ZERONORTH™

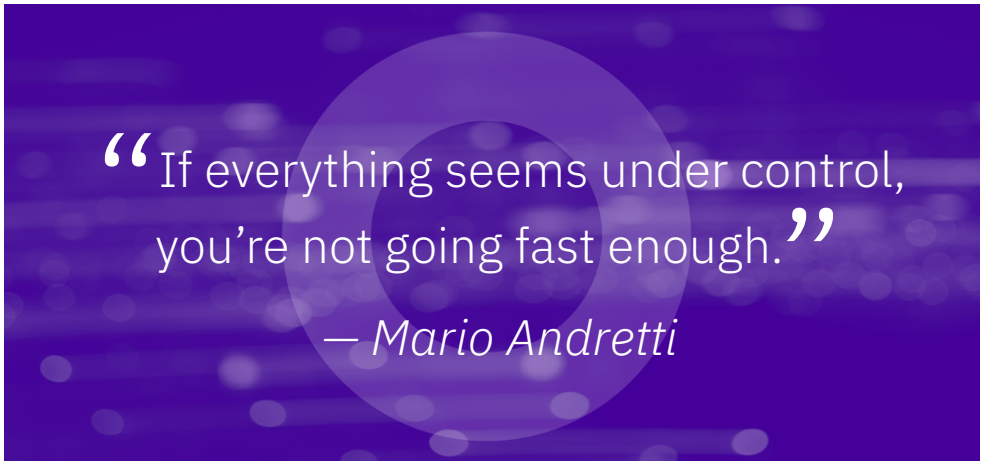
Federated Responsibility for AppSec: A New Model to Power Secure DevOps

A ZeroNorth White Paper

The Federated Responsibility Model

As DevOps has revolutionized software development in terms of speed, capability and agility, securing the software development life cycle has become table stakes for CISOs. Ready or not, organizations put themselves at risk when application security (AppSec) and developers do not share a common vision on how to deliver the secure software capabilities required by the business. Making sure security is integrated throughout the software development life cycle (SDLC) cannot be solved through technology alone.

Beyond tools, secure DevOps requires a fundamental shift in mindset and approach, moving from product to program, from ownership solely within corporate security to a federated, shared model of responsibility that spans security and software organizations. Only through this Federated Responsibility Model for AppSec can enterprises consistently deliver secure applications at the speed of innovation.



The Cultural Divide Between DevOps and Security

The pervasiveness of public clouds, containers and microservices in the enterprise has transformed software development and its practitioners. Product features are continually released at a rapid pace and on a rolling basis through a series of agile practices. New technologies and tools that automate development processes are allowing many organizations, from medical technology to software vendors and financial services, to accelerate innovation and time to market. In contrast, we find security teams are still following the same playbook they have been using for decades, which is largely tool-based and centered on an obsolete mode of command-and-control.

The reality of application security today is that organizations have no visibility into their application risk. They don’t have a clear picture of critical vulnerabilities. They aren’t able to assess the potential

business impact of these vulnerabilities. They lack the ability to prioritize their vulnerabilities, so attempts at remediation thus far actually slow down the development process. This shift stirs up conflict and mistrust between the development and security teams.

This conflict is exacerbated when AppSec and developers do not share a vision for delivering secure software capabilities required by the business. Organizations put themselves at risk when the software and security teams fundamentally are not aligned in the prioritization and implementation of security in software development. When AppSec and DevOps cannot agree on the organizational responsibility for security and the integration of security throughout the development process, a cultural divide emerges.

The perception of security as a hindrance casts a shadow and widens the gulf. This cultural divide, or the lack of common vision between corporate security and developers (and their inability to work collaboratively), must be resolved before developers can build and deliver secure code quickly and continually: 77% of developers say the cultural divide affects their ability to meet deadlines, and 70% of AppSec professionals believe it puts the security of applications at risk.[1]

The Federated Responsibility Model is an approach to application security that bridges this cultural divide between software engineers and security teams. In this model, which promotes shared accountability and ownership, the role of the CISO can evolve into that of an advisor and coach, providing the framework, objectives, motivation and tools for secure DevOps to be successful. In other words, the CISO becomes the enabler for both the business and developers, without getting in the way. Only through building strong partnerships between product and security teams—and equipping them with capabilities that automate security for DevOps—can these organizations create and sustain the velocity their business mission requires. This paper explains how CISOs can adopt the Federated Responsibility Model as a programmatic approach to AppSec through the following phases:

1. Defining the Federated Application Security Model
2. Laying the Foundation for Federated Security Policy and Enforcement
3. Identifying the Federated Responsibility Architecture
4. The Shifting Role of CISO

Defining the Model

Under enormous pressure to move quickly, development organizations have decentralized IT and leveraged automation and agility to better support the business. Within the new world of DevOps, however, AppSec governance and operations represent different responsibilities for different organizations. In the Federated Responsibility Model, roles and responsibilities that were previously siloed among corporate security, product security, operations and development must be integrated.

In the traditional model for security, corporate security leaders centralize all aspects of security, risk management and compliance. CISOs and their teams establish and oversee policies across the enterprise. Corporate functions and business units must adhere to these policies or face consequences for violations. Corporate security policies are set (and sit) for long periods of time; change is the exception, rather than the rule.

On the flip side, product security teams are chartered with ensuring the security of their respective product lines and understand, better than anyone else, the risk these businesses are willing to accept. These teams also recognize the importance of the delivery requirements placed on developers. In this context, product security should be freed to support their product lines at the speed of business, while also ensuring corporate security and risk management frameworks are addressed.

[1] Source: Ponemon Institute research report, "Revealing the Cultural Divide between Application Security and Developers"

Too often, however, a development team on the eve of pushing out new code is stopped dead in its tracks because of late-breaking reports from security on discovered vulnerabilities and quality issues. So the business is left between the proverbial rock and hard place. Either plow ahead with launch and fix quality issues in a subsequent release, which opens up potential liability and harm to revenue and reputation, or halt production to fix last-minute security tickets.

Just as DevOps has radically changed IT, security must also decentralize in order to remove obstacles and go faster. But when it comes to governance in this new world of DevOps, who should set the policy? Who should measure performance against the policy and report results? Who can help those actually responsible for operations improve? With regard to operations, w*ho is really responsible for security?*

Integrating Governance, Operations and Security

In the Federated Responsibility Model for AppSec, all four elements—corporate security, governance, product security and operations—come together into an integrated partnership (see Figure 1). Today, the CISO champions cybersecurity regardless of which team across the enterprise is creating and pushing software into production. Not surprisingly, the CISO or corporate security leader is ideally suited to set enterprise-wide standards for risk and compliance given the broad nature of these requirements, while the product security leader, being closer to the product, can best apply these corporate standards to the AppSec and development processes. Security takes on governance for which it is naturally suited. Corporate security can continue to set organizational security policy, maintain corporate security visibility, measure the overall risk to the business, and advise product security and operations teams. With a continuous application security program in place, the CISO and his or her team can assume the role of coach, providing AppSec expertise to driver further improvements. DevOps becomes the enforcer.

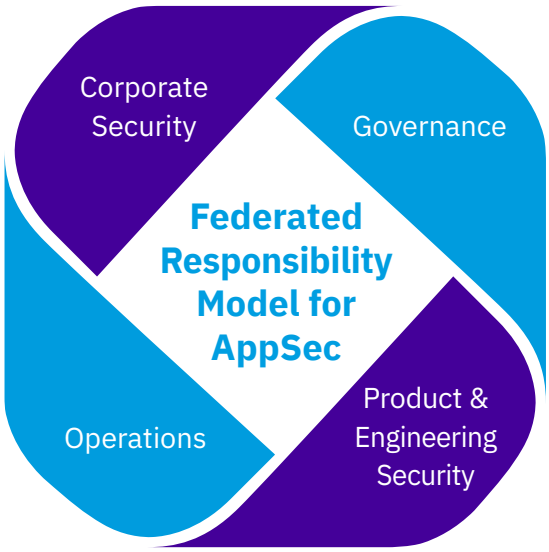


Figure 1. The Federated Responsibility Model for AppSec integrates governance, operations, corporate security and product security.

In the federated AppSec program, DevOps, product and engineering teams now own the actual operations and implementations of the model. Consequently, product security teams are empowered to own the security of their applications. The corporate security team can provide policies and tools that enable the software engineering and product security teams to consistently integrate security at each stage of development, with the agility and velocity of DevOps. If the CISO sets the standard, DevOps teams ensure standards are enacted and visibility is available to support the security, risk and compliance requirements of the enterprise.

As the walls between development and security dissolve, the extent of shared responsibility in this new model, and delineating the boundaries to make the solution work, is unique to each organization. Development and security teams must strike the right balance for their own enterprise to create an integrated partnership that aligns product and corporate security, risk and compliance with the needs of the business. The question is: how does this new alignment and transformation occur without disrupting the flow of software getting out the door?

Laying the Foundation for Policy and Enforcement

Even as responsibility for AppSec is shared, we must keep the mission clearly in sight: enable DevOps to rapidly and securely deliver innovation. The federated approach to AppSec achieves this by maintaining enterprise control, accelerating software pipeline velocity and unleashing developers.

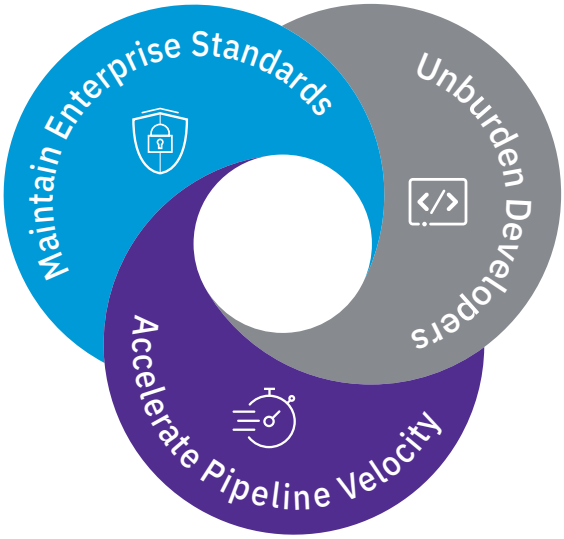


Figure 2. The foundation of Federated Responsibility Model for AppSec is about enterprise control, pipeline velocity and DevOps empowerment.

Maintain Enterprise Standards

Enterprise control needs to meet consistent corporate standards for security performance. Security standards provide an understanding of risk across the enterprise and prevent exceptions made by product line or business unit. Global controls allow security leaders to define, manage and report against corporate and compliance requirements. Unified security standards, policies and analytics let CISOs and security leaders take a global view of risk and gain a holistic perspective on their organization. They can then streamline the risk mitigation processes for compliance-related vulnerabilities and measure progress against SLAs.

With this holistic view of risk across the entire application portfolio, corporate and product security leaders can pinpoint key gaps, identify needed AppSec enhancements and take the right steps to continuously improve the enterprise security posture. With insight into an organization's AppSec program and performance, the extended security team can gain real-time access to a full list of applications in the portfolio and clarity into the relationships between them.

Maintaining standards also makes it easier for security leaders to bring together normalized intelligence to identify patterns and trends, make informed business decisions on application risk and provide board-level reports and analyses on the health of the business.

But because each business and application has different requirements and risk criteria, the risk profiles will not be the same. Centralized standards are necessary, yet enterprises must also allow these security policies to be enacted locally, based on risk criteria that are specific to the line of business or application. This redistribution of security responsibility is critical.

The development teams are best positioned to ascertain this criteria, such as whether an application drives revenue, who will use it or the type and sensitivity of the data. Development teams can then enact policies based on the application business risk and enforcement locally.

Accelerate Pipeline Velocity

The flexibility of the shared model to enforce policy both locally and at the product level helps accelerate application delivery. Velocity is the litmus test.

Arming security and product teams with local enforcement and product control allows for seamless integration of security throughout the development life cycle. This makes it easier to incorporate

technology that orchestrates continuous discovery and remediation of vulnerabilities within DevOps pipelines. This allows software engineers to fix code while they are developing without slowing delivery. They avoid having to go back weeks or months down the line when it's far harder or nearly impossible to do without severe consequences to schedules, quality and culture.

DevOps taking on responsibility for security requires centralizing, normalizing and streamlining vulnerability findings into meaningful and manageable outputs that can be remediated much faster and with less effort. Speeding up vulnerability discovery and remediation also reduces friction between the security and development teams. Transparent and seamless security lets developers move at the pace of development. Security and product teams can take action quickly and confidently. Velocity is now built-in. This is the promise of DevSecOps: security as code at the speed of DevOps.

Unburdening Developers

By facilitating pipeline velocity, federated AppSec delivers a value proposition that empowers developers. Because DevOps is a decentralized, distributed model, it embraces entrepreneurship and agility. Security must be addressed as part of the development process—but must be enforced through processes and systems that drive (not drag) development velocity. Security teams should help developers meet security standards without touching their workflows. They should enact security in the background, without developers having to interact with security tools (unless they specifically want to). Alternatively, security can enable developers to use the tools they choose, while still providing corporate visibility. If a development team wants to procure and use a specific tool, let them. It needs to be incorporated into the broader program to ensure it's part of and contributes to the centralized, normalized view.

This centralized view should prioritize the vulnerabilities based on business risk and compress the findings down, so developers are only fixing what is deemed to have the most impact. Creating a flood of tickets for DevOps that are not properly assessed, or are duplicates, is a common and huge problem, almost like a denial-of-service attack that takes teams out of commission.

Streamlining and prioritizing vulnerability remediation based on the potential impact is the key to making AppSec transparent and friction-free for developers. Through the integrated Federated Responsibility Model, security lightens the load for developers by partnering as policy advisors to help them improve their AppSec performance without changing their workflows or swamping them with unimportant issues. Organizations can now meet enterprise standards and control requirements, while empowering the security and operations teams with the structure, rulesets and technology needed to deliver secure applications at the velocity the business demands.

Architecture of the Model

While the shared responsibility model is holistic, centered on people and process, the technology component cannot be overlooked. Too often, security teams are forced to manage multiple tools, each requiring a breadth and depth of expertise that is highly expensive, complex and unsustainable over time. Security analysts are put in the position of making incorrect assumptions about the data being presented because of the significant differences in reporting from one tool to the next. Without automation, multiple security teams armed with multiple tools cannot rationalize and normalize their data. Security analysts end up making poor decisions about remediation based on bad data, leaving their companies exposed to a possible breach, IP theft or other catastrophic loss.

Emerging technologies with the ability to compress and reduce noise down to only the most critical elements of developer productivity are needed. These capabilities enable the federated model and contribute significantly to the acceleration of development pipelines through:

Centralized management platform powers secure DevOps

Orchestration deploys and automates security scanning tools across disparate DevOps pipelines

Intelligence compresses, normalizes, analyzes and correlates security scan results based on business or product-line risk

Streamlined remediation, enabled by intelligent, orchestrated scans integrated with DevOps tool chains, removes friction between DevOps and security

Analytics and reporting delivers board-ready risk dashboards that support enterprise, business and product line requirements

The Shifting Role of CISO

As the champion for enterprise security, the role of CISO should set the standards, define security policies and centrally set the bar. That means CISOs need to set expectations for performance and remediation. To do so, they must be able to codify risk management policies into the enterprise control model and gain access to enterprise-wide reporting. This is critical because, with metrics and reporting capabilities at the board level, at the C-level, at the business unit level and at the product team level, they can implement a continually-improving program and eliminate friction between teams.

Overcoming the cultural divide today between security and development is critical to the CISO's mission of supporting fast, secure application delivery to the business and its customers. The CISO's role will continue to help break down organizational barriers so automation (if it's in place) can help bring about shared responsibility for security. To remove existing obstacles, the CISO should develop programs, processes and systems that enable developers to drive security within their teams on a continuous basis, and with repeatable consistency. By aligning security with the pace of development, CISOs can finally make security transparent to developers while eliminating animus and disruption.

The Federated Responsibility Model transforms the approach to application security and helps the CISO bring value to the executive leadership team and the business. This shift gives CISOs a seat at the table. As stewards and advisors for security, CISOs can help software teams work together effectively while also delivering enterprise-wide control, velocity and empowerment.

The federated AppSec approach shifts the importance of software away from the sidelines and back to the center of organizational success. With the movement to DevOps, application security is now the responsibility of many. Business, security and development teams are united through a federated application security program and ready to improve security while reducing risk. Sharing the vision and responsibility for security can be a positive force for the business, for AppSec and for the good of software.

The Federated Responsibility Model's Value to CISOs

- **Balance the need for centralized security policy with the velocity of agile development**
- **Partner with business, product, engineering and operational teams**
- **Inspect the deployment of AppSec strategies across development teams and tools and audit it all at the application, business unit and corporate levels**
- **Support governance with automated, granular reporting**
- **Motivate development teams to prioritize security without sacrificing agility**

Next Steps

1. Read the Ponenom Institute's Report on the Cultural Divide

2. Analyze potential cost of vulnerability discovery with the **ZeroNorth TCO calculator**

3. **Schedule a demo** to speak with a security automation and orchestration specialist

ZERONORTH™ ZeroNorth brings security, DevOps and the business together to improve application security performance and reduce organizational risk. The company's application security automation and orchestration platform unites enterprises to rapidly identify, prioritize and remove the vulnerabilities standing in the way of software excellence. In an age where the security of applications needs to be everyone's responsibility, ZeroNorth is where organizations come together for the good of software. For more information, follow ZeroNorth on Twitter (@ ZeroNorthSec), or LinkedIn—or visit www.zeronorth.io