

Software-defined law enforcement

Platform needs for first responders

Executive summary

Law enforcement agencies are facing unprecedented challenges in dealing with technology-savvy criminal organizations, as well as state and commercially sponsored threat actors. Modern organized crime operates across national borders, using sophisticated tools and cloud infrastructure and creating unprecedented challenges for law enforcement agencies. The large volumes of crime-related data make it difficult to identify and prosecute criminal organizations. Instead, intelligence-led enforcement agencies have to deal with a high signal-to-noise ratio in the stream of data. Examples of international success such as [Operation Ironside](#) in 2021 tend to result from years of tried and trusted police work to compromise encrypted communications run by criminal organizations.

The ability of tech-savvy criminal organizations to test the system and adopt new technologies is pressuring law enforcement agencies to respond with speed, using systems that scale. However, law enforcement organizations are often hampered by technical debt, legacy applications and services, and isolated team structures that limit collaboration. Their processes and IT systems also have to comply with government regulations around transparency and accountability. For example, system design activities often include prosecution representatives who protect the chain of custody of evidence, ensuring those systems stand up to legal scrutiny.

In law enforcement, speed, scale, and trust traditionally have a relationship based on tension and compromise similar to how project managers have to balance time, scope, and cost. A platform-based architecture supports a coordinated approach to achieve speed, scale, and trust across law enforcement teams, legal and information technology processes, and systems.

Intelligence-led law enforcement using a platform-based architecture

How do law enforcement agencies solve for speed, scale, and trust while under the scrutiny of the judicial system?

These agencies need a modern IT platform that supports flexible, streamlined interactions with agency partners.

“A law enforcement agency’s relationship with its community relies on two-way communication and effective partnerships.”¹

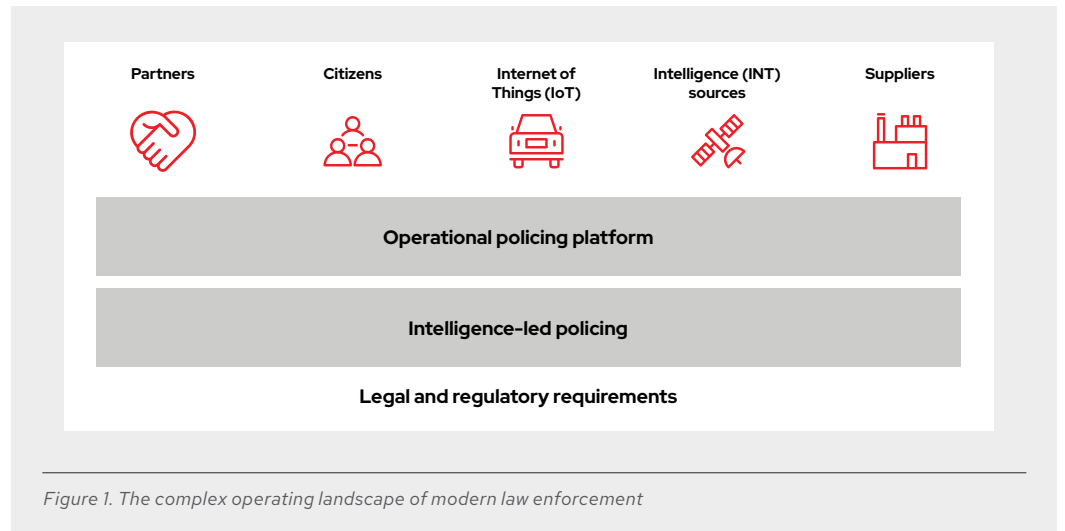


Figure 1. The complex operating landscape of modern law enforcement

Partners

Law enforcement agencies have an increasing need for cross-agency and interjurisdictional collaboration in response to the globalized nature of crime and the challenges of enforcing laws around digital activities across borders. The traditional methods of information sharing do not scale with the new pace of operations. There is a pressing need for automated information sharing and governance supported by a set of managed application programming interfaces (APIs) and event streams.

Front-line officers and citizens

In the past, delivering an enhanced user experience has not been a priority among many law enforcement agencies. However, as new community engagement applications have been deployed and tested, agencies have seen their positive impact on building trust and relationships with the communities they serve, improving social and law enforcement outcomes.

Well-designed chatbots and virtual assistants quickly provide relevant information and simplify the citizen experience, helping to reduce officer workload and build goodwill. Additionally, research has shown that chatbots with enhanced empathy-based frameworks ask questions to increase user engagement and provide data points that form part of predictive policing capabilities.¹

Technology can improve how first responders engage their communities. However, the additional information these systems provide comes with the risk of cognitive overload, especially when used at the end of a tiring shift. The combination of stressful interactions, a tired officer, and cognitive overload can lead to suboptimal or even dangerous outcomes. Historically, research on fatigue by the military² and aviation industries³ has shown how a combination of fatigue, stressful situations, and a complex environment can lead to degraded performance and fatal incidents. Personnel should not be overwhelmed by information—instead, they should be given simple next-best-action instructions informed by context and delivered at the right time to deliver higher quality outcomes.

¹ Norris, Dave. “Artificial Intelligence and Community-Police Relations.” *Police Chief*, June 2019.

² Kingston, Donald L. “Hurtling Toward Failure Complexity in Army Operations.” *Military Review*, Aug. 2014.

³ Gawron, Valerie J. “Summary of Fatigue Research for Civilian and Military Pilots.” *IIE Transactions on Occupational Ergonomics and Human Factors*, vol. 4, no. 1, 2016.

Internet of Things

The Internet of Things (IoT) and connected sensors have become useful for more than just predictive maintenance. Emerging use cases allow these technologies to impact the physical environment in which people live in real time. Law enforcement has quickly begun using connected sensors for faster evidence collection, incident response, and crime control. The Video Doorbell Burglary Initiative in London is a prime example of law enforcement deploying connected devices to reduce the impact of crime.⁴ The Metropolitan Police Service (MPS) proposed that they provide smart video doorbell devices to people living in high-volume burglary areas as both a deterrent and an evidence-gathering system.

Connected devices highlight two information technology and communications (IT&C) challenges. First, traditional systems are designed to support the scale and elasticity required to deal with the ingestion, processing, integration, and prompt analysis of large data streams. Secondly, vendors often use different standards, and already stretched IT organizations cannot connect with these IoT data sources fast enough, especially using legacy processes and integration tools.

Unstructured intelligence

For years, law enforcement agencies have been working to access and take advantage of the expansive set of unstructured data from open source intelligence sources (OSINT). They are also looking at combining the OSINT data sources with human intelligence (HUMINT) sources to preempt threats and inform evidence collection, processing, and prosecution efforts. Over the last decade, niche solutions have emerged to ease the ingestion and analysis of unstructured data sources for intelligence purposes. The rise of data science is changing how organizations expect to interact with the output from these solutions.

The models that data scientists produce need to deliver the same performance once deployed in production and run alongside existing services in a supportable manner. Data scientists need to be able to use proven software engineering practices and governance processes using automated workflows. The algorithms and models they produce should progress through development pipelines just like other code does and run on a security-focused platform that delivers the expected qualities of service. Providing data scientists with these capabilities facilitates repeatability and reproducibility in intelligence-led law enforcement, supporting fair and consistent evidence collection and processing.

Software providers

An underutilized benefit of modern declarative infrastructure is the ability to provide production-like environments for external software developers and vendors. This capability allows developers to showcase and test their applications within an organization's constraints. As a result, law enforcement agencies can assess how well applications comply with their governance requirements earlier in the software provider supply chain, speed software evaluation processes, and reduce implementation risks.

Agencies can also use declarative infrastructure to gain access to a broader set of skills through develop-low-deploy-high development and delivery models.

A platform that supports stakeholders with these capabilities—with speed, scale, and trust—operationalizes data streams for intelligence-led policing. Law enforcement systems can better process data and produce insights that augment the core policing platform for improved citizen experience, faster response to crime, and ultimately safer communities.

⁴ *"Video Doorbell Burglary Initiative."* Greater London Assembly, June 2019.

Speed, scale, and trust

Kubernetes has become the preferred engine for platforms that provide declarative infrastructure to line of business developers. However, Kubernetes by itself often does not provide sufficient enterprise capabilities for development, security, and operations.

A platform supporting DevSecOps teams with speed, scalability, and trust is an essential operational capability for the modern law enforcement agency.

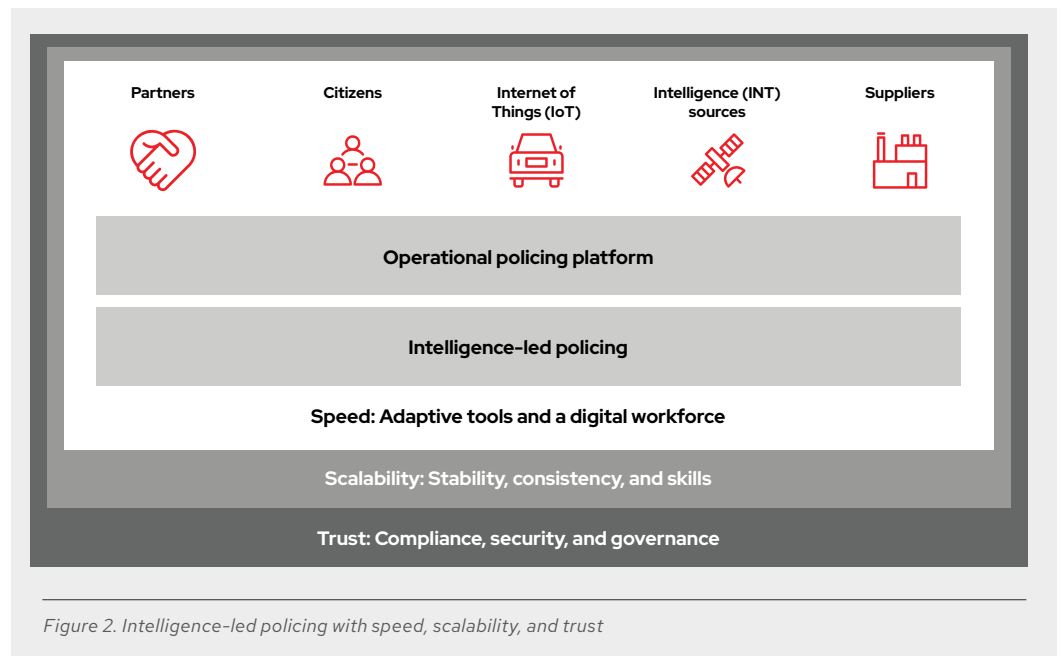


Figure 2. Intelligence-led policing with speed, scalability, and trust

Equip developers, data scientists, and partners to act with speed

When choosing a platform for your organization, think about the ecosystem of capabilities and third-party software on the platform. Providing everything from API management through automation to artificial intelligence and machine learning (AI/ML) capabilities via a catalog on the same platform provides developers with a consistent set of procedures and tools that ultimately speed delivery.

Kubernetes can be cumbersome for new developers to learn, so consider Kubernetes distributions that provide a low barrier to entry through capabilities such as development environments-as-code, source-to-containers, and parity in the graphical and command-line interfaces. Using platforms with these capabilities reduces the skills gap and accelerates the time-to-value for your organization.

Allow operational teams to scale skills and workloads across environments

The right Kubernetes platform provides the consistency that allows workloads to run in different environments as dictated by the application configurations. For example, a Kubernetes platform allows you to burst out a workload to hyperscalers during a short period of intense intelligence gathering or run Kubernetes in edge environments on forward-deployed command centers.

Look for a Kubernetes platform that allows your workloads to run the same anywhere—whether you are using a hyperscaler or other underlying infrastructure providers—and provides integrated policy automation. This consistent management approach allows operations, development, and security teams to scale their knowledge and skills across different infrastructure and cloud providers.

Maintain trust within the platform as part of the service

Trust is the combination of applying the right security and compliance policies consistently and transparently across the complete life cycle of an application or platform.

The US Department of Defense (DoD) [DevSecOps reference design](#) describes the adoption of platform-based architecture as an opportunity for operations and security teams to build governance and compliance into the services that developers consume.⁵ The document also shows the need for trust in Kubernetes to be applied top to bottom, as higher levels inherit the controls from the components they consume.

Using this approach, the National Geospatial-Intelligence Agency (NGA), for example, has expedited their Authority to Operate approval process from 6–18 months down to a single sprint using Red Hat® OpenShift® to further the agency’s hybrid cloud strategy.⁶

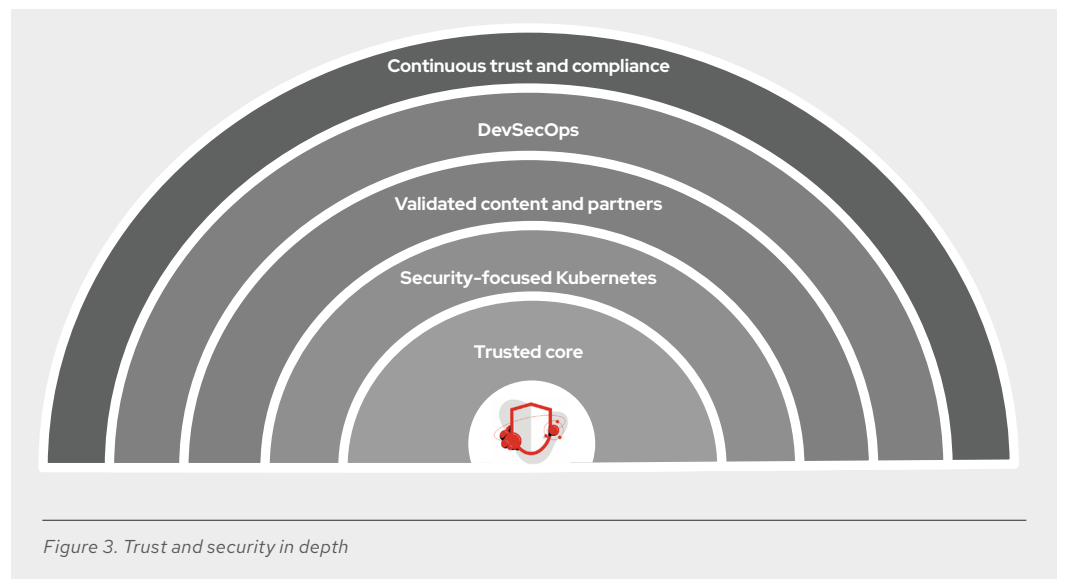


Figure 3. Trust and security in depth

To successfully execute a cloud strategy that supports intelligence-led law enforcement, your organization needs a Kubernetes platform that simplifies and improves the security of your DevSecOps processes. Make sure that your platform provides the appropriate levels of trust:

- ▶ The Linux® distribution that forms the heart of your platform needs to come from an organization with a proven security and enterprise track record. Kubernetes orchestration and security build on Linux’s ability to run processes securely and stably.

⁵ “DoD Enterprise DevSecOps Reference Design.” Department of Defense, Aug. 2019.

⁶ Red Hat video. “OpenShift at National Geospatial-Intelligence Agency James Cherry OpenShift Commons Gathering 2019.” YouTube, May 2019.

- ▶ Not all Kubernetes platforms are designed and developed with the same level of rigor and security in mind. Think about the workload isolation capabilities and the security, context, and constraints control you require. Having the right security capabilities could be the difference between rushing to patch your systems when a critical vulnerability is published and executing a measured, planned incident response, confident in the knowledge that your platform mitigates the vulnerability through good configuration.
- ▶ Your Kubernetes solution should include access to certified content and robust base containers that apply sound security practices from the start and help you avoid simple pitfalls like running containers with unnecessarily elevated privileges.
- ▶ Look for a partner that can accelerate adoption with blueprints and prior experience. Red Hat contributes to community projects around DevSecOps as a baseline for building trusted software supply chains with initiatives like the open source [Ploigos project](#).
- ▶ An integrated Kubernetes-native security capability is critical. Red Hat fields many security questions around continuous vulnerability and compliance management, automated threat detection, analysis and response, and network segmentation. Consider how the platform allows you to shift traditional runtime policy enforcement left to the development cycles.

Learn more

Modern policing has changed with the rise in globalized crime. There is a need to act with greater speed and agility and an opportunity to tap into the explosion of data. Software-defined policing platforms built on Kubernetes are essential to build greater community trust and keep pace with digitally equipped and savvy criminals.




Few Kubernetes vendors can credibly help organizations deliver workload where the mission demands it, while providing the required versatility, speed, scale, and trust. [Red Hat OpenShift](#) allows organizations to adopt more agile processes and practices. When your teams can safely increase delivery speed, they tend to develop a learning culture built on collaboration, leading to more significant innovation and better overall outcomes.

To learn more about how Red Hat can help law enforcement IT innovate, visit redhat.com/nationalsecurity.



About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. [A trusted adviser to the Fortune 500](#), Red Hat provides [award-winning](#) support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.

 facebook.com/redhatinc
 @RedHat
 linkedin.com/company/red-hat

North America
 1 888 REDHAT1
www.redhat.com

**Europe, Middle East,
and Africa**
 00800 7334 2835
europa@redhat.com

Asia Pacific
 +65 6490 4200
apac@redhat.com

Latin America
 +54 11 4329 7300
info-latam@redhat.com