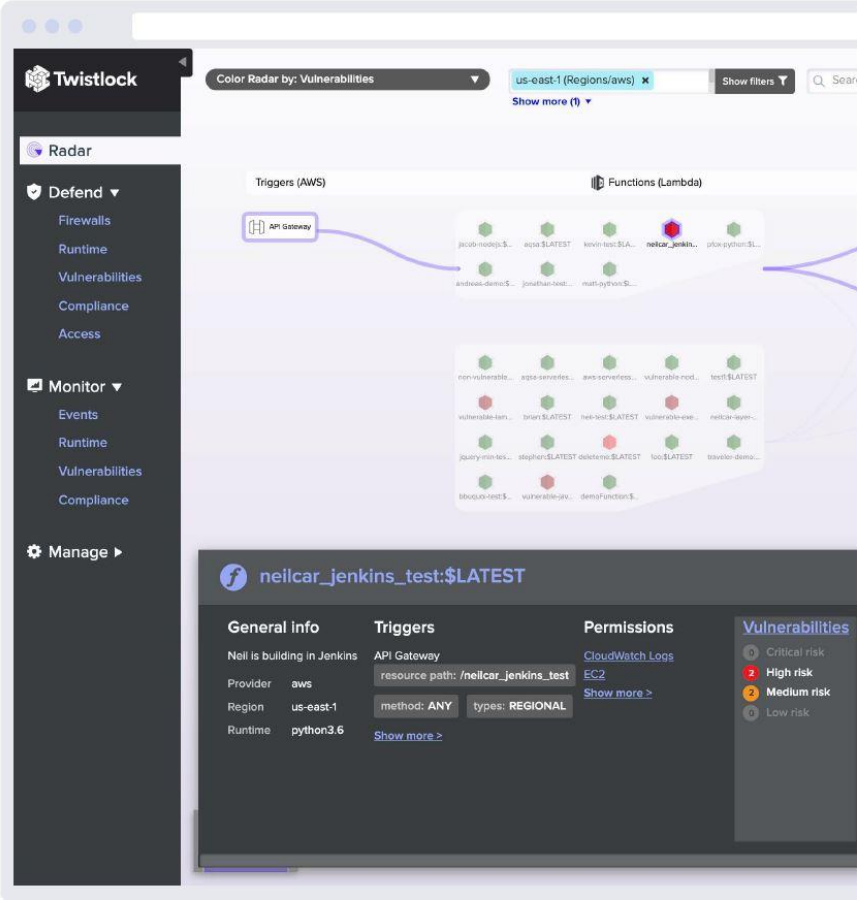
TWISTLOCK

CONTAINER- & CLOUD-BASIERTE SICHERHEITSLÖSUNG

Welche Eigenschaften müssen moderne Cloud-Umgebungen eigentlich bieten können? Zum einen müssen sie skalierbar sein, zum anderen müssen Dienste schnell hoch/herunter gefahren werden können, um flexibel auf Kundenwünsche zu reagieren. Mit Containeranwendungen, Microservices und dynamischen Infrastrukturen investieren immer mehr Unternehmen in ihre Effektivität. Zugleich sehen sie sich damit aber mit einer nie dagewesenen Komplexität der zu verwaltenden Anwendungen konfrontiert. Eine Komplexität, die sich schnell auf die Sicherheit auswirkt. Daher ist es umso wichtiger, eine zuverlässige, umfassende und moderne Lösung einzusetzen. Unsere Empfehlung: Twistlock.

Unser Partner Twistlock ist der führende Anbieter von Full-Stack-, Full-Lifecycle-Container- und Cloud-basierter Cybersicherheit für Teams, die Docker, Kubernetes, Serverless und andere native Cloud-Technologien einsetzen. Twistlock lässt sich in jedes CI-Tool und jede Registry integrieren und läuft überall dort, wo Sie Ihre nativen VMs, Container und Cloud-Anwendungen ausführen möchten.



Twistlock

Twistlock bietet einen integrierten Ansatz, um Container-Sicherheit zu gewährleisten und zu überwachen. Im Gegensatz zum traditionellen Vorgehen, klinkt sich Twistlock vollständig in die Continuous-Integration-Pipelines ein, zum Beispiel mit Jenkins, und interagiert nativ mit Docker oder Kubernetes. Das Twistlock-Framework ist eine Schwachstellen-Management-Suite für Container. Sie kümmert sich nicht nur um das Härten von Containern und Images, sondern auch um die Umgebung, in der die Container laufen. Konkret heisst das, dass Twistlock die Container auf Exploits sowie auf Anwendungs- oder Konfigurationsfehler untersucht und die Container-Aktivitäten überwacht. Dabei erkennt Twistlock Verstösse gegen Sicherheitsrichtlinien, meldet diese und greift bei Bedarf korrigierend ein. Wie Twistlock im Detail funktioniert, erfahren Sie in diesem Video.

FEATURE	BESCHREIBUNG
Automatisierung	Skaliert Sicherheit durch automatisches Erlernen (Baselining) des *normalen V*erhaltens einer Applikation, wozu auch die Kommunikation mit andern Cloud Services gehört. Basierend auf dieser Information werden «Allow Rules»-Laufzeitmodelle erzeugt. Zur Integration mit existierenden Tools stehen APIs bereit.
Sichtbarkeit	Twistlock stellt dynamische Ansichten bereit von Anwendungen, Komponenten und dem Sicherheitsstatus. Vulnerabilities und Compliance Issues werden bewertet. Jeder Host und Container verfügt über einen «Flugdatenschreiber» in Echtzeit.
Prävention	Twistlock ermöglicht automatisches Blocken von nicht-normalem Verhalten von Prozessen, Netzwerkverkehr und Aktivitäten auf Files zur Laufzeit gegenüber der Baseline. Es sind nur als Compliant eingestufte Anwendungen aus vertrauenswürdigen Quellen zugelassen. Twistlock setzt «Least Privilege» Networking und Micro-Segmentierung in Ihrer Umgebung durch und verhindert somit einen Wildwuchs an Service Accounts.

Twistlock unterstützt dabei eine breite Palette von Cloud Plattformen, wie AWS, Azure, Docker EE, Google Cloud Platform, IBM Cloud, Kubernetes, OpenShift, Pivotal und Rancher.

DIE WESENTLICHSTEN FEATURES VON TWISTLOCK

VULNERABILITY MANAGEMENT

Vulnerability Management identifiziert und verhindert Vulnerabilities über den ganzen Applikations-Lebenszyklus hinweg und priorisiert die Risiken in der Cloud-Umgebung.
Entwickler haben das Bedürfnis, Vulnerability Management in ihre «Continuous Integration»-Prozesse einzubauen. Security Teams hingegen möchten ein kontinuierliches Monitoring, das Erkennen und Verhindern von Risiken in Containern, Images sowie Servern. Twistlock ermöglicht hier ein effizientes Vulnerability Management, indem es Runtime Deployment einer Anwendung einer Risikobewertung unterzieht.

Prevent Risk Throughout the SDLC	• Verhindert Risiken während des ganzen Software Development Lifecycle • Erstellen von Policies. Darin könnten Sie bspw. definieren: «Verhindere, dass ein Docker Image mit mittleren oder hohen Java Vulnerabilities, für welches Hersteller-Patches erhältlich sind, gestartet werden kann.»
Security from Development to Production	• Sicherheit von der Entwicklung bis zum Betrieb in der Produktion durch Policy Enforcement • Anzeige von detaillierten Vulnerability Findings
Integrate Security with Your Current Toolkit	• Integrierbare Sicherheit mit einem Continuous Integration Tool dank offener Formate wie CSV oder JSON • APIs nutzen, um Twistlock in die bestehende CI/CD (Continuous Integration / Continuous Develoment) Tool-Chain zu integrieren • Entwickler, DevOps Teams und Security Teams können Risiken grafisch auf der Zeitachse verfolgen. • Darstellung von Trendlinien über identifizierte und gefixte Issues • Twistlock Intelligence Stream benutzt über 30 Informationsquellen, kommerzielle Ressourcen und eigenen Research zur Gewinnung von Vulnerability-Information.

RUNTIME DEFENSE

Runtime Defense umfasst Netzwerk- und Application Firewalls sowie Runtime Security für Container und Serverless Computing. Machine Learning schützt die Runtime-Umgebung: Netzwerk, Filesystem, Prozesse und System Calls.

Identification and Prevention of Threats and Anomalies	• Identifikation und Verhindern von Bedrohungen und Anomalien • Übersichtliche Darstellung • Korrelation und Analyse von Events, um Ereignisketten zu filtern für eine effektivere und schnellere Incident Response
Automated Modeling Powered by Machine Learning	• Automatisches Erstellen von Baselines (Models) einer Anwendung durch Machine Learning. Die Models definieren den «Known Good State» von Containern, Prozessen, Netzwerk, File System und System Call-Sensoren.
Flip Your Defense Approach	• Umgekehrte Verteidigungsstrategie: Anstelle eines statischen Modells, das alle möglichen Angriffsvektoren definiert, unterstützt Twistlock einen expliziten «Allow»-Modus. In diesem sind nur die spezifischen Anforderungen einer Anwendung im Model enthalten. Alles andere ist eine Anomalie und wird geblockt.
Protection Designed for Real World Attacks	• Twistlock Labs hat 0-days in verbreiteten OS und Orchestrators gefunden.

CONTAINER COMPLIANCE

Twistlock hilft Unternehmen bei der Überwachung, Erreichung und Durchsetzung der Compliance für Container und Cloud Environments. Als Lead Autor des NIST Container Security Guide (SP 800-190) und Contributor zu den CIS Benchmarks für Docker und Kubernetes, ist sich Twistlock der Wichtigkeit von Container Security bewusst. Unternehmen benutzen den Twistlock Compliance Explorer, um Standard-Konfigurationen, Security Best Practices, die Verwendung von Trusted Registries und empfohlenen Deployment Templates sicherzustellen.

Built for Internal and External Compliance	• Out-of-the-Box-Konfigurationen und Policy Controls um HIPAA, FISMA, PCI und GDPR Compliance zu unterstützen
Automatically Leverage CIS Benchmarks	• Die CIS Benchmarks für Docker und Kubernetes entsprechen Best Practices für Docker und Kubernetes. Built-in Checks helfen, die Compliance während des SDLC sicherzustellen. • Benutzerdefinierte Policies
Don't Just Monitor – Enforce	• Compliance wird nicht nur überwacht, sondern erzwungen. Twistlock kann nicht-konforme Container daran hindern, gestartet zu werden und stoppt Deployments auf nicht-konformen Hosts und Umgebungen.
Quickly View the Compliance State of Your Environment	• Compliance Explorer ermöglicht die Übersicht über alle Policies im Environment, den aktuellen Compliance-Status und über historische Compliance-Daten. • Über die letzten 30 Tage wird der Compliance Status grafisch dargestellt.

CONTINUOUS INTEGRATION / CONTINUOUS DEVELOPMENT (CI/CD)

Twistlock integriert Sicherheit in CI-Prozesse und Workflows. Damit können Probleme entdeckt und gefixt werden, bevor ein Deployment in die Produktion erfolgt. Entwickler sehen den Vulnerability-Status bei jedem Build, ohne ein separates Tool starten zu müssen. Security Teams können Policies definieren, die als Quality Gates dienen. Damit wird sichergestellt, dass nur konforme Software deployed wird.

Plug Security Into Your Current Toolkit	• Twistlock verfügt über native Plugins für CI-Werkzeuge wie Jenkins sowie über einen eigenständigen Vulnerability Scanner. Damit kann Sicherheit besser in den existierenden Build- und Deployment-Prozess integriert werden. • Automatische und Custom Policies lösen einen Alert aus, wenn ein Build unsicher ist oder stoppen diesen.
Security As Part of the Build	• Granulare Policies ermöglichen engmaschige Kontrollen über jeden CI-Task. • Sicherstellen, dass nur den Richtlinien entsprechende Images signiert und in die Registry gestellt werden
Up-To-Date Intelligence for Accurate Enforcement	• Alle Layer des Stacks, Base Layer der Images und die darin laufenden Frameworks wie Java, Node.js, Go, Python • Eine Binär-Analyse hilft, Vulnerabilities unabhängig davon zu identifizieren, wie eine Komponente einem Image hinzugefügt wurde. • Custom Rules unterstützen bei der Identifikation von Vulnerabilities in selbst geschriebenen Codes.

CLOUD NATIVE FIREWALL	
Die Twistlock-Plattform stellt Layer 3 und 7 Firewalls zur Verfügung, die automatisch die Netzwerktopologie von Anwendungen lernen und auf die Anwendung zugeschnittene Micro-Segmentierung Ihrer Microservice ermöglichen. Dies erlaubt es, neuartigen Threats in der Cloud zu begegnen.	
Automation Combined with Machine Learning	• Twistlock mapt, identifiziert und Whitelists den gültigen Verkehr in der Umgebung. • Twistlock erstellt dynamische Filter, die automatisch verdächtigen Verkehr unterbinden. Dies unabhängig davon, wo ein Container im Cluster läuft. Dabei muss die Art, wie Anwendungen built, deployed und ausgeführt werden, nicht geändert werden.
Purpose-Built for Cloud Native Apps	• Der Twistlock Cloud Native Application Firewall (CNAF) filtert automatisch Web Traffic zu den Anwendungen. Dies unabhängig von der Cloud, dem Cluster Node, der IP-Adresse oder Port, auf dem sie läuft. CNAF ermöglicht es der Twistlock-Plattform zu wissen, wo die Anwendung läuft und leitet Inbound Traffic automatisch zum Twistlock Defender weiter. • Ein optimierter, Applikations-spezifischer Layer-7-Filter schickt nur Clean Traffic zum jeweiligen Container.
Purpose-Built for Cloud Native Networks	• Der Cloud Native Network Firewall (CNNF) ist ein Container Aware, Maschinen Learning Layer 3 Firewall, der mit jedem Cloud Orchestrator arbeitet. • Die automatische Modellierung aller Traffic Flows zwischen Microservice erlaubt es Security Teams, Traffic Flows anzusehen und einen sicheren Traffic zu erzwingen.

ACCESS CONTROL	
Access Control sind gedacht für Cloud Workloads und Cloud Native-Anwendungen. Unternehmen können Twistlock einsetzen um Hosts, Docker und Kubernetes zu schützen sowie eine Integration mit Identity und Access Management Tools zu ermöglichen.	
Real Time Kubernetes Audit Event Stream Processing	• Twistlock ist ein Kubernetes Audit Dynamic Backend, welches Audit Events aus den Clustern entgegennimmt. • Erstellen von Stream Parsern direkt im Twistlock UI oder mittels einer Filter Library. Dadurch werden Events entdeckt wie laufende privilegierte Pods, Mounting Host Namespace und andere wesentliche Events.
Integrated, Full-Spectrum Secrets Management	• Twistlock hat das Authorization Framework in Docker und OpenShift wie auch das Pluggable Secrets Management in Docker Swarm erstellt. • Integration mit Secrets Management Tools wie Hashicorp Vault, CyberArk Enterprise Password Vault, AWS Secrets Manager, Microsoft Azure Key Vault
Host Auditing Capabilities	• Twistlock liefert vertrauenswürdige Audit Details über sensitive Operationen in Echtzeit (sudo, sshd, Docker API access).
File Integrity Monitoring	• Integriertes File Integrity Monitoring, um Compliance-Anforderungen durch Überwachung von Zugriffen auf spezifische Files und Pfade zu erfüllen. • Alerts wenn Config Files ändern, bei Read-Zugriff auf Kundendaten etc.
Log File Inspection	• Twistlock kann Security Log Files importieren (sshd, sudo, nginx), parsen und entsprechende Benachrichtigungen auslösen. • Regular Expressions für das Log Processing
Enterprise-Grade IAM Integrations	• Twistlock ist mit AD, OpenLDAP, Ping, Okta, Shibboleth, Azure AD und G Suite für ein zentrales Credentials Management integrierbar. • Pluggable Cryptography ermöglicht eigene Zertifikate und Smart Card Authentication für Konsole und Docker Socket.
Docker Role Based Access Control	• Basierend auf den Twistlock-Beiträgen zum Authorisierungs-Framework in Docker und OpenShift ermöglicht Twistlock feingranulare Role Based Access Controls.

Mehr Informationen zu Twistlock, Cloud und Container Security finden Sie auf unserer Homepage sowie im Cyber Security & Defence Blog von InfoGuard.

TWISTLOCK

BLOG

INFOGUARD – IHR PARTNER FÜR CYBER SECURITY

InfoGuard ist der Schweizer Experte für umfassende Cyber Security. Unsere über 120 Sicherheitsspezialisten in Zug und Bern sorgen täglich für die Informationssicherheit bei über 300 Kunden in der Schweiz. Wir bieten Ihnen ein ganzheitliches Lösungsangebot für die Umsetzung und Stärkung Ihrer Cyber Resilience.

SECURITY CONSULTING SERVICES – RISIKEN ERKENNEN UND BEHERRSCHEN

Ob Cyber Security, Governance, Risk & Compliance oder Cyber Risk Resilience: Die wachsenden Herausforderungen lassen sich nur mit einer ganzheitlichen Cyber-Security-Strategie meistern. Das modular aufgebaute Dienstleistungsangebot von InfoGuard berücksichtigt Technologien, Prozesse und Ihre Mitarbeitenden gleichermassen. Die langjährige Erfahrung im Bereich der Sicherheitsberatung und -überprüfung sowie in der Security Awareness sowie die erstklassigen Kompetenzen unserer Spezialisten stellen das reibungslose Zusammenspiel aller Elemente sicher.

NETWORK & SECURITY SOLUTIONS – ICT-INFRASTRUKTUREN OPTIMIEREN UND SCHÜTZEN

Effiziente Netzwerk- und Security-Infrastrukturen müssen das Optimum aus Performance, Sicherheit und Kosten erreichen. Das gelingt nur, wenn alle Komponenten perfekt aufeinander abgestimmt sind. InfoGuard bietet ein umfangreiches Portfolio an führenden Netzwerk- und Security-Lösungen für konventionelle, hoch virtualisierte sowie für Cloud-Infrastrukturen. Unsere erfahrenen und zertifizierten Experten unterstützen Sie im ganzen Lebenszyklus Ihrer Investitionen – von der Architektur und Design über das Engineering und die Integration bis hin zum Betrieb.

CYBER DEFENCE SERVICES – CYBERATTACKEN ERKENNEN UND ELIMINIEREN

Unternehmen müssen heutzutage davon ausgehen, dass Cyberangriffe nicht nur stattfinden, sondern auch erfolgreich sind. Eine wirkungsvolle Abwehr setzt erstklassiges Fachwissen und hochentwickelte Spezial-Technologien voraus. In unserem ISO 27001 zertifizierten Cyber Defence Center (CDC) in Baar bündeln wir modernste Technologien mit der langjährigen Erfahrung unserer Security-Experten und Threat-Analysten. Unsere Cyber Defence Services schützen Ihr Unternehmen rund um die Uhr.

InfoGuard AG
Lindenstrasse 10
6340 Baar / Schweiz
Tel +41 41 749 19 00
Fax +41 41 749 19 10
info@infoguard.ch

Office Bern
Stauffacherstrasse 141
3014 Bern / Schweiz
Tel +41 31 556 19 00