



Operationalizing zero trust

A practical guide
for modern federal
agencies

by Dennis Perrone



Contents

Understanding zero trust	02
Building your zero trust tech stack	04
• Things to consider	
• Essential technologies and frameworks	
Automating and orchestrating for zero trust	09
• Choosing your approach	
• Challenges with legacy SOAR	
• Case study: Oak Ridge National Laboratory	
• Tines and zero trust framework	
The quickest path to zero trust	19

Introduction

by Dennis Perrone



The challenges facing federal security teams are relentless.

Security teams are inundated with data and alerts, all of which are required to manage the overwhelming number of cybersecurity threats coming their way.

CISA's zero trust model was designed to give federal agencies clear guidelines on how best to protect their environments, but in many cases, it only created more confusion. Zero trust is complex, and implementing it can be a lengthy and disruptive process for security teams that are already stretched thin.

What's more, CISA's zero trust model includes several blind spots, including legacy tools and systems that weren't designed for zero trust, and don't communicate well with each other.

Factoring in the limitations of staff, budget, and technology, it's no surprise that many federal agencies are still trying to understand what zero trust looks like in their environment, years after M-22-09 was released. Now, in their efforts to meet requirements quickly, security leaders might be tempted to believe far-reaching claims made by technology vendors.

In this, Tines strives to be different. Despite what some marketing taglines may tell you, there are no shortcuts to zero trust and you can't buy it out of a box.

The good news is that, with the right technology and frameworks, the journey towards zero trust can be simplified and even accelerated. So that's what we'll focus on in this whitepaper.

We'll break down the essential zero trust tech stack, and help you choose tools and systems that align with your agency's zero trust goals. We'll show you what to look for in a zero trust solution, and crucially, what to avoid. And we'll dive deep into the cross-cutting capability that so many teams struggle with - automation and orchestration.

The truth is, your zero trust journey is never complete. This guide is all about choosing your next steps wisely.

ABOUT THE AUTHOR

Dennis Perrone is a solutions engineer with over a decade of experience designing and implementing complex systems at federal agencies, including the US Navy. He currently specializes in SOAR and cybersecurity.

Understanding zero trust

Zero trust is a security framework in which every user and device must continually prove their identity.

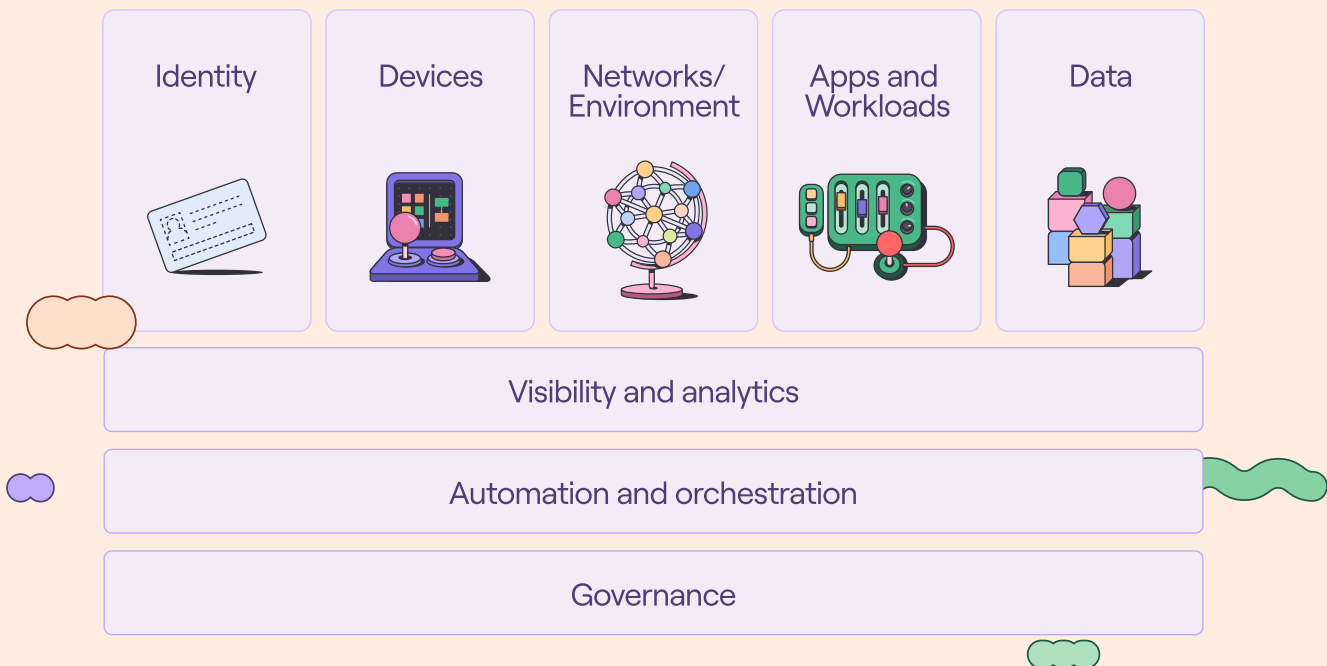
Ever since the concept of zero trust security was first popularized by Forrester in 2009, many federal government agencies in the United States (along with private sector companies) have struggled to understand its requirements and implement it effectively.

Critically, zero trust does not represent a single security method or a type of technology. CISA's zero trust framework outlines a set of security practices that should be part of most organizations' efforts to continually improve their cybersecurity posture.

The most important and useful document on zero trust security is the zero trust maturity model published by the Cybersecurity and Infrastructure Security Agency (CISA) of the United States federal government.

It defines five technology pillars that organizations must address to advance their zero trust architecture. In addition to building up the zero trust capabilities of individual technology pillars, CISA emphasizes that agencies must also create a foundation of cross-pillar coordination to provide holistic cybersecurity management.





Zero trust pillars and cross-cutting capabilities

Zero trust requires continuous authentication and authorization for every user and device attempting to access resources, regardless of their location. This approach emphasizes strict access controls, least privilege access principles, micro-segmentation, and comprehensive visibility across the network. Zero trust aims to enhance security posture by minimizing the attack surface, detecting threats early, and preventing lateral movement within the network.

Zero trust: a process, not a product

One of the most common misconceptions about zero trust is that it's something you achieve by simply checking items off a list. Zero trust is a living program that requires constant improvement and innovation. 100% compliance is an unrealistic, and therefore unhelpful, goal.

This is yet another reason why we need our technology to be flexible, adaptable, and scalable. Our systems should help us evolve, not create barriers to progress.

Ultimately, implementing zero trust is about identifying and addressing gaps in your security posture. The first step should always be an audit of what your teams are already doing.

“Organizations should be able to very quickly determine where any given zero trust implementation may have:

- Capability gaps (lacking tools, or people to do things, or procedures for doing them)
- Overlaps (having invested multiple times in providing the same capability differently)
- Seams (individual capabilities exist, but are not working, not working together, or not working together well or quickly)”

— Don Yeske, Director, National Security Cyber Division, U.S. Department of Homeland Security

And when it comes to zero trust and tech, it's not only about buying the right solution. It's also about getting your stack to communicate better, in order to meet requirements.

Building your zero trust tech stack

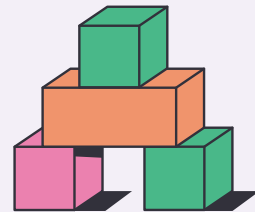
The market for zero trust security is sprawling and often confusing, as highlighted by Gartner:

“Zero trust is being misused as a marketing term. Vendors are applying the term ‘zero trust’ to market everything in security, creating significant marketing confusion.”

Zero trust has many technology categories, with many products for every category.

To further complicate matters, all the technologies in a zero trust stack should be able to work together to provide holistic control and comprehensive visibility.

To help address these challenges, we’ll discuss key considerations for how federal agencies should approach building their zero trust technology stack, as well as defining some of the most important technologies that support zero trust security practices.



Six things to consider when building your zero trust technology stack

Here are some tips for how your federal agency can prioritize its zero trust technology purchases.



1. Establish a baseline

When figuring out what technology you need to improve your zero trust defenses, start by understanding what technologies and capabilities you already have.

If you haven't already done so, conduct a full inventory and assessment of your current security tools and IT systems.

2. Focus on removing siloes

While federal organizations need to advance the maturity of each zero trust pillar, they must also build out their cross-pillar capabilities for visibility/analytics, automation/orchestration, and governance.

Critically, many federal organizations use custom GOTS (government off-the-shelf) applications and technologies, as well as an array of COTS (commercial off-the-shelf) tools, making integration of these disparate technologies challenging.

Ideally, the tools used for cross-functional coordination must be able to work with any and all the tools in your zero trust tech stack and IT infrastructure (now or in the future).

3. Consider your environment

The effectiveness of your zero trust investments depends heavily on your tech stack's ability to work within your hosting infrastructure. This presents unique challenges, in particular, for agencies leveraging hybrid cloud architectures, or those managing classified or completely air-gapped networks.

In these and many other cases, tools that are hosted on a shared stack fall short. Look instead for solutions that offer deployment options to suit your hosting environment - self-hosted, on premise, etc.

4. Determine your unique requirements and priorities

Now that you understand what you already have in place, you should be able to identify what's preventing you from advancing your zero trust maturity across the pillars and cross-functional capabilities. Next, it's time to find the technology that will help you plug those gaps.

This is a good time to identify which aspects of zero trust have the potential to make the most positive impact on your program, relative to their cost and complexity to deploy and integrate. These should become your priorities, and will result in the greatest return on investment for your efforts.

Technology evaluation checklist

Questions to ask before you go shopping:

1. Which aspects of zero trust are most important to your organization?
2. What are the biggest vulnerabilities in your security posture that need to be addressed?
3. Where is your current technology letting you down?
4. What is your hosting infrastructure - self-hosted, on-prem, cloud, or hybrid?
5. How well does your technology communicate?
6. What's the level of effort to get information from one system to another or to export it for auditing purposes?
7. How efficiently can your team find what they need?
8. Do you have visibility across all of these systems? What could help with that visibility?

5. Let the buyer beware

With a shopping list in hand, federal agencies need to keep in mind that the zero trust technology market is extremely complex, filled with hype and overreaching claims by vendors.

It's important to remember that you can't buy zero trust out of a box. There is no all-in-one solution that works for every team. Your zero trust program needs to be intentionally designed and tailored for your specific organization and mission set.

Build out a detailed checklist of needed capabilities before shopping for new tools. Any technology must clearly address these specific security requirements before it is even considered for a shortlist.

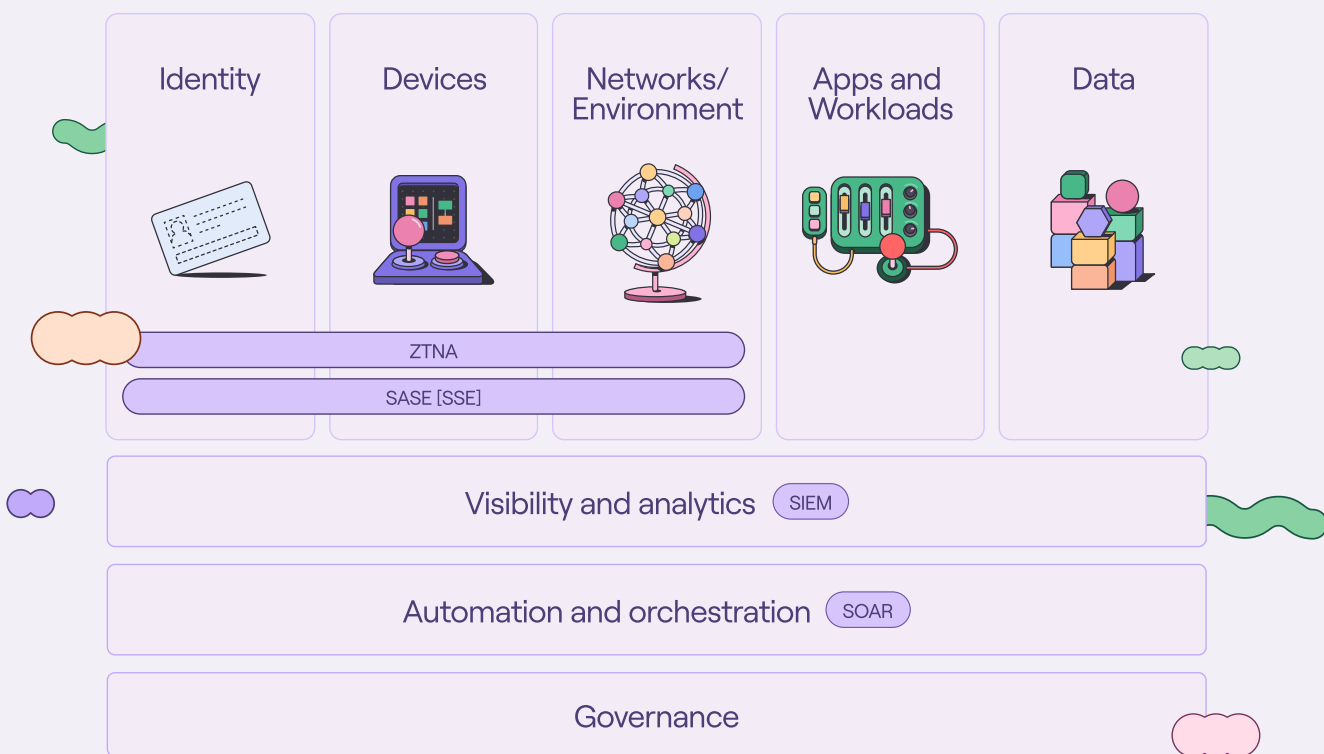
6. Select specific use cases for evaluation

Once you've created a shortlist of products, it's time to put them to the test. Collaborate with your team to establish mission-critical use cases that will help you evaluate your vendors.

Don't go easy on your vendors - choose workflows that are currently draining resources, touch multiple zero trust pillars or require multiple systems to speak to each other. And make sure to use the same use case when evaluating vendors in the same category, so you can compare like with like.

Your zero trust security tech stack: the essentials

Let's take a closer look at the key technologies and frameworks to consider when building out your zero trust technology stack. First, we'll see how these technologies and frameworks map directly to the zero trust pillars and cross-cutting capabilities.



- ZTNA is the first step into zero trust. It overlays the **identity**, **device**, and **network/environment** pillars.
- SASE is the product or suite of products that works with the tools implemented as part of ZTNA to further protect the perimeter.
- Essentially, ZTNA 2.0 would also cover **application workload** and **data**.
- SSE looks to be a subset of the SASE framework.
- SIEM falls under the **visibility and analytics** cross-cutting capability.
- SOAR falls under the **automation and orchestration** cross-cutting capability.

Now, let's look at each technology and framework in greater detail.

Zero Trust Network Architecture (ZTNA)

ZTNA replaces traditional perimeter-based security models with a dynamic, identity-centric framework that enforces strict access controls and continuously verifies and validates every access request. This access is granted based on the principle of least privilege.

So rather than building a massive wall around the perimeter of the network to prevent intruders, ZTNA assumes breaches will happen and relies instead on locking the virtual doors in all the rooms of a computing environment to limit the scope of a breach. A common way this is addressed is through network micro-segmentation.

Security Access Service Edge (SASE)

SASE technologies converge wide area networking (WAN) and security functionalities into a unified cloud-native architecture that is delivered as a service.

SASE incorporates zero trust principles and helps organizations implement secure access policies based on user identities, device health, and contextual factors across both traditional enterprise networks and dynamic cloud services. This ensures that only authorized users and devices can access sensitive resources, regardless of their location.

The most common example of SASE technology is software-defined wide-area networks (SD-WANs).

Security Service Edge (SSE)

SSE technologies, as part of the SASE framework, provide integrated, cloud-centric capabilities that facilitate secure access to websites, software-as-a-service (SaaS) applications, and private applications.

SSE supports the modern distributed and mobile workforce by enabling secure access to resources from any location while maintaining a consistent security posture.

Examples of SSE technologies include cloud access security brokers (CASB) and firewall-as-a-service (FWaaS).

Security Information and Event Management (SIEM)

SIEM refers to a set of technologies and processes used to collect, analyze, and correlate security event data from various sources throughout an organization's IT infrastructure. By implementing SIEM, organizations can improve their ability to detect, investigate, and respond to security events in a timely manner.

SIEM helps enhance an organization's overall security posture, enables proactive threat hunting, and supports regulatory compliance efforts.

Security Orchestration and Response (SOAR)

SOAR technologies provide a set of tools and features that automate cyberattack prevention, investigation, and response. They aim to streamline and enhance security operations by integrating and coordinating separate security tools into cohesive workflows.

Traditional SOAR platforms typically rely on an app-based integration model. Unless your vendor of choice has already built the specific integrations you require, these types of connections can take a lot of time and effort to develop and maintain.

A truly effective SOAR platform is only as strong as its weakest link. If it's not compatible with all the tools in your zero trust technology stack, or can't perform a desired action in that tool, then it might not work at full capability when a cyberattack hits your organization.

Automating and orchestrating for zero trust

In an ideal approach to zero trust, automation and orchestration are more than useful tools, they're essential to your agency's success. You don't need to take our word for it - security automation and orchestration is mandated by M-22-09 and M-21-31, and forms an integral part of the framework in CISA's ZTMM (zero trust maturity model).

The message from the government and security experts alike is clear - without automation and orchestration, there is no zero trust.

"There are lots of areas where automation can come into play - I think we're going to fail if we don't automate as we implement zero trust."

- DOD CISO Dave McKeown

M-22-09 | Deadline: September 2024 "CISA's zero trust model describes five complementary areas of effort (pillars) (Identity, Devices, Networks, Applications and Workloads, and Data), with three themes that cut across these areas (Visibility and Analytics, Automation and Orchestration, and Governance)."

While it's true that CISA recommends a "gradual evolution" to zero trust, automation and orchestration are listed as one of the

first steps. But that doesn't mean you have to start automating overnight. It's important to spend some time defining your automation and orchestration strategy and finding the right tools to help you execute it.

"I try to take the approach of crawl, walk, run into zero trust. You don't have to rip out everything and start over. You can be compliant with the requirements by understanding what you have deployed, and doing an internal exercise to understand what you have in place that can cover the zero trust pillars. Then you can decide what systems you need to supplement that."

- John Harmon, ex-NSA analyst and current RVP of Cyber Solutions at Elastic

So, what exactly does the government say about security automation and orchestration? How can federal agencies use automation to take meaningful strides toward improving their security posture? And what kind of capabilities do security orchestration, automation, and response (SOAR) platforms need to comply with regulations?

Let's find out.

The role of automation and orchestration in zero trust

Zero trust and automation are inextricably linked. In zero trust, users and devices are treated as untrustworthy until proven otherwise, making manual access management close to impossible. Even a large IT organization working around the clock would struggle to keep pace.

In most cases, automated workflows are the only way to implement CISA's mandate of "just-in-time and just-enough access tailored to individual actions and individual resource needs."

As agencies grapple with security events throughout their systems and cloud infrastructure, automation of security monitoring and enforcement will be a practical necessity. And without effective orchestration, you can't have complete visibility over your environment.

This is reinforced by the "automation and orchestration" cross-cutting capability listed in CISA's ZTMM.

"As agencies transition towards optimal zero trust implementations, associated solutions increasingly rely upon automated processes and systems that more fully integrate across pillars and more dynamically enforce policy decisions." - CISA's zero trust maturity model

In the document, CISA also outlines three stages in the journey to ZTMM, each requiring greater levels of protection, detail, and complexity for adoption.

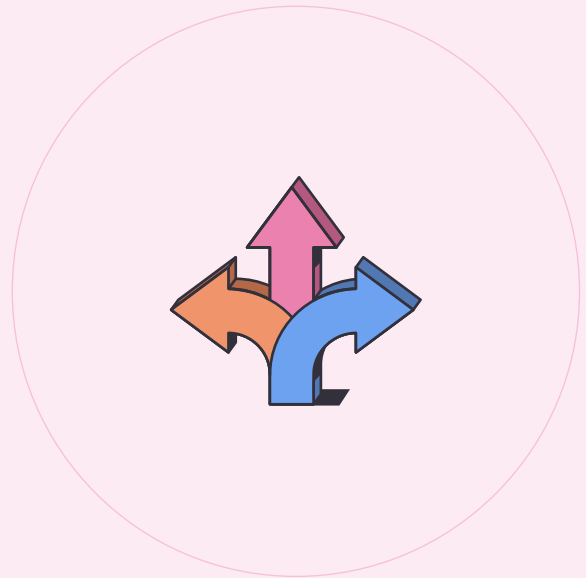
1. Initial
2. Advanced
3. Optimal

Maturity stage	Automation requirements
Initial	"Starting automation of attribute assignment and configuration of lifecycles, policy decisions and enforcement, and initial cross-pillar solutions with integration of external systems..."
Advanced	"Wherever applicable, automated controls for lifecycle and assignment of configurations and policies with cross-pillar coordination..."
Optimal	"Fully automated, just-in-time lifecycles and assignments of attributes to assets and resources that self-report with dynamic policies based on automated/observed triggers..."

Automation appears in the initial stage of the zero trust journey, which means it requires immediate attention and action.

Automation for zero trust: choosing your approach

Making security automation work - measurably improving security posture and efficiency without disrupting the daily work of the agency - will require careful tuning, iteration, and sensitivity to business needs. For an automated security system to operate effectively with a mostly hands-off approach, false positives and false negatives must be low.



Successful automation of security responses will require rich data to inform systems for orchestration, as well as permission management. This includes the protected data types and who is accessing the data.

When choosing an approach to automation and orchestration, agencies generally base their decision on their specific needs and goals. Some partner with a low-code solution, others choose SOAR platforms with a heavy code and service overhead, and others still take a do-it-yourself approach to automation.

Here are a few things to consider when choosing your approach to automation:

- Adoption speed - coding comes with a steep learning curve, meaning systems take longer to deploy
- Development speed - no-code or low-code workflow automation platforms can help your team build faster than coding
- Hosting and maintenance - high-code automation platforms can demand robust hosting infrastructure and extensive maintenance efforts

- Personnel - no-code automation enables everyone on your team to create, manage, and maintain workflows, not just engineers
- Scalability - maintaining custom scripts or code, especially as they grow in complexity, poses challenges
- Security risks - custom code can be an unintended insecure entry point for adversaries
- Cost - ineffective systems lead to costly incidents, and platforms that aren't fit for purpose can end up as shelfware

Every agency has different needs and priorities, but the list above highlights some of the key benefits of a no-code and low-code SOAR platform.

The right-fit SOAR platform will be the connective tissue of your zero trust architecture, creating a unified defense strategy by extracting data from disparate tools and orchestrating responses to potential threats. The wrong-fit SOAR platform will gather dust on the shelf.

SOAR platforms: shelfware or a fast track to zero trust?

We've already written about how you can't buy zero trust, and how vendors that promise this should be treated with caution. When it comes to choosing a SOAR, it's crucial to establish, in as much detail as possible, what you need your platform to do, before considering your options.

The truth is, many SOAR platforms are underutilized because they don't fulfill the organization's needs, or there aren't sufficient resources to support them. The problem of software becoming shelfware is well represented in data - in one study by CSO online, security leaders reported that they only use 72% of the security technologies that they purchase.

This is one of many reasons why federal agencies are moving away from legacy SOAR and towards modern platforms like Tines.

Challenges with legacy SOAR:

- Difficult and time-consuming to learn and deploy
- Requires engineers to build and manage workflows
- Long build times - playbooks can take weeks to create when they could take hours
- Lacking a relentless focus on automation and orchestration - it's often a bolted-on feature in a bigger system e.g. SIEM and TIP platforms
- Limited ability to connect to internal or external tools without a long wait time or added cost

SOAR evaluation checklist

Questions to ask before you go shopping

- What exactly do we need our SOAR platform to do? Incident response, endpoint management, etc.
- Is the platform quick to deploy? What's the onboarding process like?
- Is it intuitive to use? Can the whole team use it, or does it require engineers to build and maintain workflows?
- What's the development speed like? How long will it take for the team to build each workflow?
- Is it flexible enough to connect to all of our tools, internal and external?
- Will it work within our hosting infrastructure?



“Providers that supply broad-based, vendor-neutral SOAR... What sets these products apart is their ability to receive inputs from a broad ecosystem of security products, and organize the workflow of the security operations team. [...] Buyers who prefer the best-of-breed approach will find that SOAR still offers more flexibility, genuine vendor-neutrality, and opportunities for non security use cases.”

— Gartner’s 2023 Market Guide for Security Orchestration, Automation and Response Solutions

Now, we’ll take a look at how Oak Ridge National Laboratory, a federally-funded research organization, used a no-code, low-code workflow and automation platform to reach their zero trust goals.

Case Study

Oak Ridge National Laboratory

Oak Ridge National Laboratory (ORNL) faced the complex task of implementing the zero trust framework while managing a rotating security automation team.

They needed:

- A way to quickly automate a large number of processes that require continuous monitoring and reporting
- A platform that could connect internal and external systems in their wide and varied tech stack
- A system that could be easily used and managed by anyone on ORNL's security team, which includes team members who can't code, and team members who regularly step out for military training and deployments
- Increased metric evaluation and reporting capabilities

Pete Wood, Lead Engineer, used a phishing analysis workflow to test several vendors. Tines was the only platform that was able to achieve this in the eight-week timeframe.

Mike Crider, Cyber Vulnerability Analyst, explained,

"It was a game changer during onboarding when we could connect all our systems. We have a lot of tools in our environment. Anything that has a backend API, we're now using Tines to tie into that tool. Our ability to integrate new tools has taken out so much of our everyday tasks from before."

The team now uses Tines for:

- Organization-wide reporting
- Curating and combining information across databases
- Vulnerability management
- Cyber threat intelligence
- Endpoint management
- Firewall rule management
- Forensics
- Digital investigations
- Incident response

Before Tines	After Tines
<ul style="list-style-type: none"> • Managing automation through manual scripts • Only engineers could build, maintain or manage workflows • Long waiting periods • No automated reports 	<ul style="list-style-type: none"> • Managing automation through a flexible, scalable workflow platform • Anyone on the team can build, manage, and monitor workflows • No waiting period • Automated reporting leading to improved visibility and time savings
<p>“[Automation] was very one-off and manual. Writing individual scripts to try to automate many different applications is a tough thing to do... This was not only time-consuming but also meant only a subset of the team could actually manage their automations.”</p> <p>- Larry Nichols, Cyber Enhancements Group Lead, Oak Ridge National Laboratories</p>	<p>“With Tines, the other teams now have the power to build the playbooks themselves. They don’t have to wait on the engineering team anymore. The power is now in their hands.”</p> <p>- Larry Nichols, Cyber Enhancements Group Lead, Oak Ridge National Laboratories</p>

“Our zero trust strategy relies heavily on integration and automation. With Tines, we’re able to quickly and easily build integrations and automated workflows across our tooling to ensure our zero trust-related processes are repeatable and reliable.”

– Maria McClelland, Chief Information Security Officer, Oak Ridge National Laboratories

Tines: automation and orchestration for zero trust

Tines stands out from other SOAR solutions because of its intuitive and flexible design.

Unlike many SOARs, Tines offers a no-code or low-code interface that the whole team can use – there’s no need to wait for a developer to build or edit workflows, and no chance that it will become shelfware.

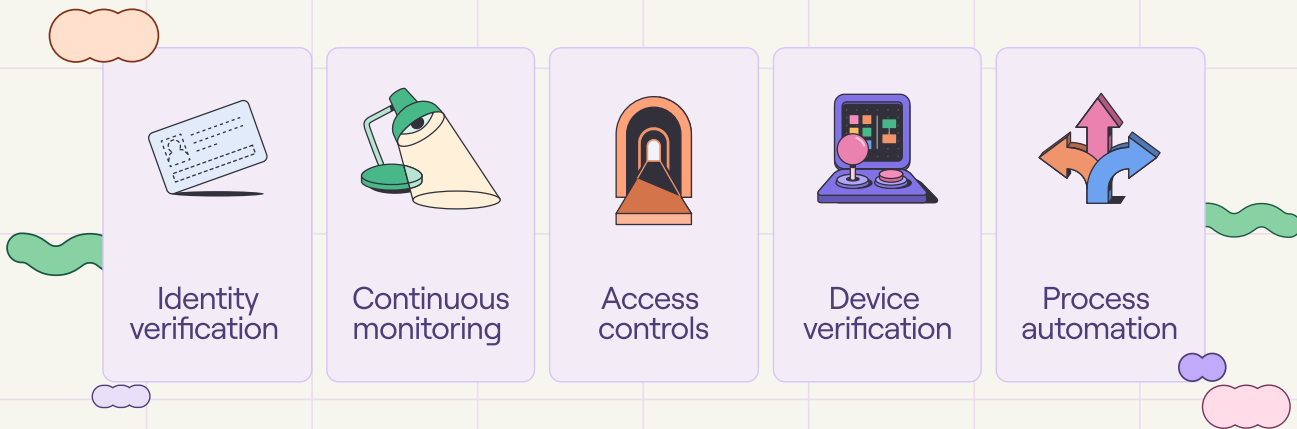
The platform’s unique approach to integrations makes it easy to connect to any tool that offers an API. This also makes it adaptable to changes in other technologies. As one customer put it, “No matter how many tools you change, you can keep Tines in place.”

Tines’ workflow interface, “storyboard,” is both documentation and automation. From action descriptions and annotations to viewer roles, there’s little to no need for external documentation. It’s all in-line and legible from the storyboard. This drives consistency and helps compliance with executive orders, particularly when combined with a next-gen SIEM like Elastic.

Why federal agencies choose Tines:

- Fast, easy implementation
- Designed for the whole team to use – anyone can build and manage workflows
- Integrates with any tool, internal or external, that offers an API
- Deployed where you need it – self-hosted, on-prem or hybrid
- Adaptable to changes in your tech stack
- Provides the controls you need to reinforce your security posture
- Documentation capabilities drive consistency and aid compliance
- Capable of handling massive complexity
- Allows teams to still use code when it’s needed

Tines and zero trust framework



Tines users can choose from hundreds of pre-built, end-to-end playbooks that they can import and customize to meet their agency's needs. Let's take a look at some popular use cases and workflows for federal agencies pursuing zero trust.

Identity verification

Monitor application access changes in Okta

Tools: Okta

Implement access control policies for multifactor authentication and access controls.

[SEE IT AT TINES.COM/LIBRARY](https://tines.com/library) ↗

Continuous monitoring



Discover and monitor unmanaged devices using Axonius

Tools: Axonius, Jira, Shodan

Auto-remediate identity and device verification to reinforce security protocols.

[SEE IT AT TINES.COM/LIBRARY ↗](#)

Device verification



Investigate & remediate critical container vulnerabilities in Aqua Security Cloud Workload Protection Platform

Tools: Aqua Security, Jira

Automate device profiling, endpoint security, and threat intelligence in a bring-your-own-device economy.

[SEE IT AT TINES.COM/LIBRARY ↗](#)

Access controls



Block suspicious IPs by creating firewall rule groups with CrowdStrike

Tools: CrowdStrike, Slack

Control access across environments and applications dynamically.

[SEE IT AT TINES.COM/LIBRARY ↗](#)

Process automation



Implement data loss prevention policies

Tools: Google, Panther, Slack

Enrich, prioritize, de-duplicate, and auto-respond to alerts and incidents for scaled security response.

[SEE IT AT TINES.COM/LIBRARY ↗](#)

The quickest path to zero trust

Federal agencies are at a critical junction in the journey towards zero trust. Next-gen technology solutions can help them get there faster, but only if their zero trust program has been intentionally designed and tailored for their specific organization and mission set.

Earlier in the whitepaper, we explained that zero trust is not a product, it's a process. But systems like Tines can be critical to an agency's success. With the right tech stack, agencies can not only meet requirements, but take meaningful strides towards improving their security posture and fortifying their defenses against evolving threats.

Smart, secure workflows for SOAR and beyond

Visit tines.com/federal to learn how Tines can help you reach their zero trust goals and reinforce their security posture.



Resources

CISA's zero trust maturity model

https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

Gartner's 2023 Market Guide for Security Orchestration, Automation and Response Solutions

Zero Trust as a Kill Chain by Don Yeske

<https://www.linkedin.com/pulse/zero-trust-kill-chain-don-yeske-ehrb/>

"Crawl, walk, run into zero trust": a Q&A with Elastic's John Harmon

<https://tines.com/blog/zero-trust-elastic-john-harmon>

Pentagon's CISO warns that zero trust will 'fail' without automation

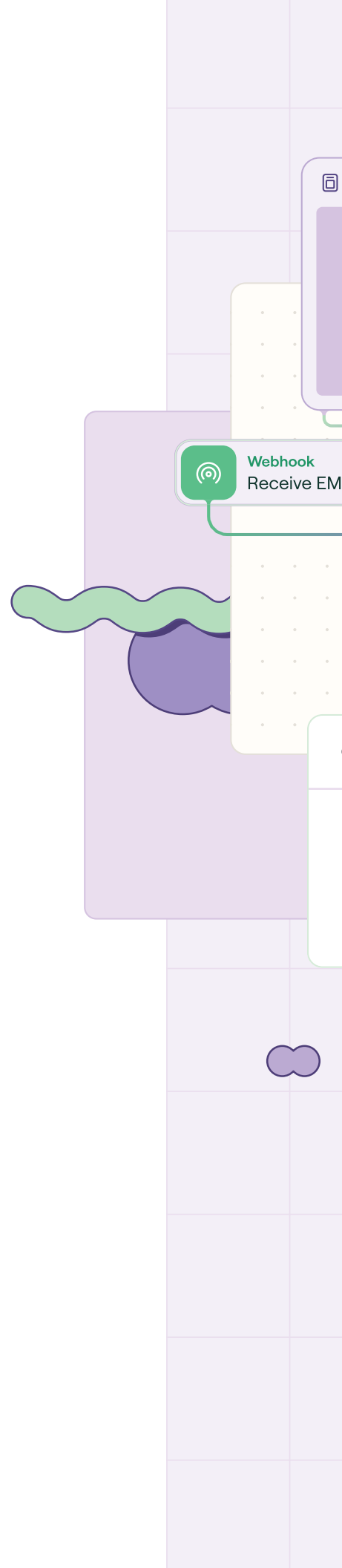
<https://defensescoop.com/2023/05/23/pentagon-dod-zero-trust-automation-dave-mckeown>

Inside cybersecurity's shelfware problem

<https://www.csoonline.com/article/570333/inside-cybersecurity-s-shelfware-problem.html>

Oak Ridge National Laboratory taps into the unimaginable with Tines

<https://www.tines.com/case-studies/oak-ridge-national-laboratory>



Upload EML file for analysis 356



Receive email 124k
Receive email

Trigger 73k
If email has attachment

Event transform 73k
Add reporter

L file for analysis 92k

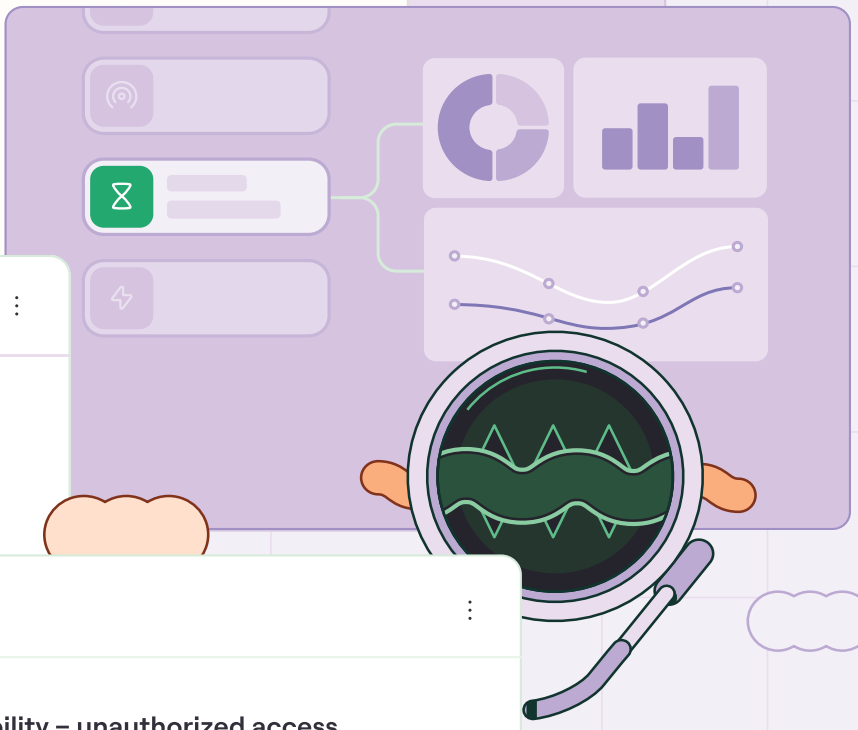
Send to story 165k
Analyze Headers in IP Quality score and IP-API

Cases resolved




716

Records

2,923



☰ High priority cases

- 
Active Azure vulnerability – unauthorized access
 #721 • Created 33m ago • 2 comments
High Database A
- 
Investigate Elastic anomaly
 #720 • Created 1h ago • 1 comment
High IOC B R
- 
Check NVD for similar incidents
 #719 • Created 3h ago • 4 comments
High Incident response R Y O

