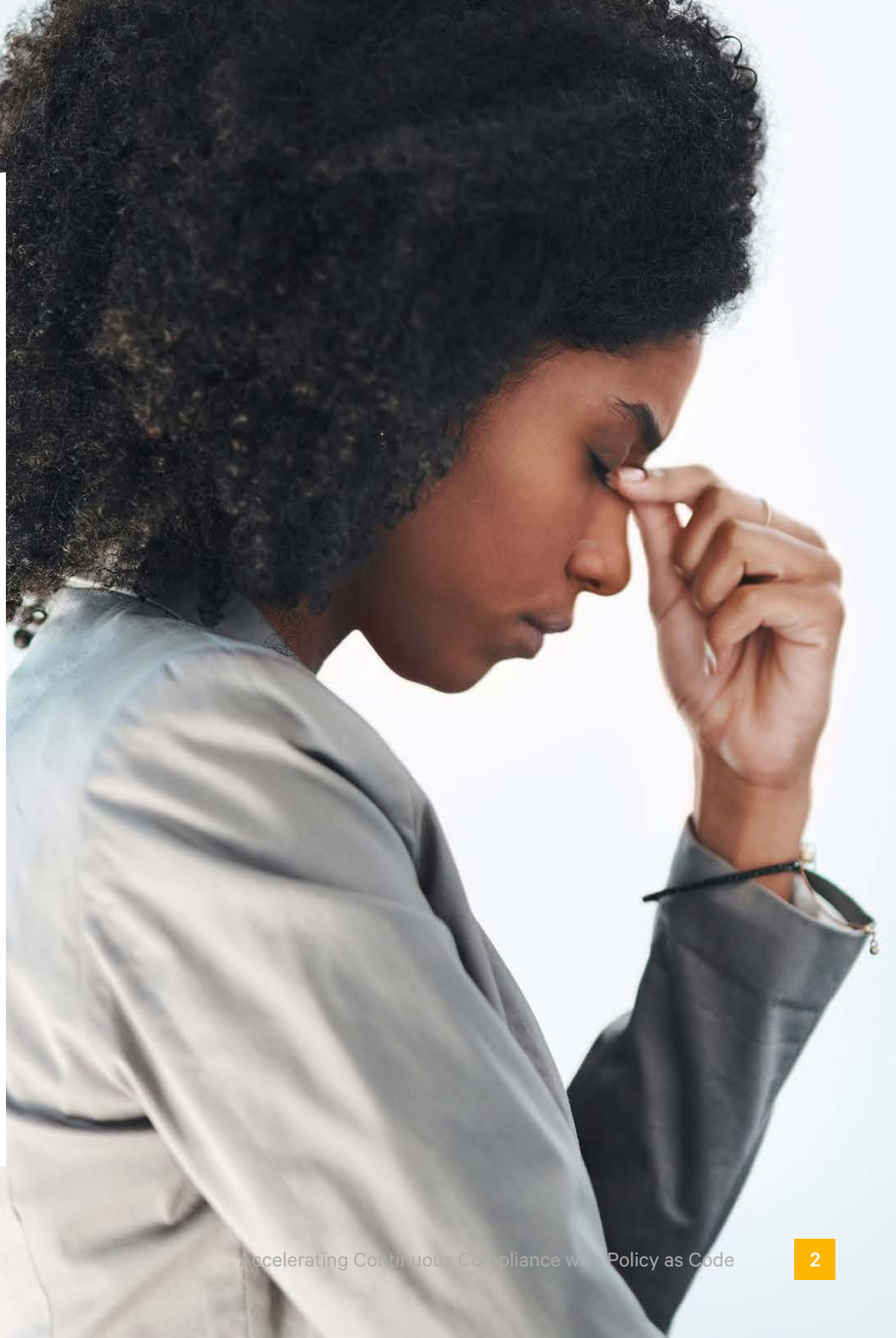
puppet

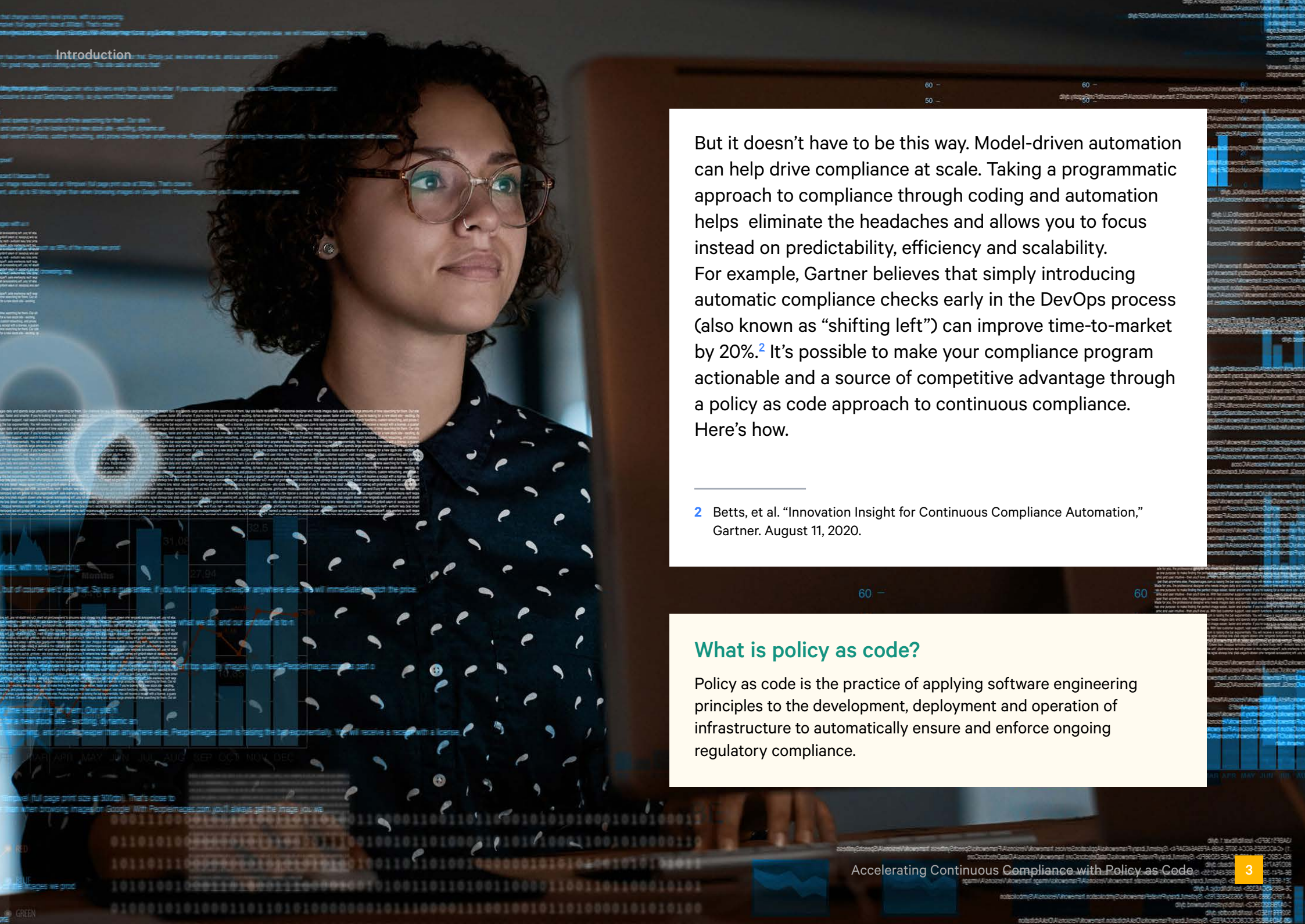
Accelerating Continuous Compliance with Policy as Code

Introduction

If you're like most organizations, your approach to regulatory compliance is largely reactive. You scan periodically against a framework (CIS, PCI/DSS, etc.), surface failures, fix the problems, scan again to make sure they're really fixed and then wait for something to go wrong. If you're lucky, you've already begun to integrate compliance checks in your DevSecOps toolchain to catch compliance and security issues early. But in both cases, these are typically manual processes, introducing significant inefficiency and points of friction into the system. A recent report by Telos Corporation published in Security Magazine says that a survey of 300 IT professionals found that respondents typically had to comply with up to 13 different regulations and spent an average of $3.5M annually on compliance activities.[1] It's a never ending battle.



1 "Compliance activities and fines cost organizations nearly $4m per year," *Security Magazine*. October 15, 2020



But it doesn't have to be this way. Model-driven automation can help drive compliance at scale. Taking a programmatic approach to compliance through coding and automation helps eliminate the headaches and allows you to focus instead on predictability, efficiency and scalability.
For example, Gartner believes that simply introducing automatic compliance checks early in the DevOps process (also known as "shifting left") can improve time-to-market by 20%.[2] It's possible to make your compliance program actionable and a source of competitive advantage through a policy as code approach to continuous compliance.
Here's how.

2 Betts, et al. "Innovation Insight for Continuous Compliance Automation," Gartner. August 11, 2020.

What is policy as code?

Policy as code is the practice of applying software engineering principles to the development, deployment and operation of infrastructure to automatically ensure and enforce ongoing regulatory compliance.

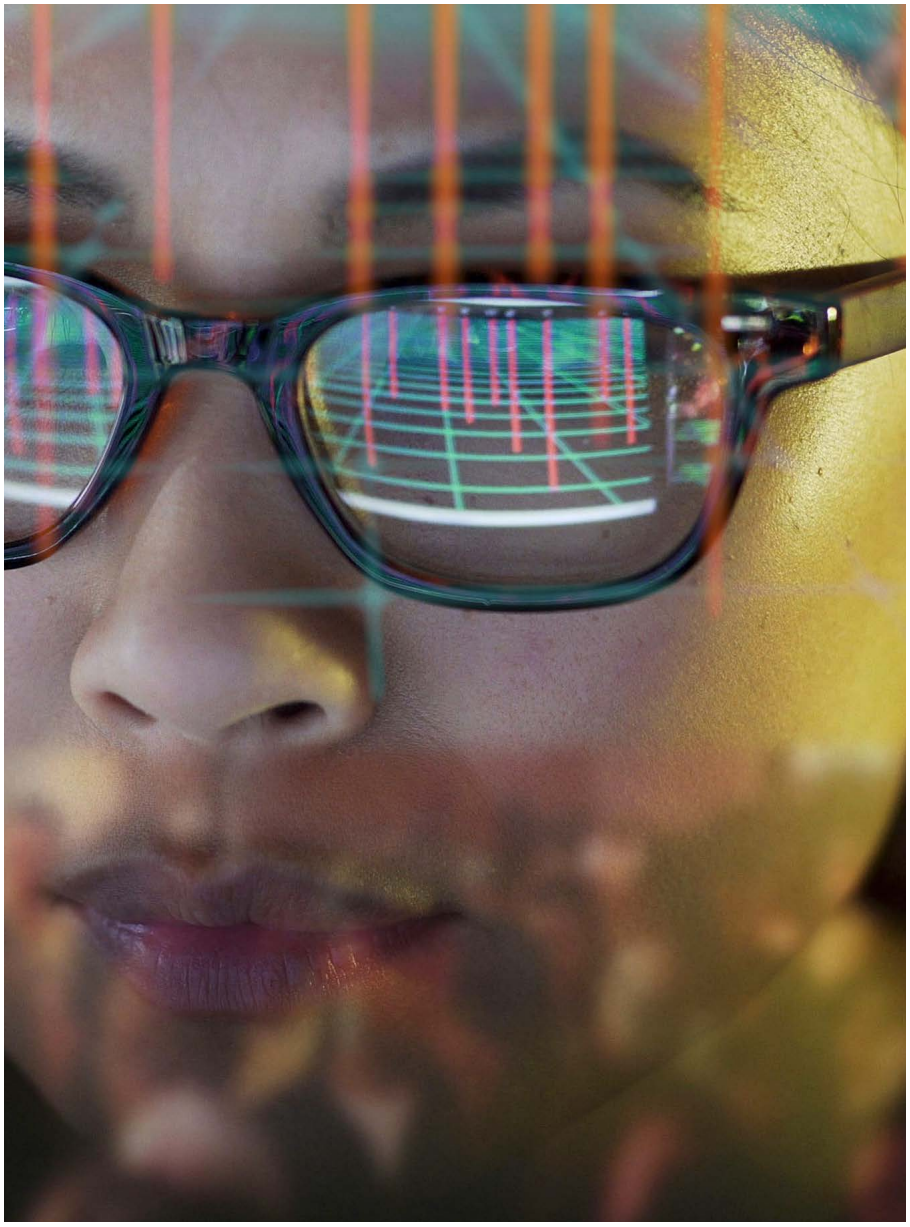
Predictability: Operate with confidence

The challenge

Large enterprise IT environments are extremely complex, with hundreds of applications and tens of thousands of nodes across multiple vendors and operating systems in multiple locations. There are lots of operating models as well, mostly hybrid (owned data centers, co-lo, MSPs, private cloud and public cloud). A lot can go wrong. These environments need to be continually updated, maintained and kept in compliance. These tasks typically fall to a combination of the Development, IT Operations and Security teams.

The rise of DevOps and Agile practices has enabled development teams to accelerate customer value by releasing a steady stream of new functionality and maintenance updates. Traditionally, compliance testing takes place near the end of the release cycle, long after a problem is baked into the infrastructure. This often makes the delivery process slow, unpredictable and costly. It creates drag and friction, resulting in a loss of business agility.

Another challenge involves the system settings for the infrastructure, such as maximum password age, ensuring that packet redirect sending is disabled, etc. These settings are the mechanisms that ensure alignment with various compliance frameworks. They are set when the systems are initially deployed and updated over time when a new version of a service becomes available. Most updates are made manually or by utilizing scripts, and in both cases the process is error prone.



In addition, people on the technical staff will sometimes make changes to infrastructure settings to address a problem, invalidating an otherwise compliant configuration. This produces what's referred to as configuration "drift." Drift will not only result in failed audits, but misconfigurations, which are responsible for a large percentage of system outages. That can cost money in terms of lost revenue from missed ecommerce transactions, brand damage, staff time to remediate, lost customers, etc. A server misconfiguration in March 2019 caused millions of Facebook customers to lose service for 14 hours and cost the company an estimated $70M in lost advertising revenue and an immediate 1.5% drop in share price.

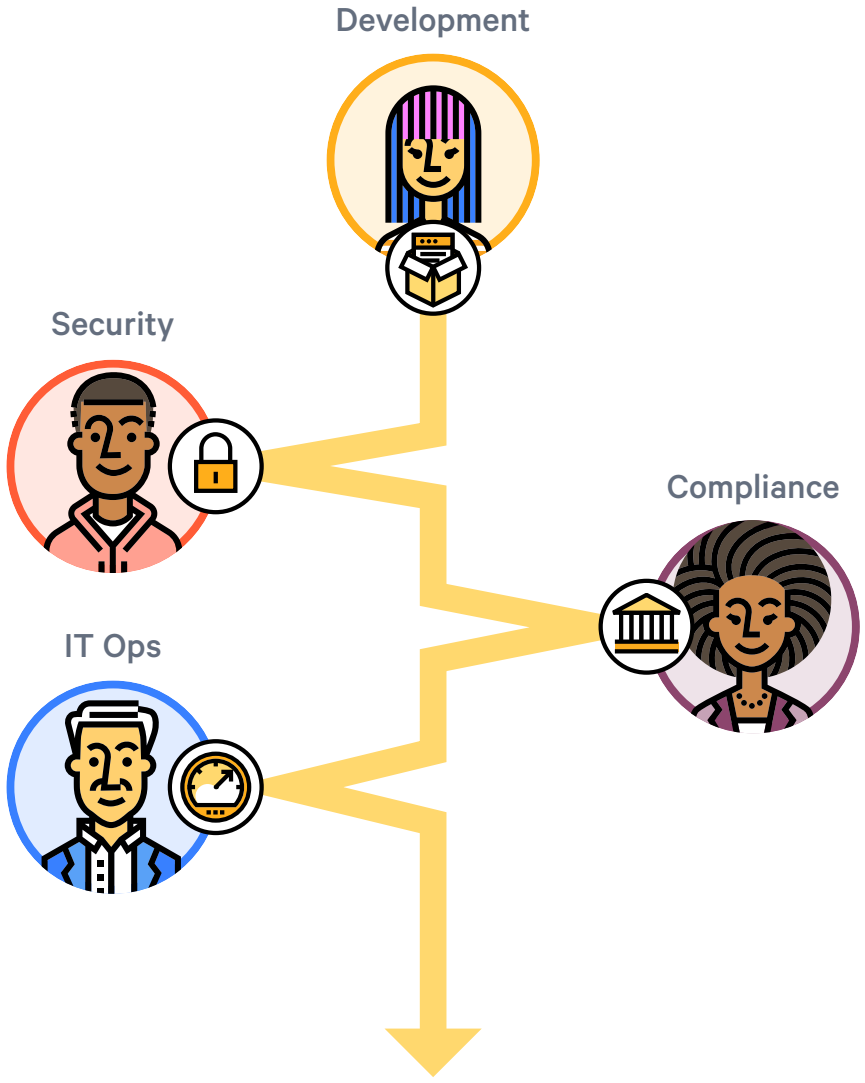
The typical way to identify compliance failures in any subset of the environment is to ask the Compliance or Security team to run a scan and then address the issues. In some companies, these scans happen frequently. Depending on what needs to be fixed, a scan could involve considerable time and effort. Management can't predict in advance what the scan will uncover, and how long it will take to remediate. And the scan itself takes a long time, since with traditional remote management and monitoring (RMM) tools you can normally scan only a few systems at once. This begs the question, how can you operate with confidence when your IT estate is one big morass of unpredictability? How do you face your next audit?

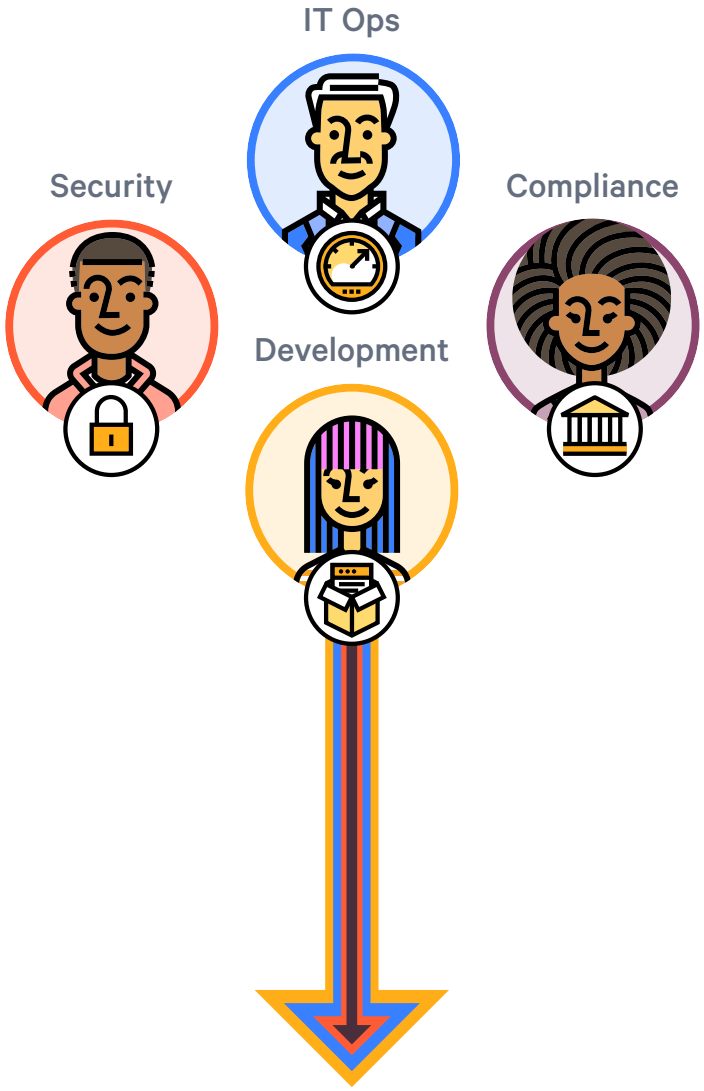
Why this is hard

Siloed organizations and resistance to change are the two largest factors. On the DevOps side, Development is laser focused on getting code into production. They often have no interest in working with Security or Compliance early enough in the development cycle to nip problems in the bud. Similarly, Security, Compliance and IT Ops are all focused on their own projects and don't have the spare cycles to get involved with Development.

On the configuration/IT Ops side, there's often ingrained but understandable resistance to automation. Practitioners know that mistakes can be made, and feel that sacrificing efficiency and scale to prevent a cascade of misconfigured software hitting 50,000 nodes at once is a prudent choice. (AWS and Facebook being cautionary tales.) Fair enough. That said, there are effective procedural and testing controls that can be put in place to minimize the risk (version control, canary testing, green/blue deployments, code reviews, etc.).

A third factor is lack of visibility into current compliance status. Running scans is typically resource-intensive, so it's not something you do lightly. And even if you could, the resulting reports are often complex and require time to interpret. The default behavior is to just assume that everything's OK and wait for the next scheduled audit.





Making this easy

No more silos. Policy-as-code-based tools like Puppet put everybody in control by removing bottlenecks. Together, teams can now run their own scans and control the complete development, validation and delivery of continuous compliance to automate the services they own. The introduction of compliance automation has forced the conversation between SecOps, IT Ops and Compliance, and the result is that compliance and security controls can now be baked into the development process earlier to catch compliance problems. And the assessment and remediation of compliance status is completely automated and predictable, improving confidence in an organization's compliance posture and making it easier to run more frequent, ad hoc scans. What's not to love? Compliance automation now offers the path of least resistance for the entire organization.

Efficiency:
Removing friction from the customer value stream

The challenge

As organizations advance in their digital transformation, they become increasingly aware that the IT infrastructure is the foundation for their digital enterprise. The IT infrastructure is the business. Networks need to be dynamic, agile and resilient. Yes, unplanned downtime can result in huge losses, but that's just the tip of the iceberg. Digital businesses are increasingly competing on the basis of service quality and customer experience, both of which are delivered through IT infrastructure. What that means is that the infrastructure needs to be totally locked down, efficient and bulletproof from a compliance perspective. It needs to be operating at peak efficiency. And the processes that support the infrastructure need to be grooved to support that efficiency. While this may seem just aspirational, think again. It's business critical.

Why this is hard

Gaining enough efficiency from your IT infrastructure to use it as a competitive advantage is a multidimensional problem, and all the pieces need to fit together. First, most medium and large IT estates are massively complex. There are multiple flavors of technologies, generations of equipment, vendors, operating systems, applications and security infrastructure. It's spread all over the world in multiple hosting environments.

Second, compliance is a moving target. There are multiple compliance frameworks, often with hundreds of rules each (companies typically need to comply with up to 13 frameworks) and the rules get updated regularly. These rules are implemented by configuration settings on individual systems.

Third, organizational processes are usually not aligned with the need for efficiency. One glaring example is the fact that the vast majority of configuration settings are updated manually, with RMM tools and scripting. It will come as no surprise that this is error prone, and again, we're talking about hundreds or thousands of nodes.

Similarly, the synergy between DevOps, Security, IT Ops and Compliance often does not support the efficiencies needed by the business to deliver the service quality and value demanded by customers. Compliance issues are discovered late in the development cycle, derailing product delivery. And the audit and remediation cycle is less than smooth, resulting in an undercurrent of friction between the groups.

Making this easy

Digital transformation is a process that touches every aspect of your business model from strategy, change management and human capital, through go-to-market and the IT infrastructure that supports it. While it's tempting to "boil the ocean" and do everything at once, it makes more sense to start with something that is concrete, under your control and that can have an immediate, measurable impact.

Automating your compliance program can act as a catalyst for digital transformation in your organization. And it can happen right now. Beginning with the modernization of your DevOps process by shifting left and embedding automated compliance testing early in the software development cycle to accelerate value delivery for customers, all the way through to automating compliance configuration controls for all of the nodes in your IT environment, Puppet is doing this today for hundreds of customers. As we said above, Gartner believes that integrating compliance controls into your DevOps toolchains (for starters) will improve your lead time by 20%. And Puppet's ability to lock down and automatically enforce compliant configurations across all nodes in the IT environment eliminates inefficiencies in existing processes, freeing up hundreds of hours for driving customer value.

Scalability:
Digitize your approach to compliance enforcement

The challenge

Managing the initial and ongoing configuration of a large IT estate is a huge challenge. There are multiple platforms running various flavors of operating systems, all configured with different sets of system commands. Many need software updates, periodic scans and configuration updates.

DevOps produces a steady flow of new functionality and updates, and prior to releasing to production, compliance tests are conducted manually. As we mentioned above, the software updates, scans and configuration changes are handled by RMM, scripting and/or very strict change control. The problem is that these are all really mitigation strategies vs. compliance solutions and none can scale in even medium-sized IT environments. For RMM and scripting approaches, you need to deploy to every server and execute on every server manually. This is a huge drag on IT's ability to help deliver digital transformation.

Why this is hard

Well, you might as well ask why an enterprise would choose to do things the hard way when they could do things the easy way. Sure, there's a point in time before your infrastructure and the regulatory environment become hopelessly complex when it probably makes sense to manage things manually. But after that, automation is the only reasonable path. So why isn't everyone on board? It really comes down to a combination of organizational inertia, fear and resources. DevOps, Security and Compliance teams typically have a testing model that they've been using for a number of years, and the staff are used to doing things a certain way.

Similarly, many IT Ops staff have been doing configuration management manually for most of their careers and they feel that automating the process could result in a loss of control and unintended side effects. You're asking people to adopt a change in their operating model where they need do some simple coding vs. running a command. For a lot of people this is a big leap.

And finally, all organizations in the midst of a digital transformation have a lot on their plates. It's easy to rationalize delaying an upgrade to a process that is familiar and seems to work, albeit imperfectly.

Making this easy

Model-driven automation can drive compliance at scale. Taking a policy as code approach, compliance and security checks can be embedded into DevOps environments to catch compliance-related coding errors early in the software development lifecycle, prior to deployment. These checks can be executed automatically at various stages in the development process.

For deployed infrastructure, declarative, policy-as-code-based tools like Puppet can help you achieve the control and uniformity you need. They allow you to define a compliant configuration for any regulatory framework at a high level and then apply and automatically enforce that configuration on different devices across the estate every 30 minutes (configurable). The configuration is established in a centralized manifest along with the classification settings for each category of infrastructure. This makes it easy to determine whether the same configuration rule needs to be specified differently on different infrastructure.

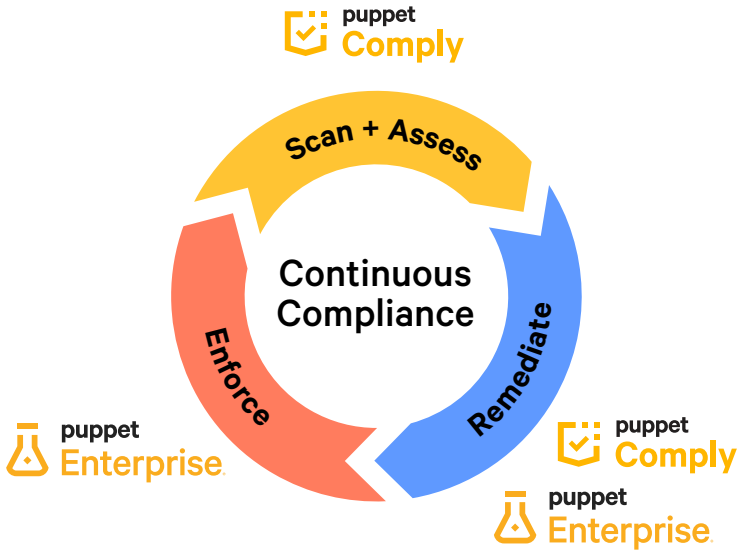
No need to log into each server or understand the OS-specific commands and steps needed for configuration. Teams can now run their own scans and control the complete development, validation and delivery of policy as code to automate the services they own.

Moving forward with a foundation for the digital enterprise.

Digital transformation is not something that happens overnight. It's a multifaceted journey and touches every facet of the enterprise.

That said, there are workstreams like automating compliance controls that don't involve major dependencies with other aspects of the transformation, but are powerful enablers of the program's overall success.

Automating your compliance program is eminently doable and the technology is proven. Taking a programmatic approach to compliance through continuous compliance and automation eliminates the headaches and instead allows you to focus on **predictability, efficiency and scalability.** The impact will be immediate and measurable. And most importantly, it will give you a highly leveraged starting point and a solid foundation to support your digital transformation.



puppet

Puppet is driving the movement to a world of unconstrained software change. Its revolutionary platform is the industry standard for automating the delivery and operation of the software that powers everything around us. More than 40,000 companies — including more than 75 percent of the Fortune 100 — use Puppet's open source and commercial solutions to adopt DevOps practices, achieve situational awareness and drive software change with confidence. Headquartered in Portland, Oregon, Puppet is a privately held company with more than 500 employees around the world. Learn more at puppet.com