Trend Micro

DEVOPS PROTECTION WITH DEEP SECURITY

Build secure. Ship fast. Run anywhere.

INTRODUCTION

Today’s fast pace economy is changing how businesses respond to customer behavior and internalize an on-demand culture.

DevOps methodologies are being adopted in order to meet new market opportunities, as well as competitive and regulatory requirements. Enabling a continuous integration and continuous deployment (CI/CD) pipeline for developers requires a collaborative focus on security between InfoSec and DevOps teams.

Trend Micro™ Deep Security™ platform automates security within your DevOps processes and delivers multiple XGen™ threat defense techniques.

Deep Security offers protection for runtime physical, virtual and cloud workloads, and containers, as well as scanning of container images during development phases.

Deep Security reduces the number of point solution security tools and offers a single dashboard with combined capabilities for full visibility into leading environments like VMware®, AWS, and Microsoft Azure. Trend Micro Deep Security lowers the cost and complexity of securing workloads across multiple environments, including purchase options aligned to the way you want to buy, automated deployment, extensive API integration and security capabilities that can virtually shield servers from the latest advanced threats like ransomware and network-based vulnerabilities.

Why Trend Micro for DevOps?

• Ensure security works with you and integrates with your DevOps tools and environments
• Reduce disruption of development schedules and workflows with protection for images, containers, and your host
• Bake security into you development processes via APIs to improve development cycles and reduce human touch points and errors
• Maximize threat detection in your pre-runtime and runtime application development with threat intelligence from the Trend Micro Smart Protection Network™ infrastructure
• Help meet compliance requirements without impacting productivity and interfering in the CI/CD pipeline
DEEP SECURITY

Deep Security provides the freedom developer’s need to deploy applications rapidly, with the visibility and control that IT security needs to protect the developer’s intellectual property and the business platforms and environments. With an increased threat landscape and multiple development vectors available to exploit, organizations must become vigilant in providing appropriate security processes regardless of the environment.

SMART CHECK

Shifting security to the left, Smart Check delivers robust protection for Docker images with automated continuous scanning within the registry prior to deployment. Smart Check provides a unique two-pronged approach with vulnerability assessment, as well as malware detection. By understanding what vulnerabilities exist in an image, developers can fix issues before the images are scheduled in orchestration tools like Kubernetes.

PROTECTION FOR DEVOPS WITH DEEP SECURITY SMART CHECK

PROTECTION FOR THE BUILD CYCLE

Deep Security Smart Check delivers automated continuous image scanning with both vulnerability assessment and malware detection, image assertion, and access control. This is designed to secure images earlier in the CI/CD pipeline without negatively impacting the ability for DevOps teams to continuously deliver production-ready applications and meet the needs of the business.

BENEFITS OF DEEP SECURITY SMART CHECK IMAGE SCANNING

Prevent Exploits Prior to Runtime

Protect against vulnerabilities and malware with pre-runtime scanning of Docker images. Ensure threats are detected before applications are deployed and filter out false positives by correlating patch layers with packages that are vulnerable in the same image. Address vulnerabilities in images before being released in orchestration tools such as Kubernetes.

Expedite Deployments with Image Assertion

Development engineers have the ability to push images to production automatically. Allow images that meet security requirements to be deployed to production. Take advantage of automation features to minimize any need to manually oversee Smart Check and to configure authorized users and groups accordingly for role-based access.

Scan Images by Preference

Effective protection of containers begins with security for images. Deep Security Smart Check unpacks each layer of the image and performs detailed scans on the content. Benefit from fully automated, continuous scanning, triggered by new CVEs and take advantage of ad-hoc scanning enabling targeted inspection of specific vulnerabilities within specified images. Use the Smart Check console and scan coverage dashboard to look up scan results, target configuration, and to manage users and views. Additionally, you can access product operations through a documented collection of API-first resources, allowing DevOps to bake security into the CI/CD pipeline for simplified integration.
BUILD SECURE. SHIFT FAST. RUN ANYWHERE.

IT and DevOps are adopting technologies at a pace that makes sense to their goals and objectives, however their chosen tools must be able to cross multiple platforms and environments. IT security and DevOps teams see the value today more than ever in working together to mitigate security obstacles, while maximizing protection from threats that can infiltrate the perimeter or bypass the clutter of individual point security tools to harm the CI/CD pipeline. Visibility is key in managing and mitigating threats and vulnerabilities across multiple teams and security requirements. DevOps must be cyber-resilient and design security into their processes.

Continuous Container Security
Deep Security works seamlessly in the cloud to protect not only DevOps team’s container images, but also the container and host located on data center and cloud workloads. Designed with strong API integration for leading cloud vendors, Deep Security can protect cloud environments with auto-generated deployment scripts for critical security controls and exceptional protection for both containers and the Docker host, while DevSecOps can bake security into the CI/CD pipeline for frictionless pre-runtime scanning and automated protection of images. The Trend Micro Hybrid Cloud Security solution, powered by XGen™, leads the market in server, workload security, with proven deployments in thousands of customers, where we are protecting millions of physical, virtual, containers and cloud servers. Understanding and delivering on the need for security to be optimized for each strategic environment like VMware, AWS, and Microsoft Azure, Trend Micro provides organizations with an intuitive and consistent security experience across the hybrid cloud, including:

- **Extensive protection capabilities across both deployed containers and pre-runtime container images** which allows enterprises to:
  1) consolidate security providers and focus on a reduced toolset, 2) simplify the purchase process (fewer vendors, as well as options for marketplace purchases). This reduces ongoing management overhead and speeds compliance efforts (more controls in one product eases compliance efforts), 3) assure DevOps adoption of security controls with integration directly in to their CI/CD pipeline.
- **Automated, high performance security** that fits data center, virtual, container, and cloud environments (VMware, AWS, Azure). This includes securing applications that, 1) may live across environments (physical, virtual, cloud, multi-cloud, containers), and 2) are changing more frequently than in the past (changes hourly/daily/weekly compared to monthly/quarterly/yearly) as a result of microservice architectures.
- **Built on strategic partnerships** that align with customer strategic environments (VMware, AWS, Azure), enabling deep integration AND alignment with the evolution of how the environment works (technical, purchasing, market message, evolution of customer needs in application development).
- **Ability to secure physical, virtual, cloud and hybrid deployments** consistently, with an optimized solution that spans the control that IT security requires with the flexibility and non-intrusive security methods that DevOps teams demand.
- **Leverages the Trend Micro Smart Protection Network (SPN),** global threat intelligence for accurate and zero-day protections.
  - Antimalware
  - Vulnerability protection
  - Zero-day machine learning protection (machine learning in the cloud for latest machine learning algorithms)

Why Choose Trend Micro Deep Security for Containers?

- Security that is shifting left into the pre-runtime development process, to ensure application integrity in your pipeline with continuous image scanning
- Container protection against the latest malware, ransomware and vulnerabilities with IPS/IDS, application control, machine learning and more
- Leading cloud native security optimized for your hybrid cloud, CI/CD pipeline, legacy application migrations, and compliance needs

BUILD SECURE
Increased security and compliance requirements are causing unplanned work which means DevOps teams are not being efficient. Development and Operations teams need security-as-code that will help to reduce disruption but still satisfies security and compliance teams. Deep Security has smart security controls that ensure you meet security and compliance requirements from the first build.

Deep Security is shifting left with protection coverage for container images, as well as runtime workload protection.

SHIP FAST
While securing business environments is critical, DevOps teams are missing production targets because security is hard to implement and isn’t automated. Your teams need automated security to reduce friction and increase speed. With Deep Security, security is connected through automation and integration in your CI/CD pipeline with the tools that you already use today. Automate manual processes with security that integrates into your DevOps toolchain using RESTful APIs.

- Orchestration tools: Chef, Puppet, Ansible, AWS OpsWorks, Salt Stack, Kubernetes
- Monitoring tools: New Relic, AWS CloudTrail, AWS Config
- Continuous delivery: GitHub, Jenkins, Atlassian
- IT service management: ServiceNow for workflow efficiencies

RUN ANYWHERE
Security tools are often incompatible or simply not optimized for the cloud or your deployment processes. This means that security ends up causing high overhead, due to multiple environments requiring unique tools, thus hindering your ability to streamline operations. To fit into your processes, you need adaptable security tools that fit for anywhere you build, from data center to any cloud. Deep security is optimized for the place that best suits your application, ensuring that you can run your applications anywhere. Trend Micro Deep Security is an optimized security solution with API integrations to seamlessly build across leading cloud (AWS, Azure), virtualization (VMware), container (Docker), and data center environments.
AUTOMATED SECURITY FOR IMPROVED OUTCOMES

IT security must work with the needs of the business and help build the best security parameters into models that ultimately make the business more successful. The cloud model requires a shared security responsibility to be successful. Developers can build code into the CI/CD pipeline with rules that automate security into the development process, therefore removing manual interaction and allowing applications to be deployed more often while improving time to market.

**Updating Traditional Applications**

Updating traditional applications to run in modern infrastructure, like containers, requires consistent, automated security policies for optimal protection.

Developers are frequently improving software applications to reflect evolving customer needs. Smart Check introduces security earlier in the CI/CD pipeline to address security concerns and vulnerabilities prior to test processes and runtime deployment, eliminating deployment threats and building customer trust. Deep Security’s vulnerability assessment prevents problems by blocking network intrusions at the container level and vulnerability exploitation that can occur between containers and their host.

**Transitioning to a Hybrid Cloud**

Migrating some of your existing applications to the cloud allows developers to take advantage of cloud services and hybrid or multi-cloud environments. Deep Security Smart Check provides frictionless security out of the box that won’t slow down development while giving IT security the visibility and confidence in knowing that container images and the host are protected. Deep Security is designed for hybrid cloud environments with proven layered security techniques for protection of workloads and container deployments. Deep Security provides a single solution for container and host protection across the cloud and collaborative container development environments.

**Continuous Integration and Deployment**

Deliver integrated development practices that deliver applications to market faster with more reliability while being secure and reducing run-time complications. Developers can build applications at the speed of cloud, with multiple containers built into a single application, and shipped with the knowledge that it is protected from exploits. Smart Check provides concise scanning of threats and vulnerabilities across images. Automated image scanning and container protection helps to reduce human touch points and errors, improve run-time success, and deliver agile deployments of applications. Smart Check also implements security early in the CI/CD workflow process, where image vulnerabilities are less likely to impact production and business reputation, and can be identified, tracked, and mitigated automatically without relying on manual interaction. Container breaches can occur at the host level, whereby the underlying host OS must be hardened.

**Help with Compliance Requirements**

Deep Security helps meet governance and compliance requirements with effective security for cloud environments and container deployments. Organizations have the freedom to use multiple cloud platforms while keeping in touch with on-prem environments. It is important that security is applied with consistency across an organization for better governance and compliance. The nature of cloud environments means different security approaches are required. Deep Security meets compliance requirements with appropriate techniques, such as vulnerability assessment and malware prevention, while having full visibility and control of workloads across all environments, enabling automated protection based on the server (OS, application) and where it is (physical, virtual, cloud). This removes security gaps and eases compliance risks for IT security and DevOps.

To learn more about Deep Security for containers visit

[www.trendmicro.com/containers](http://www.trendmicro.com/containers)