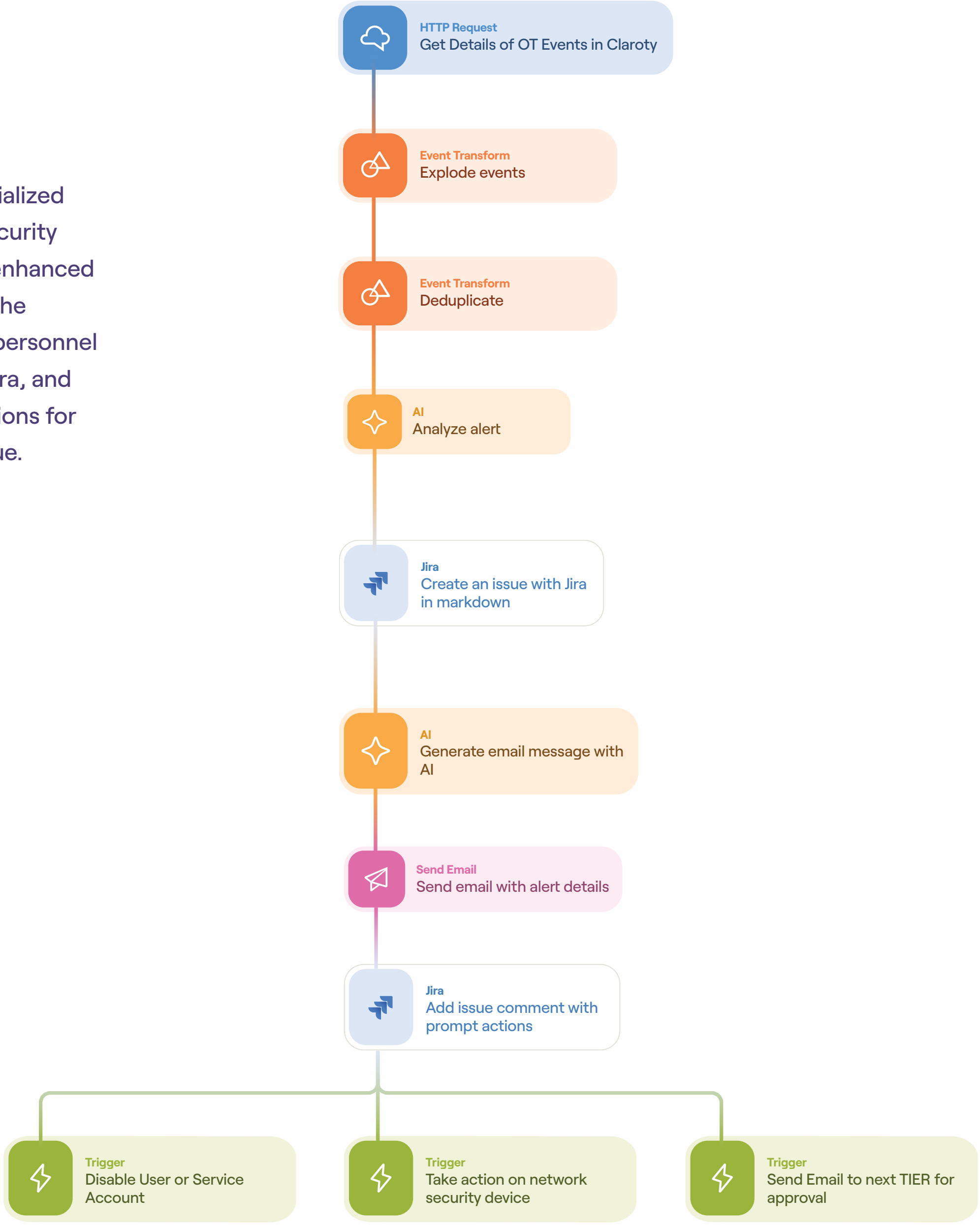
This story utilizes Claroty's specialized Operational Technology (OT) Security Alerts, which are subsequently enhanced and expanded with AI in Tines. The system swiftly notifies relevant personnel via email, generates a ticket in Jira, and offers actionable recommendations for security staff to address the issue.

TOOLS

Claroty xDome, Jira Software

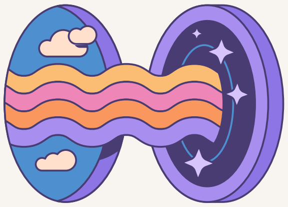
USE THIS WORKFLOW

tines.com/hcefr



HTTP Request
Get Details of OT Events in Claroty
Event Transform
Explode events
Event Transform
Deduplicate
AI
Analyze alert
Jira
Create an issue with Jira in markdown
AI
Generate email message with AI
Send Email
Send email with alert details
Jira
Add issue comment with prompt actions
Trigger
Disable User or Service Account
Trigger
Take action on network security device
Trigger
Send Email to next TIER for approval

Conclusion



Energy companies must address unique challenges and risks that require specialized solutions.

Their IT and OT environments are extremely complex and face extensive threats, making comprehensive security protections both challenging and essential.

Tines, with its robust automation and orchestration capabilities, provides comprehensive solutions to address these critical issues. By enhancing security, improving visibility, and optimizing operational efficiency, Tines enables organizations to secure their environments and ensure continuous, reliable operations.

With Tines, you're not just solving today's security challenges — you're future-proofing your operations against evolving threats. Imagine a world where your team can focus on strategic initiatives while Tines handles the complex, repetitive tasks that often bog down security and operations teams. This is the future of energy sector security and efficiency, and it's within your reach.

ABOUT TRACE3

Trace3 is an IT consulting organization specializing in cloud, data, and cybersecurity, with the unique ability to harness AI to help clients realize value from their technology investments.

Learn more at trace3.com.

ABOUT TINES

Tines powers the world's most important workflows. With secure AI capabilities, the flexible and intuitive platform eliminates the need for programming skills, enabling teams to build, run, and monitor their mission-critical processes.

Learn more at tines.com.