DevSecOps for GCP and Platform Engineering

Whitepaper

Learn the fundamentals of Platform Engineering and about the GCP DevSecOps accelerator UST PACE

ust.com

Table of contents

Despite many companies embracing the speed and agility of GCP for their software design, they still face challenges in delivering secure digital solutions due to their sub-optimal approach to security. Traditional security practices are still prevalent even f or companies in the Cloud, treating security as a separate activity executed late within the software development life cycle (SDLC). This reactive approach to remediating security issues not only slows down delivery but also increases costs. Cyber attacks primarily target the application layer, accounting for 84% of incidents, highlighting the need for a more proactive security approach.

The lack of early detection of security issues underlies much of this problem. The engineering process often neglects secure development practices and industry best practices, such as Zero Trust. As a result, security flaws go undetected until production, leading to significant costs. A staggering 76% of applications have some form of security flaws, which cost 100 times more to fix when discovered in production.

Addressing these challenges requires a shift towards a more proactive and integrated approach to security. In this whitepaper, we explore how companies can enhance their ability to deliver secure digital solutions efficiently and cost-effectively.

DevOps, DevSecOps - What's next?

DevOps and DevSecOps are two essential concepts in software development and operations, especially for environments such as GCP, which accelerates the speed at which software is produced. With this increase in speed comes the risk of introducing security issues endangering sensitive data and operations.

In response, DevOps helps build security into the process, focusing on improving code quality and operational efficiency by breaking down barriers between development, operations, and security teams. By fostering a collaborative and cross-functional mindset, organizations can overcome resistance to change and promote shared responsibility.

DevSecOps, on the other hand, takes this a step further by incorporating security considerations early in the software development process. This shift to the left ensures that security measures are integrated seamlessly into the development lifecycle. However, this integration can be challenging, as it requires the seamless integration of tools, testing, and compliance measures without impeding development cycles.

Implementing DevOps and DevSecOps is easier stated than done. It takes a combination of learning new skills, automating processes, and implementing the right tools into the automation to streamline development processes while maintaining the optics to prevent security or compliance issues before they make their way into production.

DevOps Maturity

While adopting and implementing DevOps practices, organizations go through different stages of growth as they mature into fully operationalizing the necessary components. There are five phases of DevOps maturity that organizations can progress through. Depending on the source, these phases exist under different names, but the main concepts remain consistent no matter the name. The higher the maturity level, the better the outcomes regarding code robustness, code quality, development speed, and adherence to agile enterprise standards.

The first phase of DevOps maturity is the “Explore” phase, where organizations are in the early stages of DevOps adoption. They are exploring and experimenting with DevOps principles and practices. This is followed by the “Engage” phase, where organizations start to see the benefits of DevOps and actively involve development and operations teams in collaborative efforts. Communication and collaboration improve while the organization implements initial automation efforts.

The “Optimize” phase is where organizations focus on refining their DevOps practices and optimizing their workflows. They identify and eliminate bottlenecks, automate repetitive tasks, and prioritize continuous improvement.

Moving on to the “Scale” phase, organizations begin to scale their DevOps practices across teams and departments. They establish standardized processes and tools, enabling consistency and efficiency throughout the organization.

Finally, in the “Transform” phase, organizations fully embrace DevOps as a cultural and organizational shift. DevOps principles are deeply ingrained in their DNA, and continuous improvement and innovation are the norms. They leverage advanced automation, DevOps analytics, and other advanced practices to achieve exceptional outcomes.

Assessing their current position in these maturity phases is crucial for organizations. It can be done through self-assessments, benchmarking against industry standards, or consulting with DevOps experts. Understanding their DevOps maturity level allows organizations to identify areas for improvement and set realistic goals for advancing their DevOps journey. Achieving higher maturity levels in DevOps ultimately leads to increased code robustness, improved code quality, faster development processes, and adherence to agile enterprise standards.

Challenges of Scale

As organizations scale their operations in GCP and manage complex software systems, they face various challenges in maintaining consistency and efficiency in their DevOps and DevSecOps practices. Coordinating multiple teams, managing numerous environments, and handling distributed systems require careful planning and automation to avoid bottlenecks and ensure smooth operations.

One major challenge that arises with scale is threat monitoring and incident response. As the organization grows, the attack surface expands, increasing the need for effective monitoring and timely response to security incidents. While some resources, such as Cloud Storage, only have limited exposure through the GCP API. Other technologies, such as Compute Engine, increase the attack surface as native tools running on the customer-chosen OS, such as SSH or RDP, create additional exposure.

Managing the scaling in GCP requires a combination of optics, analysis, and response which become more complicated as the environment scales. Monitoring must extend across a larger space, security information and event management (SIEM) solutions must process more data, and incident response plans become more complex as coordinating responses involves multiple teams and projects. Implementing all of these is crucial to respond to security incidents promptly and effectively.

Additionally, scaling introduces complexities in terms of infrastructure and resource management. Ensuring the necessary resources are available to support the growing operations becomes essential. This involves managing and optimizing GCP infrastructure, maintaining high availability, and ensuring scalability to handle increased workloads.

Furthermore, maintaining consistency across different environments and platforms poses a challenge. It requires establishing standardized processes and tools, implementing configuration management practices, and ensuring seamless deployments across various environments.

Organizations must invest in automation, monitoring, and incident response capabilities to address these challenges and are designed to operate in GCP, not just on-premises. They should adopt robust security practices, leverage threat intelligence, and implement proactive measures to detect and mitigate vulnerabilities and threats. Coordinating across teams and projects becomes critical, with clear communication channels and well-defined incident response procedures.

The Developer = Your Customer

Recognizing developers as business customers is a break from the traditional approach of leveraging developers as human assets. This shift acknowledges their importance, rather than making them a line on a spreadsheet, and aims to cater to their needs, provide value, and foster a positive experience. Companies adopt this approach as they understand developers play a vital role in the success of a business by building and maintaining the software systems that drive its operations. By prioritizing their satisfaction and productivity, they can empower developers to work efficiently, deliver high-quality software, and contribute to the organization's overall success.

Developers are instrumental in driving business agility and innovation as they are responsible for developing new features, implementing improvements, and addressing various customer needs through software solutions, making it crucial to provide developers with the right tools, resources, and support that enable them to perform their tasks effectively.

Improving how organizations treat developers is also crucial for retention and recruitment. Skilled developers have ample opportunities to choose from, and businesses need to foster a positive relationship with them to increase their satisfaction and engagement with the organization. Satisfied developers are likelier to stay with the company, reducing turnover and maintaining a stable and productive workforce.

In order to treat developers as customers, businesses should listen to their feedback, involve them in decision-making processes, and provide growth and professional development opportunities. Offering a supportive and collaborative work environment, recognizing their contributions, and acknowledging their expertise can go a long way in building a solid relationship with developers.

Enter Platform Engineering

Platform Engineering is one of the ways to improve the developer experience as it aims to enhance developer productivity by reducing the complexity and uncertainty associated with modern software delivery. It focuses on streamlining the development process by reducing operational complexity and removing friction. The goal is to align development practices with business priorities, allowing developers to focus on delivering value without getting bogged down by managing a complex web of tools and infrastructure across the application lifecycle.

Platform Engineering plays a crucial role in improving developer productivity. Providing standardized platforms and tooling enables developers to work more efficiently and effectively. This includes automating repetitive tasks, simplifying deployment processes, and facilitating collaboration among development teams.

One of the key benefits of Platform Engineering is its ability to reduce operational complexity. Establishing standardized practices and infrastructure eliminates the need for individual teams to manage their own tools and environments. This reduces the burden on developers, enhances consistency, and reduces the risk of errors.

Moreover, Platform Engineering aligns development practices with business priorities. Creating a unified platform supports the organization's strategic objectives, enables faster time-to-market, improves scalability, and enhances overall business agility. It also allows for better resource allocation, as infrastructure and tooling can be shared and utilized more efficiently across multiple projects.

Developer Self-Service

Companies can also empower developers by implementing developer self-service, which provides them with the necessary tools, resources, and access to take ownership of their security responsibilities and integrate security practices into their development workflows. It enables developers to run automated security checks on their code or applications, such as static code analysis, dynamic application security testing (DAST), and software composition analysis (SCA).

In the context of DevSecOps, developer self-service aligns with infrastructure-as-code (IaC) practices central to GCP development. Developers can define and provision secure infrastructure resources using code, and self-service platforms can offer templates, scripts, and libraries to facilitate this process. This ensures that security measures, such as network configurations, access controls, and encryption, are consistently applied across the GCP environment and different deployments.

One of the core benefits of developer self-service is reducing dependency on security teams for routine security tasks. By empowering developers to perform security checks, access resources, and follow secure coding practices independently, organizations can streamline processes and eliminate bottlenecks caused by security reviews and approvals. This enables faster development cycles while maintaining the required security standards.

By integrating security practices into the developer's workflow and providing self-service capabilities, organizations foster a culture of security ownership and responsibility among developers. It encourages them to address security concerns proactively and ensures that security considerations are not an afterthought but an integral part of the development process. This ultimately leads to improved application security, reduced vulnerabilities, and increased efficiency in software development.

Shifting Security Left

Shifting security left is an approach within the SDLC that emphasizes integrating security practices and considerations early in the development process. In traditional approaches, security concerns were often addressed late in the development cycle or even after software application deployment. However, with the rise of DevOps and Agile methodologies, there has been a shift in mindset to prioritize security from the beginning stages of development.

Organizations insert security directly into the CI/CD pipeline by shifting security left, benefitting from early vulnerability identification. By incorporating security practices and tools into the early stages of development, potential vulnerabilities can be detected and addressed at an earlier point, reducing the chances of security breaches or issues in the final product. This allows for more efficient issue resolution, as security concerns can be addressed in parallel with the development process rather than as an afterthought.

Furthermore, shifting security left helps reduce security risks associated with software applications. Organizations can mitigate potential risks and vulnerabilities early by proactively integrating security measures, such as secure coding practices, threat modeling, and security testing. This proactive approach helps build more robust and secure software applications, protecting against potential threats and attacks.

Collaboration and shared responsibility are also important aspects of shifting security left. By involving security teams, developers, and other stakeholders from the beginning, organizations can foster a culture of shared responsibility for security. This collaboration enables better communication, knowledge sharing, and alignment of security practices across the development team. Developers become more aware of security considerations, and security teams gain insights into the application's development process, resulting in improved security outcomes.

Reusability = Time Savings + Best Practices Built-In

Reusability brings significant time savings and allows developers to build upon established best practices. Developers can streamline their development process by designing and implementing reusable components, modules, or code snippets and avoid reinventing the wheel for each project. Instead, they can leverage existing, tested, and reliable code that has undergone multiple iterations and received feedback.

Reusable components are typically built following established best practices and design patterns. These components incorporate the knowledge gained from previous projects, ensuring higher quality, improved reliability, and consistent adherence to industry standards. They promote consistency and standardization across projects, ensuring that similar functionalities or features are implemented consistently. This reduces the chances of introducing errors, simplifies maintenance and troubleshooting, and enhances the overall quality and reliability of the software.

Moreover, reusability enables rapid prototyping and iteration. Developers can quickly assemble and test different combinations of reusable components to create prototypes or proof-of-concept solutions. This encourages faster experimentation and gathering of feedback. Developers can iterate and refine their solutions more efficiently, quickly incorporating user feedback and adapting to changing requirements

SDLC Governance

Part of shifting left is gaining control over the processes, policies, and controls an organization establishes to guide and oversee software development activities, known as SDLC Governance. The governance process persists throughout the entire SDLC. Its primary objective is to promote consistency, quality, and compliance in software development practices. By defining and enforcing policies and standards, SDLC governance ensures that software development projects align with organizational goals, standards, and regulatory requirements.

One of the critical aspects of SDLC governance is the establishment of policies and standards related to software development. This includes coding standards, documentation practices, security measures, testing procedures, change management processes, and compliance with relevant regulations. SDLC governance ensures that development projects follow established processes and methodologies by providing a foundation for consistent and compliant software development practices. It creates a consistent approach to software development, such as Agile, Waterfall, or hybrid model, and ensures that projects align with the chosen methodology.

SDLC governance also involves identifying, assessing, and mitigating risks associated with software development projects. This includes security vulnerabilities, data privacy concerns, regulatory compliance, and project delivery risks. By integrating risk management practices into the development process, organizations can implement appropriate controls to address identified risks.

Furthermore, SDLC governance emphasizes the importance of quality assurance and testing throughout the SDLC. It defines testing standards, methodologies, and tools to ensure thorough software testing for functionality, performance, security, and reliability. It also enhances software quality by adding processes for tracking defects, resolution, and regression testing.

Change control and release management processes are also part of SDLC governance. These processes effectively manage changes to software applications by ensuring that changes are properly documented, reviewed, and approved before implementation. Additionally, SDLC governance includes controls for managing configuration baselines, version control, and deployment processes. This ensures that changes are made in a controlled and coordinated manner to minimize disruption and maintain stability.

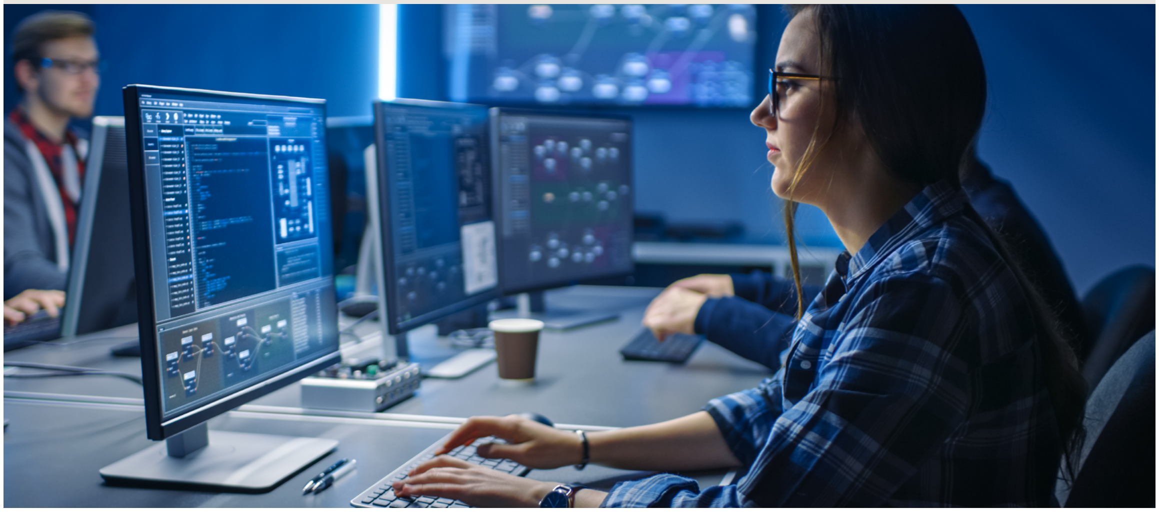
App Health + Portfolio Visibility

App Health and Portfolio Visibility are two interconnected concepts that enable organizations to monitor and assess the status and performance of their applications while gaining insights into their overall portfolio. App Health evaluates individual applications' current state and well-being within an organization's software ecosystem. This assessment includes monitoring various metrics, indicators, and performance factors to determine each application's overall health, stability, and reliability.

On the other hand, Portfolio Visibility focuses on gaining a comprehensive view and understanding of an organization's entire portfolio of applications. It involves aggregating and analyzing data from individual applications to provide insights into the overall performance, strategic alignment, and resource allocation within the application portfolio. By obtaining portfolio visibility, organizations can assess their applications' value, impact, and risks and make informed decisions regarding resource allocation, investments, and prioritization.

These two concepts are interconnected, as individual applications' health contributes to the application portfolio's overall health and performance. By monitoring app health and gaining portfolio visibility, organizations can proactively identify and address issues, prioritize resources effectively, and make data-driven decisions to optimize the performance and value of their application ecosystem. Ultimately, App Health and Portfolio Visibility empower organizations to manage their applications more effectively, align their strategies, and drive successful outcomes.

How UST PACE Enables Developers



PACE (Platform for Accelerated Cloud-native Engineering), offered by UST, is a world-class development platform designed to orchestrate the DevSecOps tool stack and empower organizations to shift security and quality left in their software development processes. By transforming processes into code and providing clarity across the entire development environment, PACE enables enterprise engineering teams to build high-quality software faster. The UST PACE platform seamlessly integrates with your existing tools and can be deployed on your GCP infrastructure. UST's expert DevSecOps team configures the platform to ensure you start experiencing its value from day one.

With UST PACE, organizations can achieve true Continuous Integration/ Continuous Deployment (CI/CD) automation, improve their security posture, enhance code robustness and quality, and accelerate development. The platform enforces agile enterprise standards, allowing teams to adhere to best practices and achieve greater efficiency. By leveraging PACE, organizations can streamline their SDLC, reduce manual efforts, and leverage automation for improved productivity.

UST PACE enables developers to focus on building high-quality software by providing a comprehensive platform that integrates seamlessly with their existing toolchain. With its on-premises promise, UST PACE ensures that organizations have complete control over their development environment and can leverage the platform's benefits while maintaining their preferred infrastructure.

DataMorph

PACE's DataMorph offering is a lightweight low-code Extract Transform and Load (ETL) framework that empowers developers to consolidate disparate data while seamlessly moving it from one place to another. This framework simplifies consolidating data from multiple sources stored in different formats or locations. Developers can configure DataMorph to extract data from various systems or databases, apply specific business rules to transform it, and then load it into a desired target destination.

Data consolidation facilitated by DataMorph creates a unified view of the data, making it easier to analyze, utilize for reporting, make informed decisions, or integrate into other systems. Additionally, DataMorph enables efficient data migration or synchronization between databases, data warehouses, cloud platforms, or other storage systems. Developers can define the required data transformation operations and specify the destination for the data, providing flexibility and agility to support various integration scenarios.

One of the advantages of DataMorph is its lightweight nature, making it suitable for a wide range of projects and environments. It easily integrates into existing systems and infrastructure without causing significant performance or resource overhead. Moreover, DataMorph efficiently handles large volumes of data, ensuring smooth data processing and maintaining performance even as the data size grows.

With DataMorph, developers gain a powerful tool to consolidate data from diverse sources, transform it according to business rules, and seamlessly move it to target destinations. This enables organizations to create a unified and reliable data foundation, supporting effective analysis, reporting, decision-making, and integration processes.

UST PACE: On-Prem Promise

n today's hybrid IT landscape, organizations often operate with a combination of on-premises infrastructure and cloud environments like GCP. To effectively manage this hybrid infrastructure, having the right tools to provide unified visibility and detection capabilities is crucial. UST recognizes this need and offers a solution through its on-premises promise through the PACE platform.

UST's PACE platform aims to centralize visibility and monitoring by unifying events from both on-premises and cloud environments. With the ability to integrate multiple Security Information and Event Management (SIEM) systems, the platform enables organizations to monitor alerts and incidents from both on-premises and cloud infrastructures in a single, consolidated view. This multi-SIEM capability streamlines the monitoring process, allowing security teams to efficiently detect and respond to security events across their entire IT landscape.

By providing centralized visibility of both on-premises and cloud monitoring, UST's PACE platform ensures that organizations comprehensively understand their security posture, regardless of their infrastructure. This unified approach to monitoring allows organizations to manage security incidents effectively, identify potential threats, and take proactive measures to safeguard their systems and data.

Working Across AWS

Every organization adopts the cloud technology that is right for them. UST PACE recognizes the diverse needs of organizations and provides the flexibility to work seamlessly with GCP, empowering developers to orchestrate and shift left in their GCP-based development processes.

PACE drives digital agility transformation at scale by design, synergizing with GCP. It allows developers working on GCP to leverage the power of PACE and benefit from its orchestrated automation capabilities to rapidly scale in GCP.

With UST PACE, developers can quickly create new development projects on GCP using an intuitive user interface and a library of reusable components. The platform is architected to promote sharing best practices and adherence to enterprise standards. This ensures consistency and efficiency in the development process while aligning with the organization's standards and requirements.

UST PACE empowers developers working on GCP by providing them with an agile environment to move at the speed of business. By leveraging enterprise standard templates, frameworks, pipelines, and secured runtime environments, developers can accelerate product engineering and adopt best practices across DevOps, software development, and security teams. The fully enabled development and delivery workspace offered by UST PACE fosters collaboration among developers while maintaining the security and integrity of sensitive data.

UST PACE: Orchestrate Your Enterprise

The UST PACE solution empowers organizations to seamlessly coordinate and automate various processes and tasks throughout the software development and delivery lifecycle. By automating complex and repetitive tasks associated with DevSecOps, Impact streamlines workflows, reduces manual errors, and enhances overall efficiency.

With UST PACE, organizations can orchestrate and sequence activities such as code builds, testing, security scans, deployment, and monitoring. This automation not only saves time and effort but also ensures consistent execution of tasks. Security policies and compliance requirements can be implemented and enforced throughout the software development process, integrating security checks like static code analysis, dynamic application security testing (DAST), and software composition analysis (SCA) into the deployment pipeline.

UST PACE provides visibility into the entire DevSecOps process, capturing and consolidating data from various tools and processes, enabling real-time monitoring, tracking, and auditing of activities and events. This enhanced visibility into the software development and delivery lifecycle helps organizations monitor their security posture, facilitate compliance audits, and identify areas for improvement.

UST PACE also ensures scalability by coordinating the deployment and management of software components across different environments and infrastructures. It enables organizations to effectively manage scaling requirements, load balancing, and failover scenarios. Additionally, UST PACE seamlessly integrates security controls and monitoring mechanisms, ensuring the resilience and availability of the software in production.

Route To Live With UST PACE

UST offers cloud platforms and platform-led design services to accelerate your digital transformation and drive innovation. By leveraging our expertise, you can enhance your speed to market and unlock new opportunities. UST provides the necessary framework and tools to streamline continuous releases and continuous delivery, paving the way for faster development. We emphasize using reusable architectures based on microservices, reducing complexity and increasing scalability.

With UST, you receive comprehensive support throughout the entire software development lifecycle, from design to deployment. Our teams work alongside yours, employing DevOps, DevSecOps, or SRE best practices to make your organization lean and agile. Trusted by top enterprise organizations, UST PACE is pivotal in orchestrating DevOps tool stacks, prioritizing security and quality from the start, and driving improved development practices. By putting process to code and adding clarity, UST PACE empowers engineering teams to build high-quality software at an accelerated pace.

UST PACE seamlessly integrates with your existing tools and GCP infrastructure, expertly configured by their DevSecOps team, to ensure immediate value. By implementing our solution, you can achieve true CI/CD automation, improve security posture, enhance code robustness and quality, and enforce agile enterprise standards. Experience the benefits of accelerated development while maintaining a strong focus on security and quality with UST PACE

Together, we build for boundless impact

About UST

For more than 23 years, UST has worked side by side with the world's best companies to make a real impact through transformation. Powered by technology, inspired by people and led by our purpose, we partner with our clients from design to operation. Through our nimble approach, we identify their core challenges and craft disruptive solutions that bring their vision to life. With deep domain expertise and a future-proof philosophy, we embed innovation and agility into our client's organizations—delivering measurable value and lasting change across industries, and around the world. Together, with over 30,000 + employees in 30 countries, we build for boundless impact—touching billions of lives in the process.

ust.com

U·
ST