aws | TREND MICRO

EBOOK

Automated Security at the Speed of DevOps

Table of contents

Introduction

Software development has evolved from rigid waterfall methodologies to more flexible and streamlined approaches like Agile, and more recently, DevOps. This evolution has taken place, in large part, to shorten development life cycles and meet increased business demands. Today, businesses of all sizes have built an advantage by implementing a DevOps culture and processes, which break down silos between development and operations, allowing organizations to build applications faster.

As organizations implement DevOps on Amazon Web Services (AWS), they need to understand the security implications. The AWS Shared Responsibility Model makes clear that AWS secures what's "on the cloud," while the customer is responsible for securing their assets "in the cloud." When AWS customers go about securing their DevOps environments, they need to do so in a way that provides robust protection without limiting developer agility.

This e-book will highlight the main challenges businesses face at the intersection of DevOps and security and offer best practices for integrating security within your development processes from the start.

Traditional software development vs. DevOps

Evolving from Waterfall to Agile

Software development practices have evolved over the years to more streamlined processes for creating higher quality applications at greater speed. Many organizations have moved away from traditional waterfall models, where each phase of development is dependent on the other. In Waterfall models, testing came towards the end of development. This meant that issues often weren't found until the later stages of a project. Teams would have to backtrack to fix issues and push back release dates. Historically, the steps taken to minimize these unanticipated modifications involved long planning cycles that stifled agility and incurred excessive costs.

In the early 2000s, companies began moving away from this inefficient development model and embraced new Agile methodologies. Based on the Agile Manifesto, these development practices encouraged testing throughout a project (rather than at the end) and greater collaboration amongst different teams. This resulted in smaller, yet faster development cycles.

The rise of DevOps

In more recent years, Agile development has evolved into DevOps. The primary reason for this shift was that Agile development uncovered a new roadblock that stymied agility; the separation of development and operations teams.

DevOps removes this roadblock by bringing together stakeholders from both units to collaborate throughout the development cycle. DevOps cultures leverage a continuous integration and deployment (CI/CD) pipeline, which enables greater automation throughout a project. When combined with greater collaboration, this automation has resulted in accelerated builds and deployments. By enabling rapid iteration and the delivery of smaller packets of code, DevOps makes it easier to obtain and apply end-user feedback to create higher quality software.

Why AWS for DevOps?

AWS has made it easier for organizations to implement modern development practices like DevOps because it provides a broad and deep set of native cloud services. Access to these services removes the barriers—time, cost, and risk—that have traditionally made it hard to implement new technologies on-premises. Furthermore, AWS constantly updates its service offerings, making it easier for organizations to keep up with and take advantage of the latest technological advancements.

AWS Developer Tools is a subset of the AWS service library, which help you host code and automate the build, testing, and deployment of your applications. To build a CI/CD workflow, developers can take advantage of the following services:

Software release workflows

AWS Code Pipeline

Build and test code

AWS CodeBuild

Deployment automation

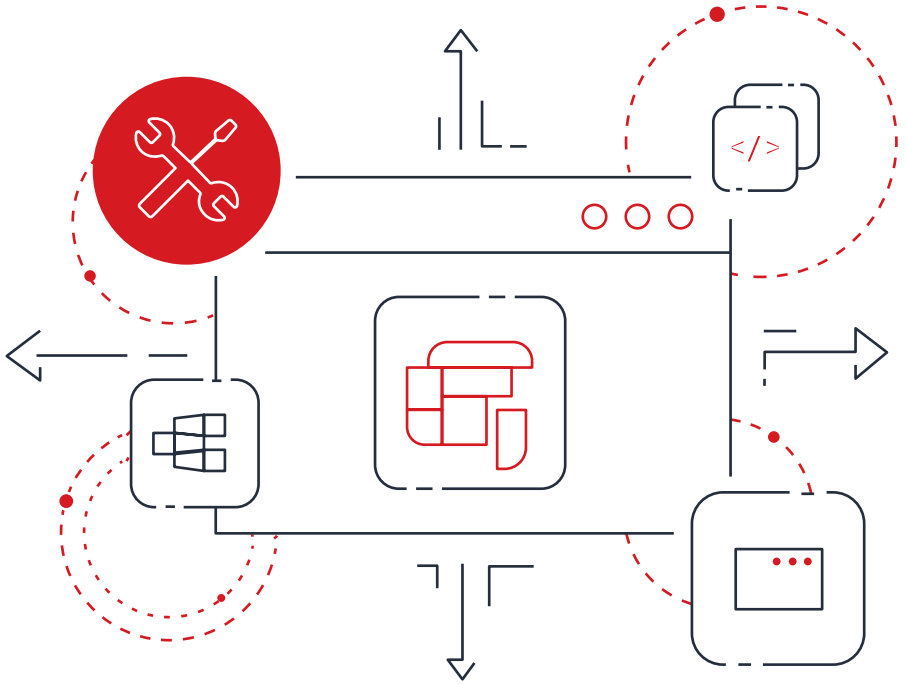
AWS CodeDeploy

Unified CI/CD projects

AWS CodeStar

Leveraging containers in your CI/CD pipeline: The core of DevOps collaboration

Development practices continue to evolve, folding in the latest technology advancements to move faster, deliver new customer value, and build a stronger competitive edge. Recently, this has led to the inclusion of containers—a standard unit of software that packages up code and all its dependencies.

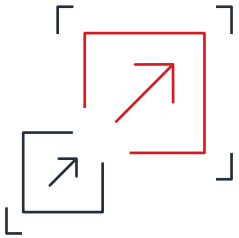


The advantage of using containers is that they consolidate an application's code, configurations, and dependencies into a single object, making them modular and easy to spin up/spin down. They also run off of an operating system (OS) kernel, as opposed to their own OS. These factors make them more resource efficient than traditional VMs, while also enabling greater development speed.

The evolution from Waterfall to Agile to DevOps development practices has been a game changer for businesses, enabling them to create better applications at greater speed and a lower cost. Now that software is at the core of most businesses, it's critical for organizations to infuse the highest level of agility and nimbleness into their development practices. Delivering value to the market more quickly than the competition can be a key driver of business success. By adopting modern DevOps practices, including the use of containers, businesses can reduce the time to market for applications and updates, accelerate the customer feedback loops, and reduce the risk of introducing new capabilities.

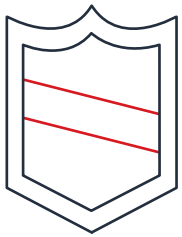
The challenge in securing DevOps environments

Even though DevOps comes with many advantages, that does not mean it comes without challenges. Many organizations are still challenged by securing their new DevOps environments. In particular, businesses face two common challenges.



Growing pains when changing culture

DevOps requires development teams to think of security from the beginning of a project and throughout its life cycle—a stark contrast from previous operations. Many see this level of security as a bottleneck and work around it to stimulate speed.



Manual security measures slow development

Many common DevOps tools lack the necessary security capabilities, including automated monitoring and analysis. Without this, it is hard to deliver robust security without slowing development or incurring human error. Security automation is especially important when using containers, as their agile and modular nature make them hard to keep up with manually.

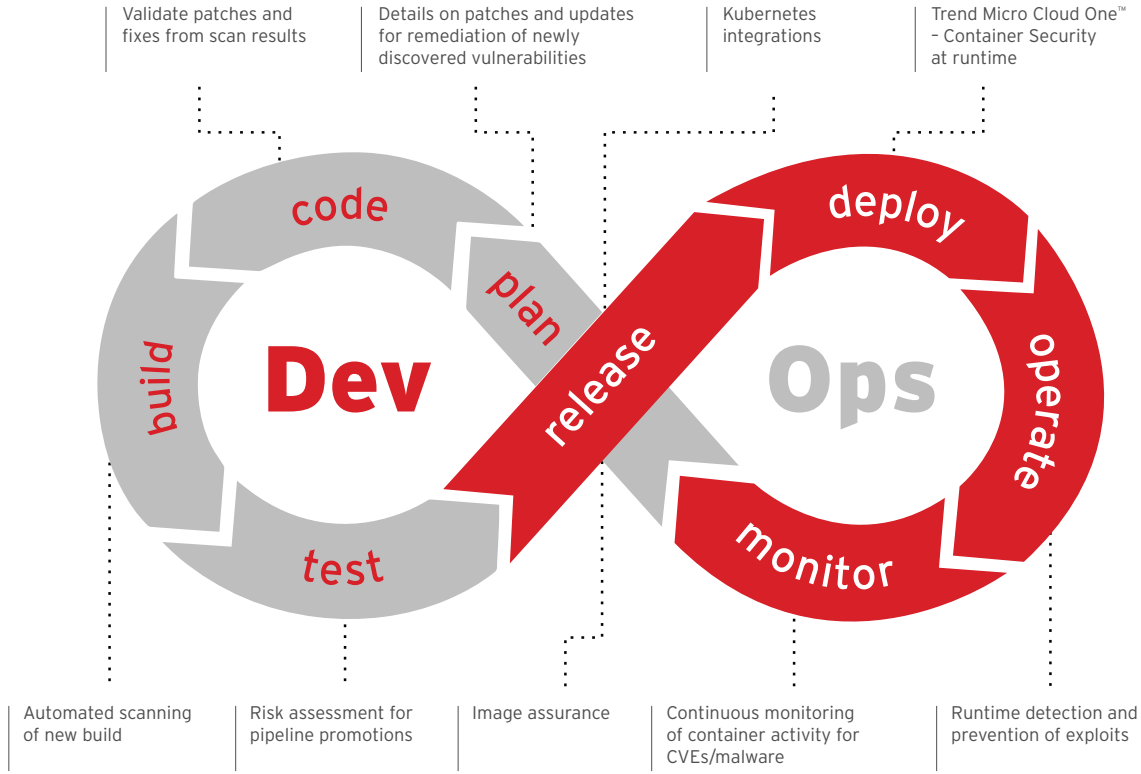
The next evolution: DevOps security

In response to these challenges, organizations began to integrate security into their development practices. Doing so has enabled robust security without extensive manual processes or the slowing of continuous deployments.

The key to accomplishing this is to make security a fundamental aspect of the DevOps culture. Security personnel should be brought into the development process early and often, and teams need security automation tools that can be integrated with the applications and environments they're already using without slowing down performance.

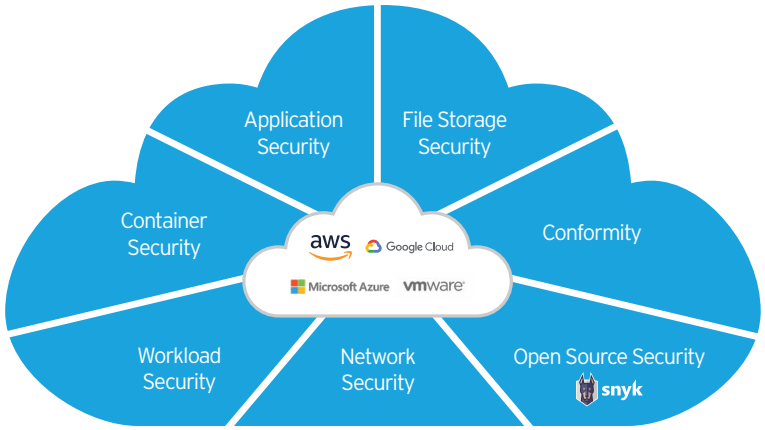
Finding the right technology to automate DevOps security

In order to execute this vision, organizations need to find a security solution that complements the speed of their DevOps culture. The optimal solution will integrate security from the initial stages of development through to deployment, and be automated, repeatable, and consistent. Using the right tooling, security teams can automate a large portion of their existing testing protocols and integrate them into the overall CI/CD pipeline. Moreover, modern tools such as security-as-code enable development teams to easily integrate and automate security themselves, without the intervention of the security team.



Introducing Trend Micro Cloud One™

With an exploding set of cloud infrastructure services and an increasing number of stakeholders involved in infrastructure and security decisions, the cloud has formed the perfect storm for security. In order to gain the benefits of the cloud and meet business objectives, cloud security needs to be made less complex. Introducing Trend Micro Cloud One, a security services platform for cloud builders, delivering the broadest and deepest cloud security offering in one solution, enabling you to secure your cloud infrastructure with clarity and simplicity. With support for all major cloud platforms, and solutions that integrate directly into your DevOps processes and toolchain, Trend Micro Cloud One is designed to provide the flexibility you need without slowing down your business or application delivery.



Trend Micro can help eliminate security roadblocks in your development practices. It does so by making security invisible and frictionless through automation. With Trend Micro, you have the right tools that are easy to implement and fit seamlessly into your team's DevOps processes, including AWS Quick Starts, AWS CloudFormation templates, deployment scripts, and extensive APIs.

Trend Micro Deep Security protects containers throughout your continuous delivery pipeline, from design to runtime using integrated image scanning, security as code, and machine learning. This enables you to deter known and unknown threats, without slowing development practices. Using Trend Micro Deep Security allows your security team to become a trusted partner across teams while increasing security adoption throughout your organization.

The Six Trend Micro Cloud One Services

With a comprehensive set of services designed specifically for the cloud, Trend Micro Cloud One secures the different parts of your environment within one simple platform

1. Trend Micro Cloud One™ - Workload Security

Runtime protection for workloads (virtual, physical, cloud, and containers)

Network security

Intrusion prevention (IDS/IPS) and firewall

System security

Application control, enhanced file integrity monitoring, and log inspection

Malware prevention

Machine learning, behavioral analysis, ransomware protection, and web reputation

2. Trend Micro Cloud One™ - Container Security

Build pipeline image scanning

Build time

Continuous build time and container image scanning within your CI/CD pipeline

Image deployment

Automatic image deployment to production/runtime

Malware scans

Scans for malware, vulnerabilities, and secrets, such as private keys or passwords, with remediation recommendations

3. Application Security

Security for serverless functions, APIs, and applications

Vulnerability detection

Detect against bots, hackers, and other bad actors who exploit vulnerabilities in web applications

Secure customer data

Secure web assets in the cloud and within local networks

No code changes required

Runs inside the process of your application without requiring any code changes

4. File Storage Security

Security for cloud file and object storage services

Decrease threat vectors

File reputation, variant protection, machine learning, and advanced intel

Gain flexibility

Automate file scanning, create custom actions, and view reporting and scan history details

5. Trend Micro Cloud One™ - Conformity

Cloud security and compliance posture management

Automate security and compliance checks

Through hundreds of automated checks against industry compliance standards and cloud security best practice rules, you can continuously improve your security and compliance posture for your cloud infrastructure

Simplify reporting

A single-pane-of-glass dashboard provides full and clear visibility of your entire multi-cloud infrastructure. Run reports on an endless combination of filters to exhaustively audit your infrastructure

Integrate with existing workflows

Conformity integrates seamlessly into your existing workflows and allows you to maintain full autonomy

6. Network Security

Cloud network layer IPS security

Network-based virtual patching

Intrusion prevention system (IPS) security at the network level to provide protection from network threats quickly

Inspection at network speed

Inspect ingress and egress traffic directly inline with network speed capabilities

Three Strategic Priorities

No matter where you are at in your cloud journey, Trend Micro Cloud One has you covered. From virtualization and cloud migration to DevOps, container, and serverless security—get an automated, flexible, and all-in-one solution for your cloud security priorities.

Cloud Migration

The transition to the cloud isn't as simple as clicking a button, and having a hybrid and multi-cloud strategy is the norm. That's why Trend Micro built the Trend Micro Cloud One platform with the ability to secure physical, virtual, and multi-cloud environments.

Cloud-Native Application Development

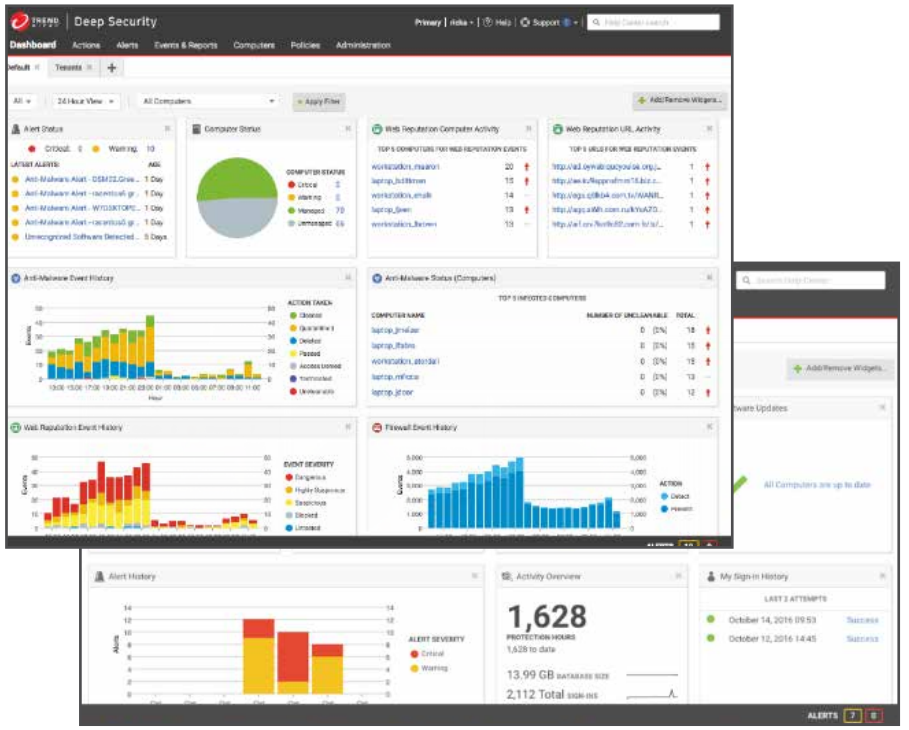
Working hard to deliver fast and iterate often, you are leveraging code in new ways and from different sources, such as infrastructure as code, open source, and public code repositories, which can introduce additional risk. Making matters more complicated, you have adopted new cloud services and processes to help you meet your objectives. You need security that supports this dynamic, complex approach without slowing you down. Trend Micro Cloud One does just that, by providing solutions for DevOps, cloud storage, cloud workloads, containers, and serverless

Cloud Operational Excellence

Organizations are adopting a cloud center of excellence model, with the goal of creating repeatable, consistent, secure, and compliant infrastructures that can be leveraged throughout the organization. Trend Micro Cloud One is optimized to be cloud efficient and will help you meet governance compliance and assurance requirements quickly.

How Pivvot secures their dynamic DevOps environment with Trend Micro

Pivvot is a software company that delivers cloud-based intelligent asset management systems to infrastructure organizations in industries such as oil and gas, power, and transport. To ensure robust security throughout the development process and life cycle of Pivvot's core product, Trend Micro was embedded into their development process. The solution also provided runtime protection for containers and the host, Amazon Elastic Cloud Compute (EC2) instances, on AWS.



With Trend Micro, Pivvot was able to:

- Enable a fast and simple development processes
- See threats in development build cycles
- Identify vulnerabilities within their systems
- Automatically scan public libraries for malicious content
- Keep up with the rapidly changing development environment on AWS

Read Pivvot's full success story **here**.

Begin securing your DevOps environment

Trend Micro Deep Security on AWS embeds security into your DevOps practices, making it frictionless to protect application stacks throughout the development life cycle. This solution complements developer agility and allows you to protect applications at scale.

Learn how Trend Micro Cloud One can fit into your DevOps environment:

aws competency

Trend Micro is an AWS Partner Network (APN) Advanced Technology Partner and Security and Containers Competency holder.

aws marketplace

Trend Micro solutions are available through **AWS Marketplace**.

[EBK02_Automated_Security_Speed_DevOps_210812US]