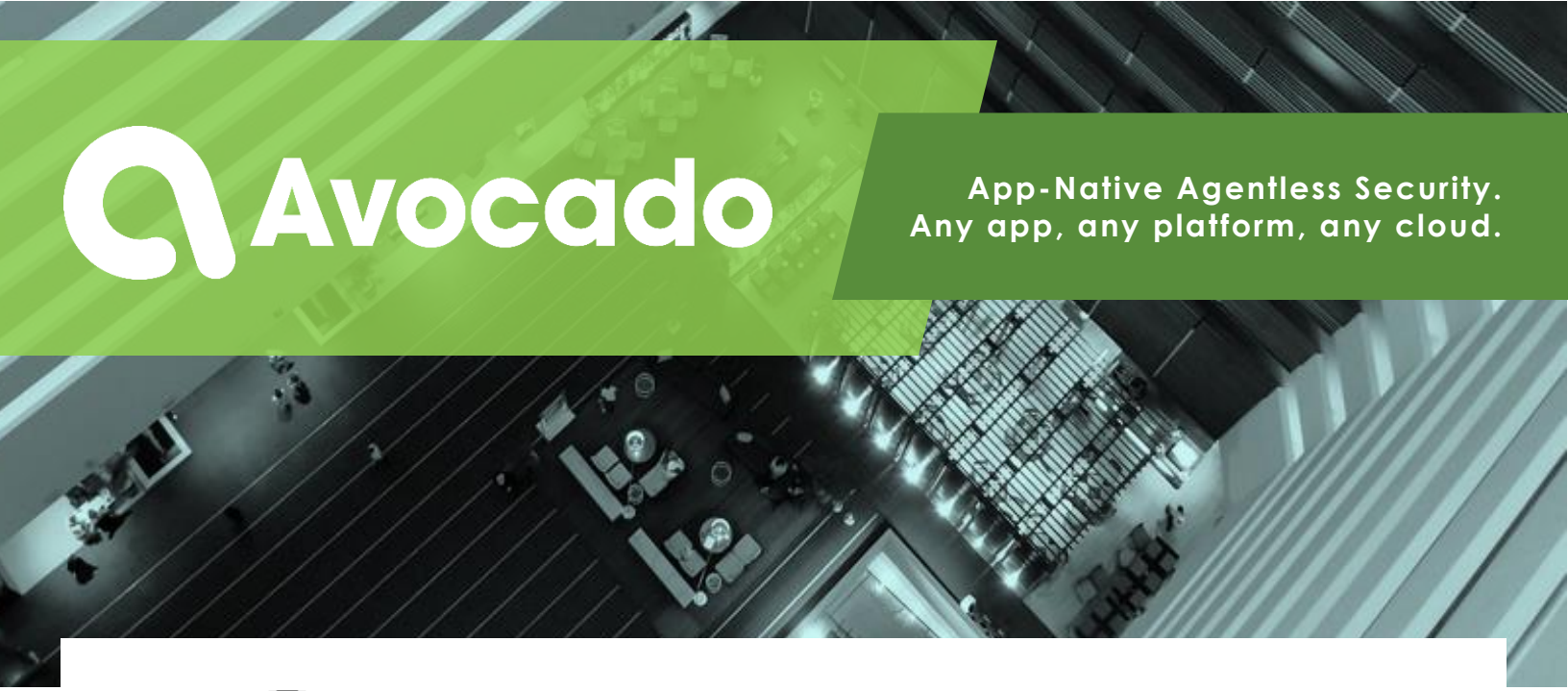
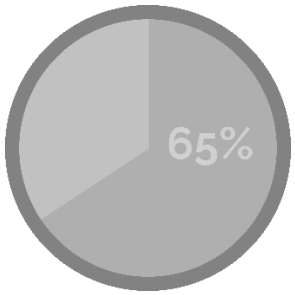
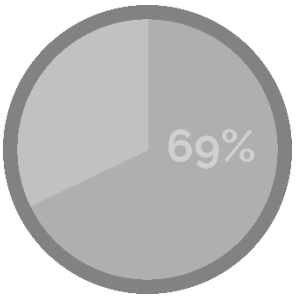


Avocado

App-Native Agentless Security.
Any app, any platform, any cloud.



65% of all public cloud breaches due to avoidable misconfigurations (Unit 42, 2019)



69% of organizations don't believe the threats they're seeing can be blocked by their anti-virus (Ponemon Institute, 2017)

Modern Threats, Modern Solutions.

Even the best perimeter defense is only as strong as its weakest link. Applications are easily exploited beyond the perimeter by Advanced Persistent Threats (APTs) and others, putting critical data and infrastructure at risk.

Current approaches simply cannot handle modern threats adequately. Network and/or perimeter security products like WAFs, NGFW, and vulnerability management tools aren't designed for runtime protection, leaving global brands, government organizations, and healthcare institutions in constant jeopardy.

On/off-prem, cloud, and container solutions of today all see similar issues:

- Complex policy configurations for signature-based solutions
- Delayed security with behavioral baselines
- Elastic, distributed apps with large amounts of internal communication leave countless vulnerabilities
- Lateral threats are often undetectable
- SSL management is complex and prone to attacks
- OWASP Top-10 is no longer enough to counter new attacks

Application-Native Security with Avocado Systems

Auto-Discover / Auto-Segment / Auto-Secure

Discover and secure application instances in runtime

- Minimize attack surface of every application instance
- Generate unique app DNA for verified communications

Bundle applications with native security and pico-segmentation

- Reduce SoC overhead with fewer false positives
- Secure all apps & DBs with no human intervention

Maximize granularity with none of the setbacks

- Reduce SoC overhead with fewer false positives
- Secure all apps & DBs with no human intervention

Runtime Deployment, Visualization, Detection, and Elimination

Deployment

- No policies to configure, no code changes, no re-compilation or re-linking required.
- Automated segment creation & policy generation
- DevOps-Friendly deployment (Chef, Puppet, OpenShift, etc)

Visualization

- Maps all session-level security events
- Logs detailed forensics for compliance & auditing
- Integrates seamlessly with SIEMs and ITSMs

Detection & Elimination

- Increased detection confidence with maximum granularity
- Detect threats at lowest possible attack surface
- Eliminate east-west threats with one-touch segmentation

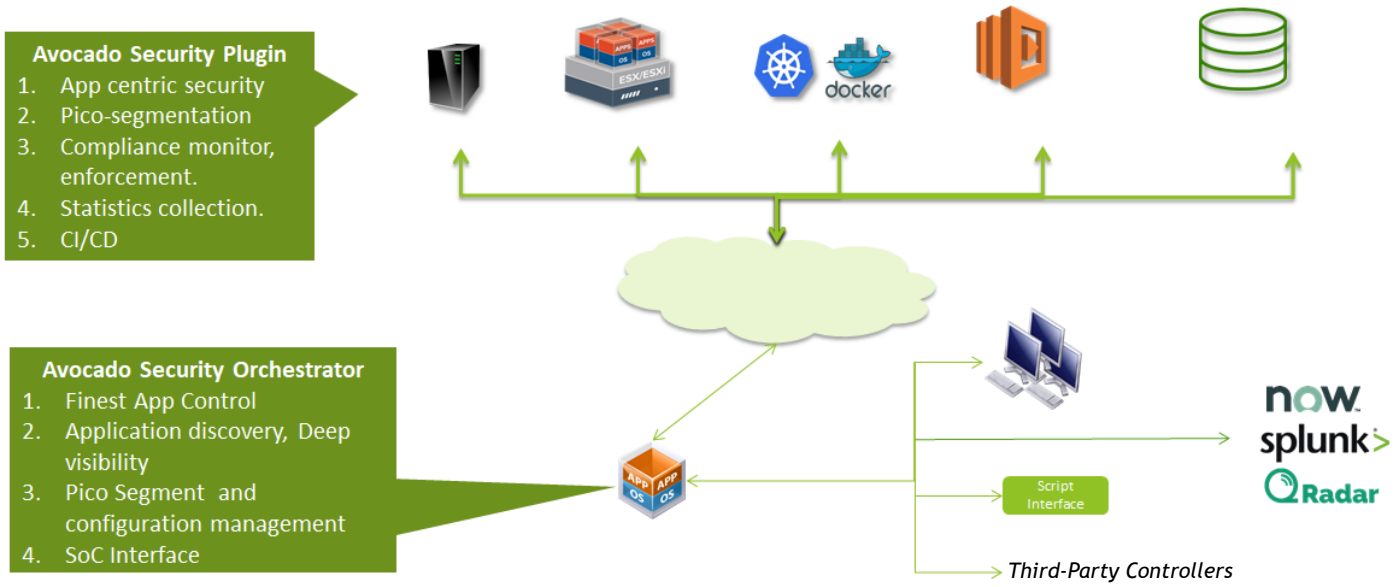
Security Orchestrator

One orchestrator for all application instances across multiple clouds, containers, and more.

Z-Ray

*Deep application visibility & dependency mapping with **fully automated discovery***

Spoof-proof Application Security & Data Protection



Avocado

Runtime Deployment, Visualization, Detection, and Elimination

Secure Applications Everywhere	- App-native security on bare-metal, virtualized, and containerized arch's - Hybrid-cloud, on/off prem, and private/public clouds supported
Stop Lateral Threat Spreads	- Default zero-trust for all unauthorized connections - Process-level segmentation on every workload
Minimized Policy Creation	- Dynamic session-level policies are auto-deployed during app launch - Unlike high level segmentation, no downside to increased granularity
Increased Threat Confidence	- Minimized threat surface increases confidence in detection - Reduced false-positives & increased application performance
Compliance Control Suite	- PCI/DSS and HIPAA compliance auditing and enforcement - Auto-generate compliant ringfences & segment legacy apps
Detect & Eliminate Pre-Existing Malware	- Automatically detect APTs that may already be inside your ecosystem - Kill APT processes instantly & generate ITSM tickets instantly
Remove Shadow IT Challenges	- Discover unauthorized applications, utilities, scripts, and more - Save time and cost with reduced IT intervention
	- Uncover communications between workloads within and across apps - Analyze with interactive graphical mapping

Linux Workloads

- RedHat 5.x, 6.x, 7.x (8.x soon)
- Ubuntu 14.04, 16.04
- SuSE Linux 11
- CentOS 7.x, Debian 8.x
- Oracle Linux 6.x, 7.x
- AWS Linux 1.x, 2.x

Deployment Tools

- OpenShift 4.1.x
- Puppet
- Ansible CentOS & Ubuntu
- Jenkins
- CloudFoundry
- Kubernetes

Certified Connectors

- Splunk 4.x, 5.x
- IBM QRadar 7.2, 7.3
- ServiceNow

Supported App Examples

- *Web Tier*
  - Apache Tomcat 7.x, 8.x, PHP
  - NGINX AvWAF 1.16.x
  - Apache WebServer 2
  - Oracle WebLogic 11.2, 12 cR2
- *App Tier*
  - Oracle RAC 11.2, Oracale DB
  - Java, C, C++, Python, NodeJS
  - C#, .NET
- *Database Tier*
  - Ingress
  - MySQL
  - MongoDB
  - Oracle Standalone/RAC 11.2,12
  - PostgreSQL, Microsoft SQL
  - CouchDB