tines

Essential Guide

# The ultimate guide to network operations management:

## secure, reliable, and governed

# Contents

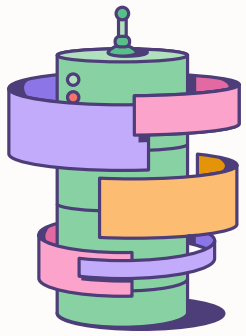
# Foreword

**Network and security teams face many of the same pressures.**

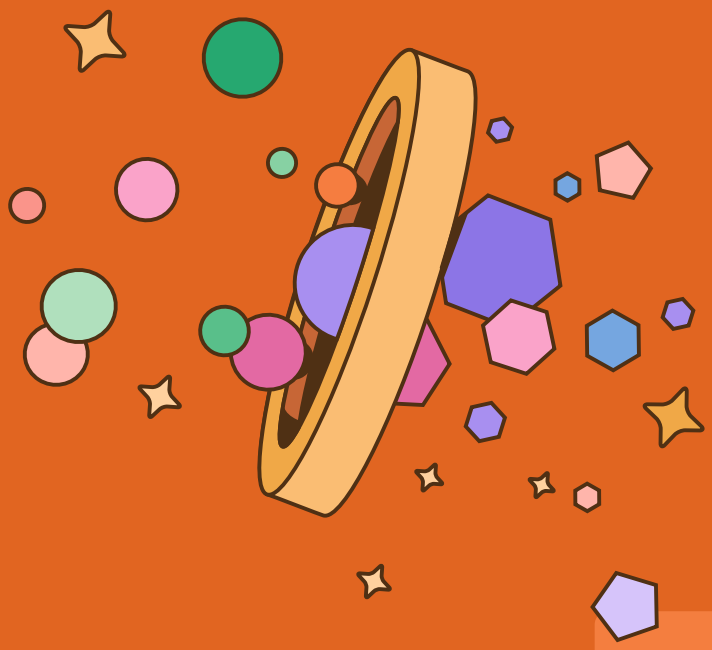
They must ensure network availability and resilience, keep critical systems performant and reliable, and prevent organization-wide impact from outages, performance degradation, and misconfigured or poorly coordinated changes. They're responsible for keeping businesses secure and compliant in the face of increasingly sophisticated threats. And they must manage all of this across a complex environment that spans legacy, on-premises, cloud-based, and hybrid systems.

But despite these shared priorities, many network and security teams operate in isolation, often due to disconnected platforms and case management systems that keep teams siloed. This fragmentation introduces delays, inconsistencies, and risk, making change coordination difficult and threatening performance and business outcomes – from increased downtime to degraded end-user trust.

To maximize their impact, network and security teams must work together. By breaking down structural silos and creating shared processes using intelligent workflows, teams can transform their network operations and shift from reactive troubleshooting to a more proactive, coordinated approach that saves time, protects resources, and strengthens control.



# When network operations can't keep up



Network operations have become significantly more complex. But as organizations scale across environments, traditional operating models struggle to scale with them, leaving teams stuck manually updating legacy systems or chasing evidence to fill gaps.

# The problem

## Traditional network operations break down due to factors like:

### Siloed tools

Network and security teams operate across a vast tech stack, including:

- Network monitoring systems (NMS) and observability platforms
- Configuration management and CMDB systems
- DDI/IPAM
- Load balancers
- Cloud networking
- Firewall infrastructure
- Identity and access management (IAM) systems
- SOAR platforms
- IT service management (ITSM) platforms

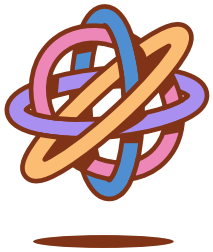
When these systems remain fragmented, teams can't collaborate effectively toward shared goals. This can lead to everything from duplicated work and inconsistent policy enforcement to missed alerts that become security issues.

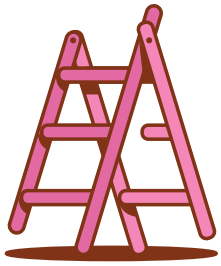
### Manual processes

Disconnected tools require teams to manually coordinate work across multiple systems. This creates significant operational overhead for routine tasks, eating up team time and resources that could be better spent on higher-impact tasks, like in-depth investigations or strategy. Manual work also increases the opportunity for errors and misconfigurations, slows incident response, and contributes to team burnout.

## On average, security teams spend 44% of their time on manual or repetitive tasks that could be automated

TINES VOICE OF SECURITY 2026





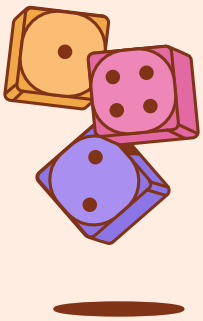
**Network professionals spend nearly half their time on manual tasks that could be automated:** 40% say half their workweek is spent on firewall management and network provisioning, with another 10% of their time spent remediating misconfigurations.

IT PRO

### Limited visibility

Gaps in visibility quickly compound, limiting teams' ability to detect threats, investigate incidents efficiently, and stay audit-ready. Without a single pane of glass across systems, evidence gathering and reporting become time-consuming and reactive, undermining compliance and weakening your organization's overall governance.

# The stakes

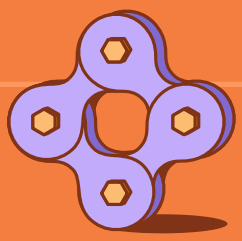


## Together, these issues open the door to:

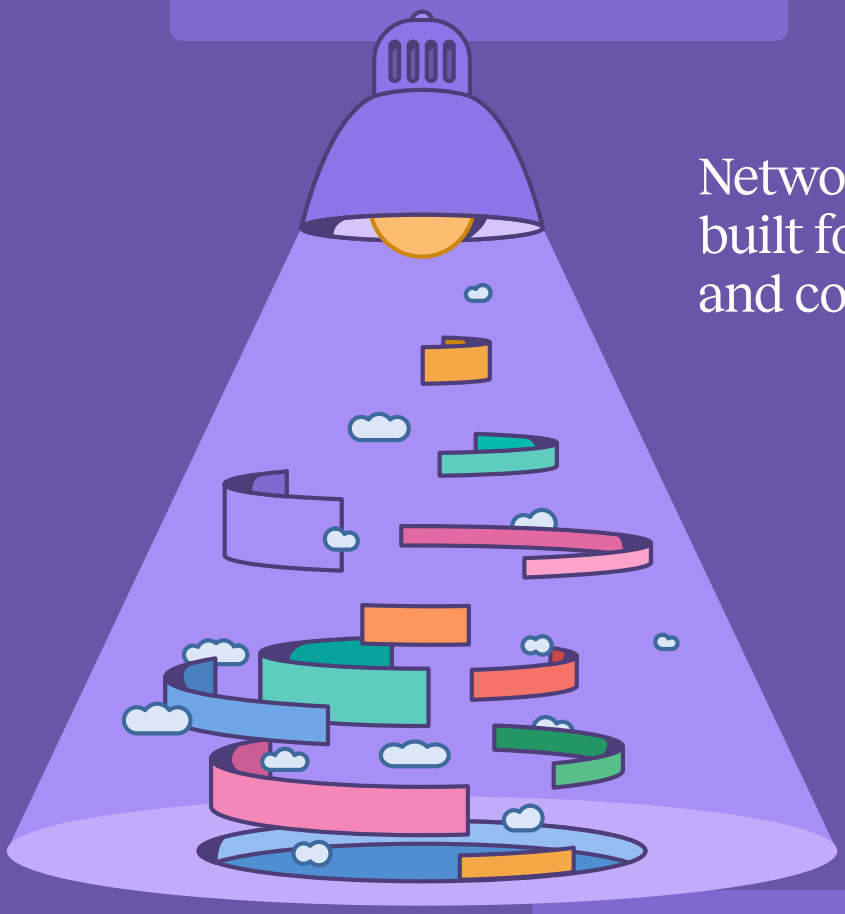
- **Outages and downtime** that cost your business money, damage your reputation, and lose end-user trust
- **Increased attack surface** due to misconfigurations, inconsistent policy enforcement, and silos
- **Compliance gaps** that leave your organization vulnerable to security incidents or penalties
- **High mean time to respond (MTTR)** due to bottlenecks and internal blockers that slow teams down
- **Burnt-out security and network teams** that are more prone to errors, exhaustion, and attrition

“61% of organizations estimate infrastructure downtime costs at least $50,000 per hour, and 34% put that figure at $100,000 or more.”

BUSINESS WIRE



# The new



Network operations built for scale, security, and control

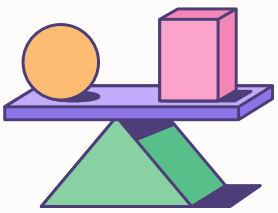
# standard

# The opportunity

The risks are clear. But what does "great" actually look like in secure network operations?

- **Consistent:** Access decisions are enforced consistently across cloud, on-prem, and hybrid environments.
- **Auditable:** Network changes are validated and auditable by default, and all actions taken on the network are logged.
- **Connected:** Performance and security signals are connected, not siloed, improving visibility and accelerating correlation.
- **Collaborative:** Network and security teams operate through shared workflows, promoting strategic alignment and faster decision-making.
- **Agile:** Every team member is empowered to create, own, and adjust workflows without waiting for custom scripts, removing bottlenecks that slow down execution.
- **Scalable:** Built on an operational layer that can grow alongside evolving requirements without adding complexity or additional headcount.

In order to reach this level of performance, however, teams must shift from siloed, manual processes to shared, orchestrated ways of working.



# **The key?** Intelligent workflows that connect network tools, identity systems, and security controls across all environments.

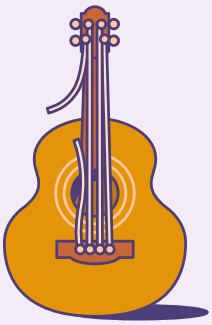
### What are intelligent workflows?

Intelligent workflows combine three essential types of workflow to give network and security teams the flexibility, control, and oversight they need to extend their resources, collaborate effectively, and enforce consistency at scale. They use:

- **Deterministic automation** to handle highly predictable, reliable, and controlled tasks
- **AI** to assess context, make decisions, and execute tasks autonomously
- **Humans** to handle high-impact and high-stakes tasks that require judgment and creativity

This enables network and security teams to create shared, auditable processes that improve performance, enforce access, and build in governance by design.

**By working together across shared workflows, teams can expect:**



# The impact

### Faster execution with reduced risk

Key processes – like incident response, configuration changes, and access requests – move through workflows efficiently, while standardization enforces your best practices and ensures consistency at scale.

### Improved visibility across network and access activity

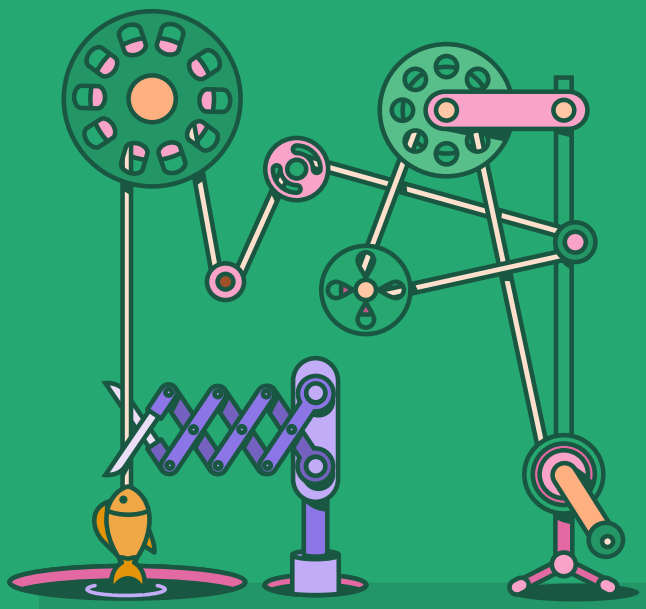
Shared workflows maintain clear approval paths and audit trails, improving accountability, speeding up investigations, and surfacing insights previously lost between siloed tools and systems.

### The end of muckwork

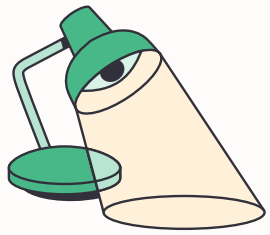
Practitioners are freed from time-consuming, error-prone, and enthusiasm-draining manual work. Instead, they can focus on high-impact tasks, like complex problem-solving, strategic enablement, and cross-functional initiatives.

Modern network operations require more than isolated tools and manual coordination. Intelligent workflows create the operational layer that helps teams move faster, stay aligned, and scale securely. Next, we'll look at how to build that foundation in practice.

# Building your secure network operations strategy



Now that you know what operational excellence looks like, the next step is execution. Follow this roadmap to reduce friction, improve performance, and enhance collaboration – then use our checklist in the next section to gauge your progress.



## Identify

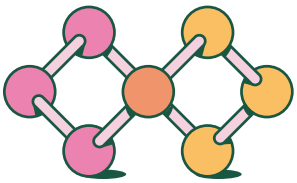
Start by mapping out your existing processes, tools, and policies to find pain points and improvement opportunities. This helps you pinpoint where siloed tools, manual handoffs, and visibility gaps introduce risk and inefficiency – and where you can leverage rules-based automation and AI to optimize workflows.

- Map network systems, identity providers, and security tools. Outline how they currently integrate (or don't) across environments.
- Define access policies and operational workflows. Do the operational workflows enforce the policies and standards you've set, or are there gaps between expectation and reality?
- Identify high-friction processes. What takes up team time, and where does work get stuck? Think: access requests, changes, renewals, and other processes that require manual handoffs or approvals.
- Document the current process for network alerts. How are alerts currently handled and resolved? How much time is spent on investigation, correlation, and escalation?

## Structure

Once you have a clear overview of how things currently work, you can start making targeted improvements based on your findings. This is where you create a shared operational baseline across network and security functions, ensuring everyone is aligned, knows who owns what, and has visibility over data and processes.Define approval workflows and governance rules. Map out who owns decisions, what criteria are used to assess approvals, and how actions are logged.

- Standardize change processes. Ensure that policies are consistent across cloud, on-prem, and hybrid environments.
- Establish policies for access and configuration management, such as least privilege, role-based access, and configuration baselines. Define how you'll enforce these policies across network and security infrastructure – including VPN, NAC, routers, switches, load balancers, DNS/DHCP/IPAM, SD-WAN, cloud networking constructs, and firewalls – and detect configuration drift.
- Upgrade your alert process. Establish how you'll use deterministic automation, agentic AI, and human-in-the-loop judgment to triage alerts, enrich them with context, prioritize by severity, and take appropriate action.



## Implement

Use an intelligent workflow platform to put your updated processes into practice. Connect systems using APIs to orchestrate work across environments, maintain visibility over all network operations, and create clear audit logs.

- Connect networking, identity, and security systems via APIs, so you can orchestrate workflows across your entire environment
- Automate access control, change management, and validation workflows to reduce manual work for your team
- Enable self-service for users or teams where appropriate, using built-in guardrails to maintain control
- Implement alert-handling intelligent workflows to reduce alert fatigue and improve response times

## Monitor

Implementing your workflows is just the beginning. Use key performance indicators to monitor the impact on operational performance, compliance and audit-readiness, and team time and resources.

- Track performance, access activity, and change metrics over time using KPIs like:
  - Mean time to detect (MTTD)
  - Mean time to restore service
  - Mean time to resolve
  - Downtime and outages
  - Change failure rate
  - Number of misconfiguration or drift incidents
  - Percentage of changes validated automatically
  - Team time spent on manual work
- Ensure auditability across all workflows and measure impact using metrics like:
  - Team time spent on evidence-gathering for audits
  - Audit trail completeness rate
  - Audit performance

- Provide shared dashboards for IT and security to further alignment and visibility, and measure cross-functional success using:
  - — Reductions in duplicate work
  - — Reductions in manual handoffs
  - — Reductions in repeat incidents due to the same operational issue or regressions
  - — Time saved per team and team member due to automation and intelligent workflows
  - — Percentage of incidents enriched or routed automatically
  - — Dashboard adoption and usage across teams
  - — Average access provisioning time
  - — Time to isolate
  - — Maintenance-window adherence

**Pro-tip:**

To fully convey the impact of your network operations strategy to stakeholders and leadership, translate these metrics into business-level outcomes. For example:

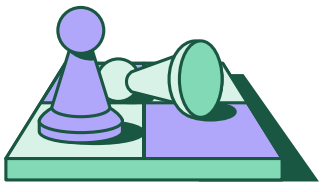
- MTTD: Faster detection reduces downtime and negative impact on customers
- Mean time to restore service: Directly tied to revenue, productivity, and customer trust
- Change failure rate: Measures business risk from network changes
- Team time spent and saved: Shows resource efficiency and productivity

## Iterate

Finally, continue to refine your workflows based on incidents and usage patterns. With an intelligent operational foundation in place, teams can easily scale their capacity and impact without needing to add headcount.

Build on your successes by expanding automation across additional systems, finding strategic ways to further reduce manual tasks, and streamlining workflows. As your organization evolves, adapt your workflows to meet new security requirements and support infrastructure growth.

Building secure, scalable network operations is an ongoing process of improving how work moves across systems, teams, and environments. Before exploring real-world workflow examples, use the checklist in the next section to assess your current operational readiness and identify areas for improvement.



# A checklist

## Ready for secure, scalable network operations?

How equipped are you to deliver secure network operations for your organization? Use this checklist to assess your readiness across performance, security, and governance, and identify gaps you can bridge with collaborative, shared workflows.

### Access and identity control

- Goal: Access is consistent, auditable, and aligned with policy
- Are network access decisions enforced consistently across systems?
- Are VPN, NAC, and firewall rules updated automatically?
- Is there a clear approval and audit trail for access changes?
- Is the principle of least privilege adhered to?

### Infrastructure trust and integrity

- Goal: Network infrastructure is continuously validated and trusted
- Are certificates rotated and managed automatically to maintain hygiene?
- Can configuration drift be detected and remediated quickly?
- Are changes validated before impacting production?
- Is there a reliable backup and rollback process in place?
- Are network devices secured?

### Operational visibility and governance

- Goal: IT and security share a unified view of network operations
- Do teams have shared visibility into network changes and activity?
- Do you have up-to-date visibility into network topology and dependencies?
- Are maintenance windows formally defined, enforced, and governed, with changes coordinated across teams?
- Can you easily produce audit evidence for network changes?

### Scalability and performance

- Goal: Network operations can scale without introducing risk
- Can your processes handle growth in users, devices, and services?
- Are performance and security signals connected?
- Are your workflows consistent across cloud, on-prem, and hybrid network environments?
- Can workflows adapt as environments evolve?

Delivering secure, reliable, and scalable network operations depends on how effectively work moves across your environment. Use this checklist to identify gaps, prioritize improvements, and benchmark your operational readiness before exploring real-world workflow examples in the next section.

# The Tines advantage

To implement this approach at scale, teams need an orchestration layer.

This is where Tines comes in. Tines enables network and security teams to operate as one, connecting systems, workflows, and decisions across both domains to improve efficiency and drive stronger results.

# Why network and security teams choose Tines

### Interoperability

Tines connects to any tool with an API, allowing teams to join the dots between networking, identity, and security systems across cloud, on-prem, and hybrid environments – without adding complexity.

### Universal accessibility

Tines always meets your teams where they are; whether they prefer working with a visual, intuitive workflow builder, or leveraging the power of code. Network teams can move from words to workflows in seconds, removing reliance on custom scripts or engineering support.

### Operational agility

Reduced manual effort and bottlenecks mean teams can implement network changes faster and more efficiently, without sacrificing control.

### Auditability

Intelligent workflow platforms ensure every action is logged, validated, and compliant by design, improving visibility, accountability, and audit-readiness.

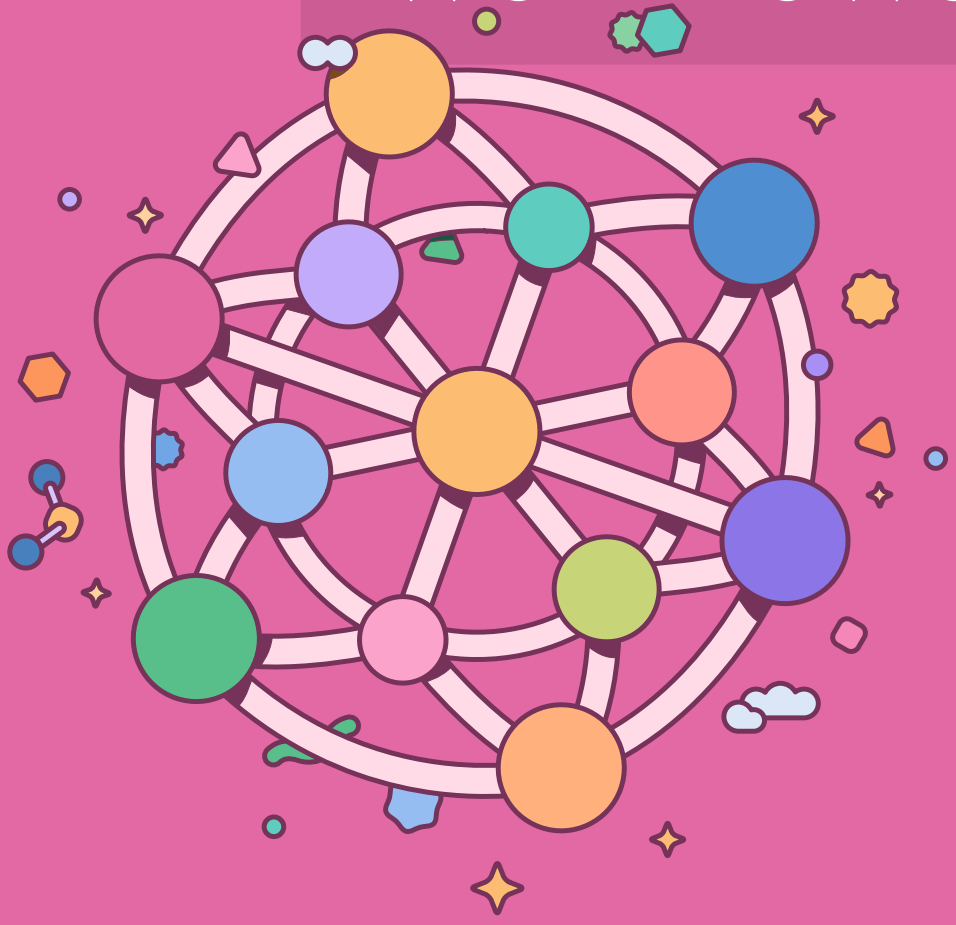
### Reduced risk

Standardization enforces consistency and scales your best practices across teams and functions, reducing human error and gaps in oversight.

### Visibility

Tines gives network and security teams a single source of truth for all actions taken on the network, fueling informed, strategic decision-making and collaboration toward shared goals and priorities.

# Pre-built workflows



**Create your own intelligent workflows, or start with pre-built templates from the Tines Story Library to accelerate results.** Here are some powerful workflows to try first:

# Automating NAC and VPN access lifecycle

Automatically provision or remove NAC and VPN access for new joiners, contractors, or leavers based on your defined policies, reducing manual approvals and over-permissioning.

## Sync on-call engineers from PagerDuty to Bowtie access groups

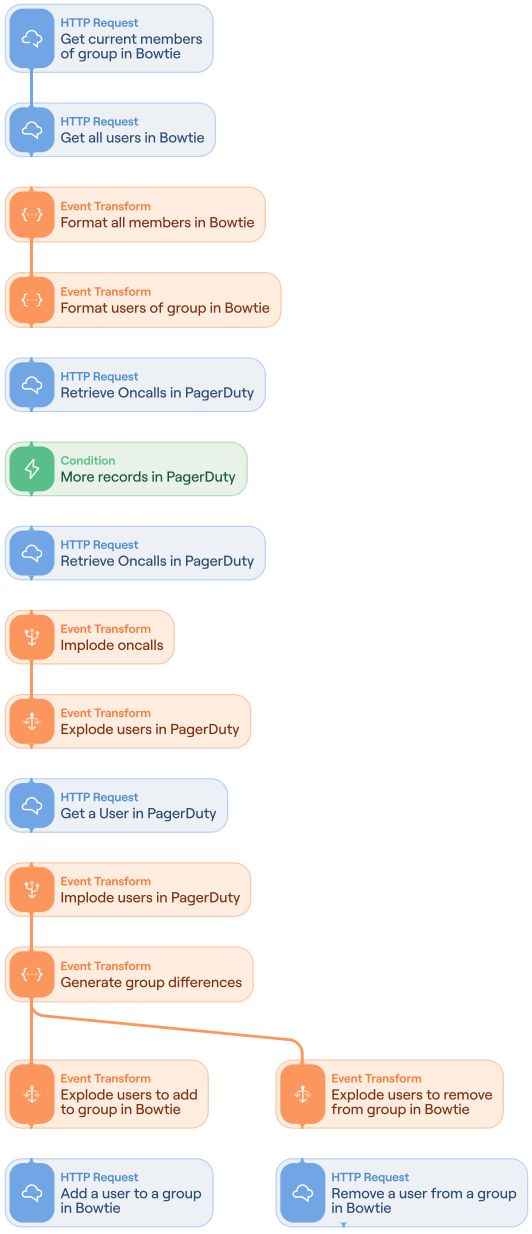
Dynamically update access groups in Bowtie to only contain engineers who are on-call in PagerDuty. Provide access to additional support only when necessary.

**TOOLS**

Bowtie, PagerDuty

**USE THIS FLOW**

tines.com/sfpac



# Firewall change approvals with audit logging

Use automation to approve or escalate requests based on risk and policy. Automatically implement changes where appropriate or route to the right channel for further review, maintaining a complete audit trail of the requester, approver, and changes made.

## Report and recategorize blocked sites in Netskope via Slack

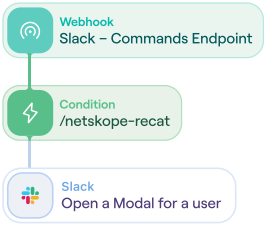
Manage blocked site reports through Slack and Netskope by validating domains, temporarily adding them to security exceptions, and automatically removing them after recategorization. Communicate status updates via Slack messages throughout the three-day review process.

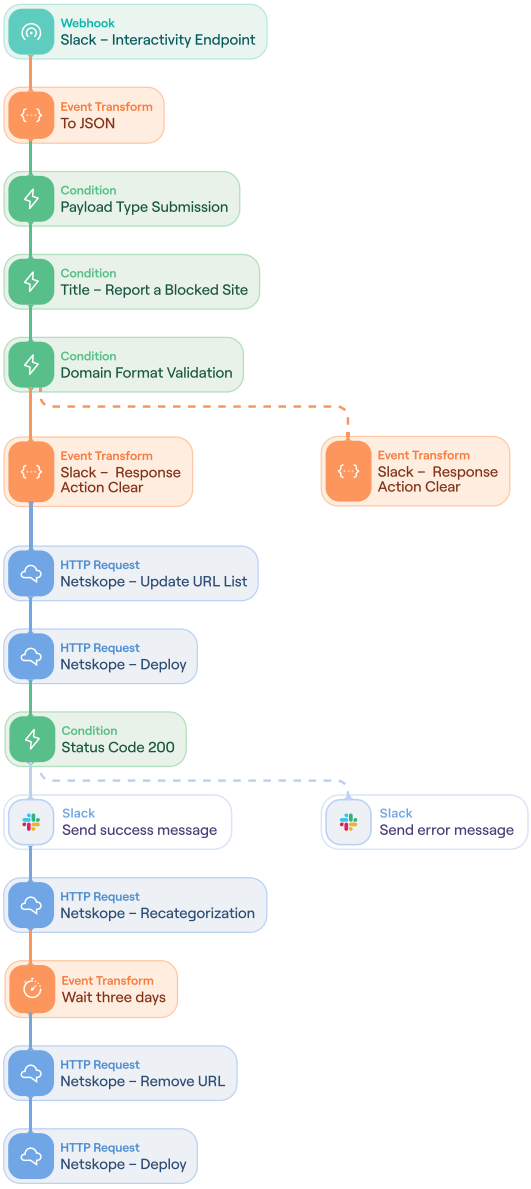
**TOOLS**

Netskope, Slack

**USE THIS FLOW**

tines.com/rarns



## Receive Azure Sentinel alerts and block IPs with firewall rules

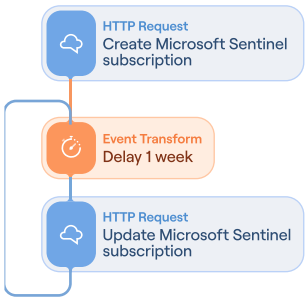
Set up an event subscription in Azure Sentinel to send new alerts to a webhook. If the alert is related to Brute Force attacks, set up a network security rule to block access from the source IP.

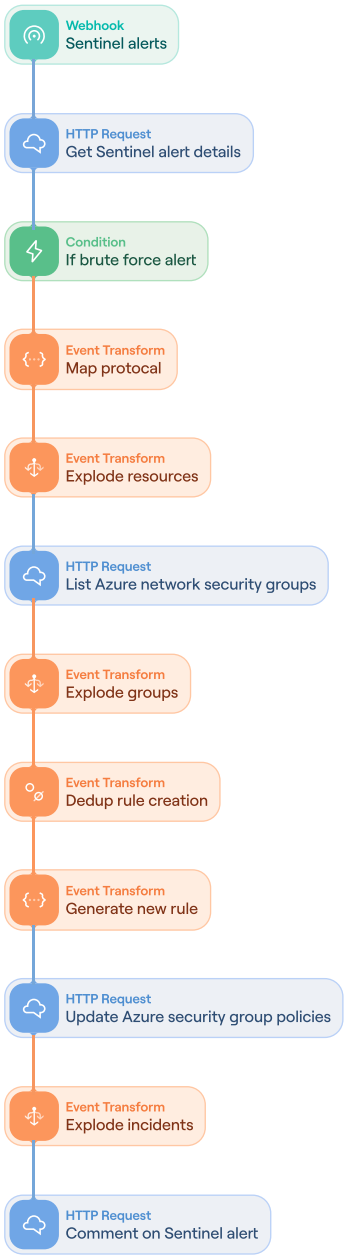
**TOOLS**

Microsoft, Microsoft Azure

**USE THIS FLOW**

tines.com/rasab



# Certificate lifecycle management and renewal

Get notified before certificates expire to avoid gaps in coverage or outages and kick off the renewal process, without requiring manual intervention.

## Monitor TLS certificates for a domain with SSLMate

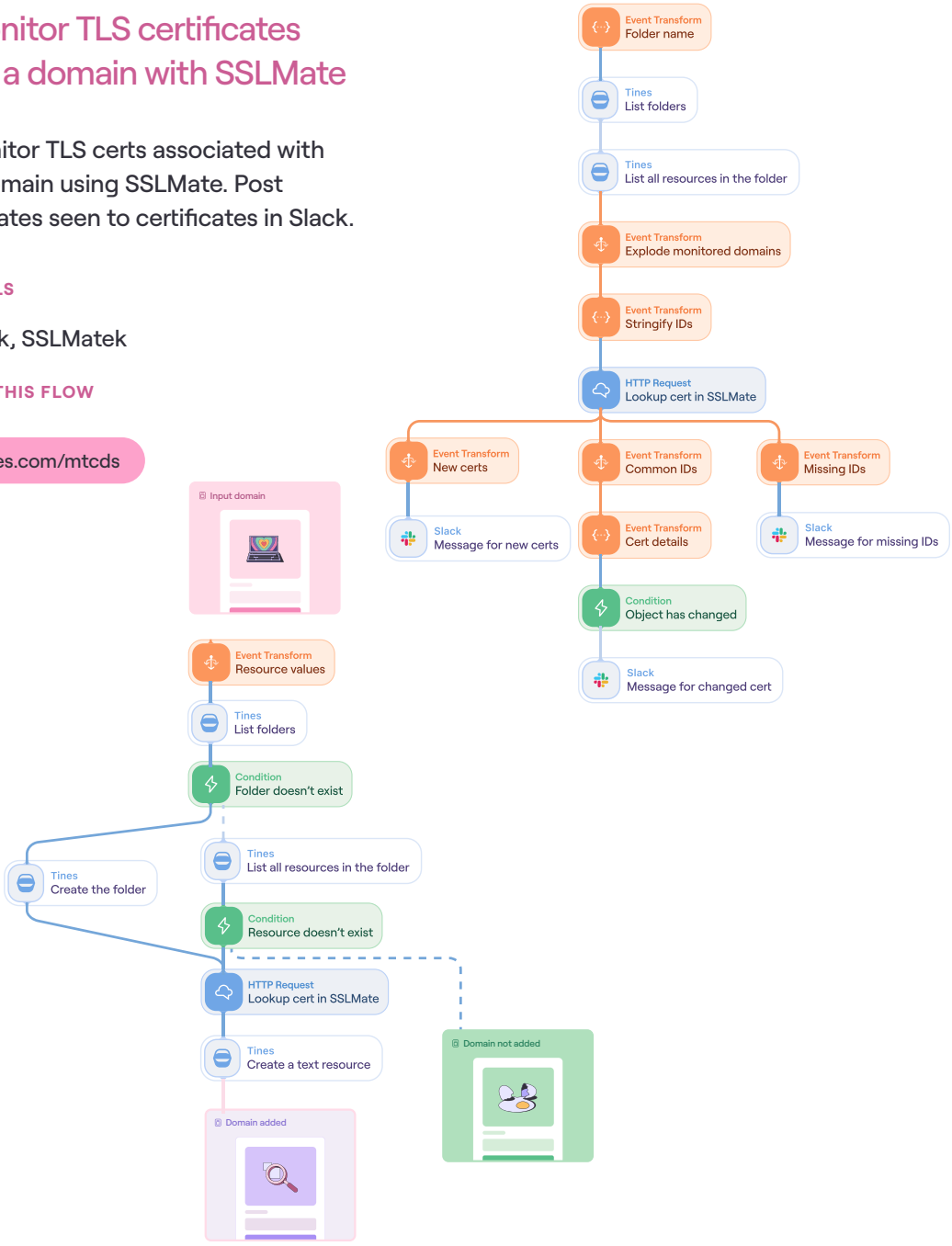
Monitor TLS certs associated with a domain using SSLMate. Post updates seen to certificates in Slack.

**TOOLS**

Slack, SSLMatek

**USE THIS FLOW**

tines.com/mtcds



# Detecting and remediating configuration drift

Monitor whether configurations adhere to your outlined policies and approved setups, and identify risks and vulnerabilities that may have crept in over time. Trigger remediation workflows automatically or escalate for further investigation to address compliance issues.

## Analyze network device configurations in GitHub using the AI Agent action

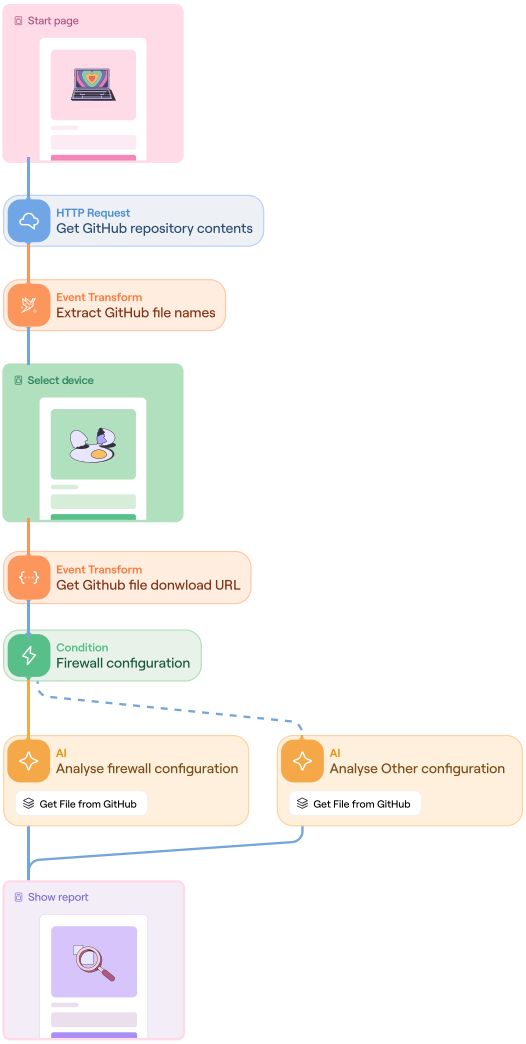
Analyze network device configurations stored in GitHub repositories using agents. Identify security vulnerabilities, compliance issues, and configuration drift using targeted AI analysis. Compile a detailed report or have a back and forth conversation about the configurations depending on your needs.

**TOOLS**

Cisco, GitHub

**USE THIS FLOW**

tines.com/ancga



## Remediate insecure AWS EC2 security groups

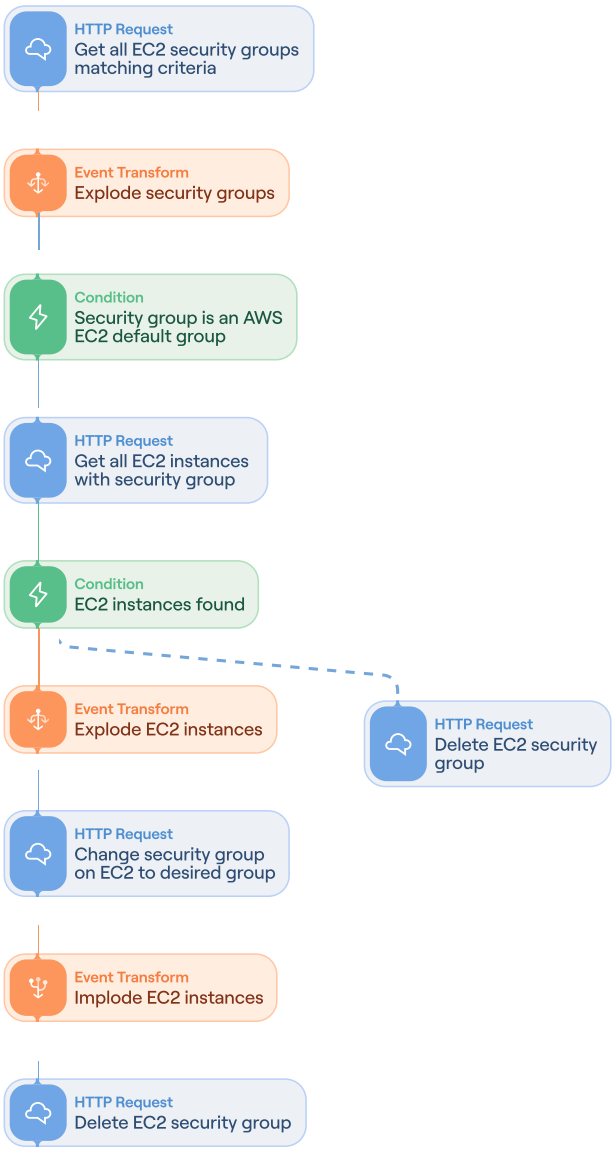
Identify default and insecure AWS EC2 security groups and locate associated instances they are attached to. Replace security groups with secure ones and remove the original insecure groups.

**TOOLS**

AWS

**USE THIS FLOW**

tines.com/riasg



# Coordinating maintenance windows and change scheduling

Keep cross-functional teams informed and aligned about upcoming changes and planned maintenance, ensuring they have visibility and can work effectively around any scheduled downtime.

## Manage temporary EC2 instances for development and testing and send notifications in Slack

Teams who frequently need to temporarily start EC2 instances for development, testing, and demos, but don't want to waste resources by leaving them up and running all of the time. Search for EC2 instances by name or tag, start them with a scheduled stop time, and optionally send Slack notifications.

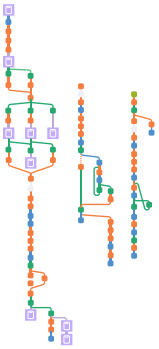
**TOOLS**

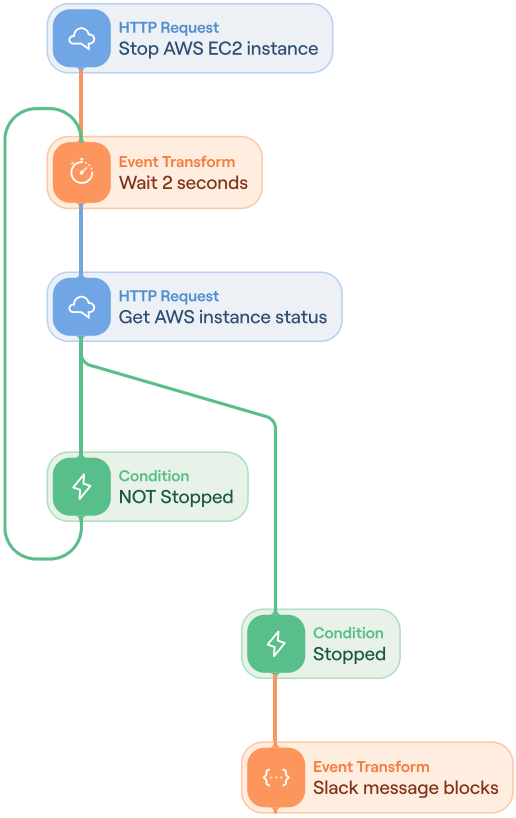
AWS, Slack

**USE THIS FLOW**

tines.com/mtidt

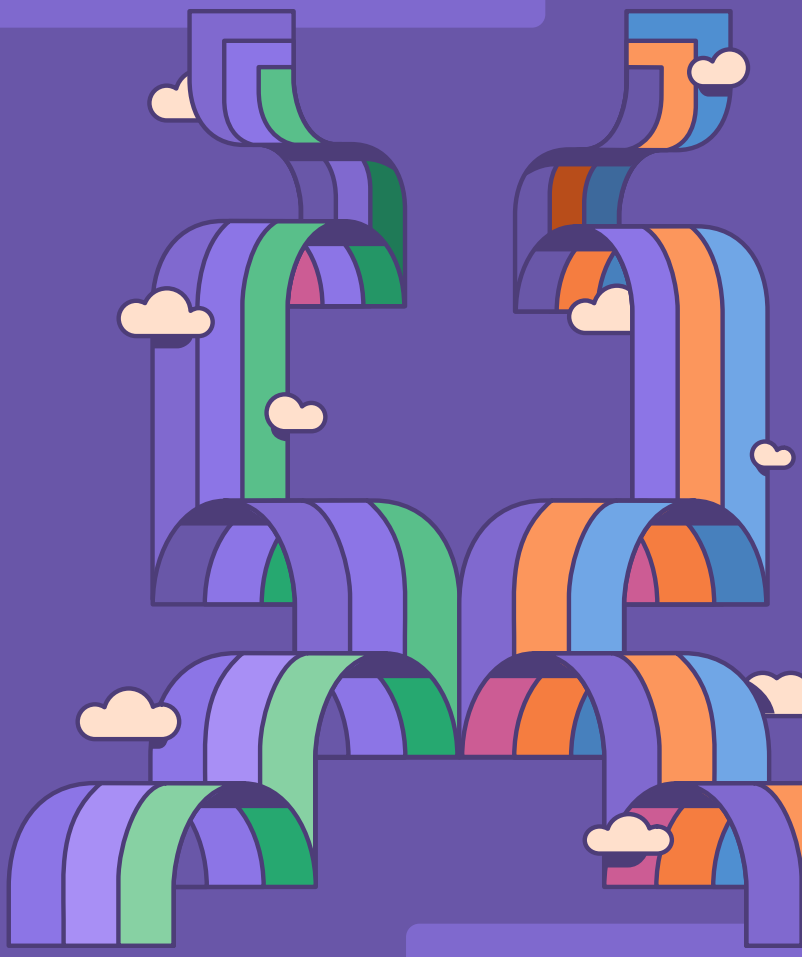
**FULL WORKFLOW MAP**






Use the **Workflow capability matrix** to explore intelligent workflows and quickly get started.

# Getting started

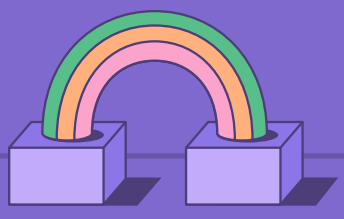


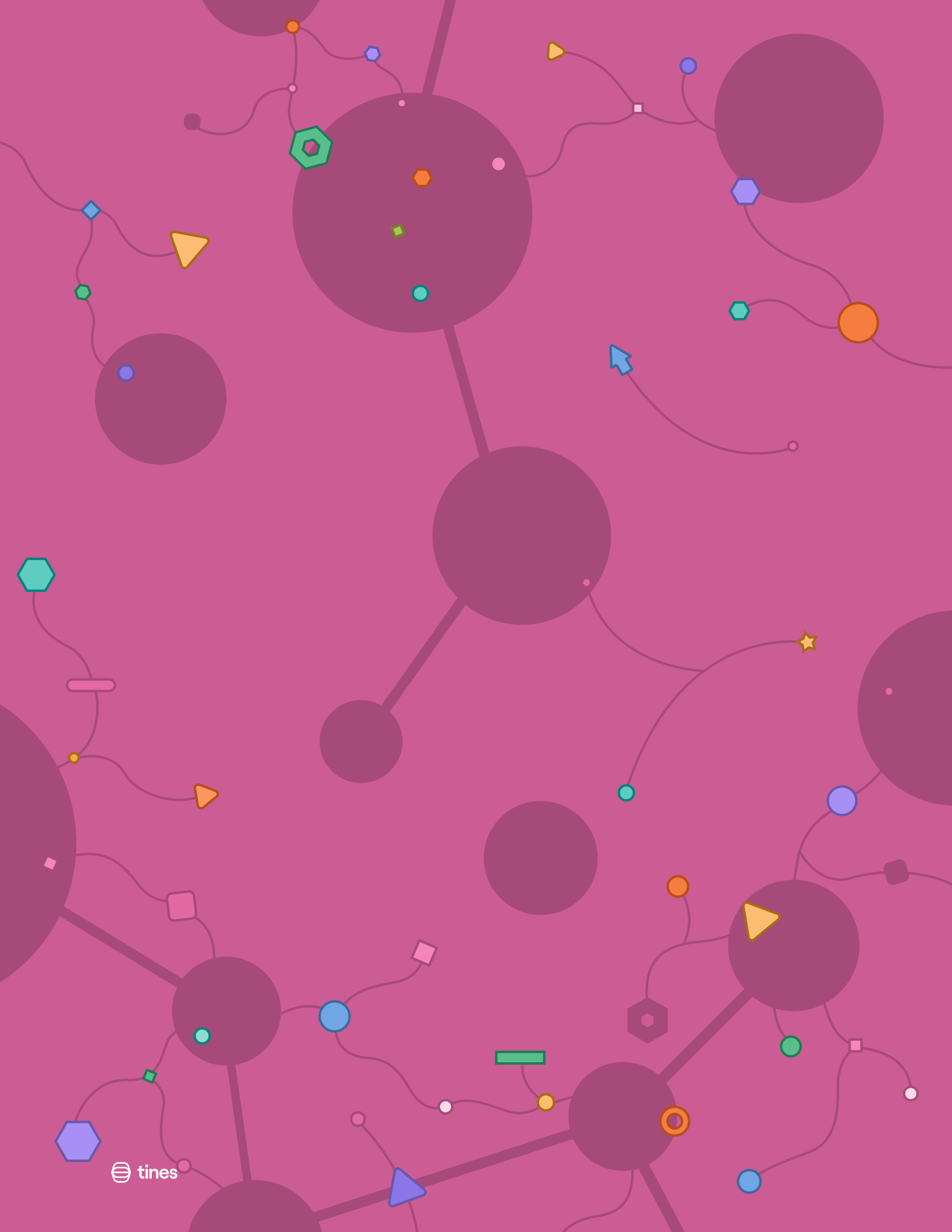
Managing the identity lifecycle is about more than provisioning accounts. Done right, it empowers IT and security teams to enforce least privilege, reduce delays, and stay audit-ready, all while giving employees seamless access to the tools they need. It's not a trade-off between speed and security; it's both, working together.

Instead, network and security teams need to rethink their foundations, building an operational layer that can scale to meet evolving challenges. With intelligent workflows, teams can work together to break down silos, reduce manual tasks, and enhance visibility and auditability – enabling faster, more secure, and compliant-by-design operations.

→ **Learn more about Tines for secure networking operations:**
tines.com/blog/why-networking-teams-need-orchestration/

→ **Book a demo:**
tines.com/book-a-demo/




tines