Advanced Security Automation Made Simple
Albert Kramer
Technical Director Trend Micro

Augment your Kubernetes or Docker Deployments with Fast, Automated Protection
The only differentiator organizations have left... This, is DevOps!
What does faster look like?

OR

```bash
aws ec2 create-internet-gateway
```

OR

```bash
aws ec2 attach-internet-gateway
> --internet-gateway-id 12345 --vpc-id 54321
```
What does faster look like?
Whoever Slows This Down is the Enemy
So what are the challenges?
• Open repositories
• Out of date libraries and code
• No built-in vulnerability checks
• No malware/malicious code analysis
• Compliancy checks

Alpine Linux Docker images ship a root account with no password

Doomsday Docker security hole uncovered

Attackers can authenticate on vulnerable systems using the root account with no password. A security vulnerability has been disclosed for a flaw in runc, Docker and Kubernetes' container runtime. The vulnerability can be used to attack any host system running containers.

AESDDoS Botnet Malware Infiltrates Containers via Exposed Docker APIs

Posted on: June 14, 2019 at 5:03 am   Posted in: Botnets   Author: Trend Micro
Operations: People, process & technology

Modern app teams look like this

Security teams need visibility like this

VS
Validate patches and fixes from scan results
Details on Patches and Updates for remediation of newly discovered vulnerabilities
Kubernetes Integrations
Deep Security Protected Docker Hosts

Automated scanning of new build
Risk assessment for pipeline promotions
Image Assurance
Continuous monitoring for Docker activity and new CVEs/malware
Runtime detection and prevention of exploits
“Security used to be thought of as an inhibitor to development, but not anymore. Our teams understand that security is built into the environment. The security team is helping to steer the effectiveness of cloud operations,” Security Team - Infor

**Security Automation** - policy creation, and updates

**Deployment Automation** - security at scale

**Reporting Automation** - customizable compliance reports and leading SEIMs integration

**Monitoring Automation** - operational and security health of your environment

**Orchestration Automation** - integrate with your pipeline tools, SOAR tools, etc.
Automation Center
API first for hybrid and cloud native environments

Find - a solution to my problem by searching on Google
Learn - simple guides and example
Code - full RESTful API documentation. Examples of code
Verify - guidance around how to use applications to test APIs
Get Help - Stack Overflow, GitHub, and Trend Help

“Using Deep Security, we were able to improve our efficiency with Docker containers to realize savings for our AWS licenses and compute costs,”
Todd Williams – Manager SecOps at MEDHOST
Full Stack Container Protection

Securing your CI/CD Pipeline and Containers at Runtime
Trend Micro Deep Security Protects Your Journey
Trend Micro Deep Security

Try it Now

Trend Micro Deep Security solution, powered by XGen™, delivers multiple cross-generational threat defense techniques for protecting physical, virtual, cloud, and container workloads deployed in leading environments.

Connect your VMware®, AWS, Microsoft® Azure™, or Docker account in seconds to get full visibility and control.

Trend Micro Deep Security Smart Check

Try it Now

Trend Micro™ Smart Check security, powered by XGen™, protects your container images with continuous security, automated within your CI/CD pipeline.

Shift security earlier in the DevOps cycle with container image scanning for leading private and cloud registries.

https://trendmicro.com/containers
Choose the Right Security to Meet Your Team’s Needs

Get your 30-day free trial for Deep Security and Smart Check
Automated hybrid cloud workload protection via calls to Trend Micro APIs. Created with real data by Trend Micro threat researcher and artist Jindrich Karasek.

https://trendmicro.com/containers