Avocado Systems™

Application Security | Any App | Any Platform | Any Cloud

Security Consequences with MongoDB Applications:

Advanced Persistent Threats (APTs) progressively exploit applications—rendering them a weakest link, endangering applications and data security.

Current approaches using network and/or perimeter security products such as WAFs (Web Application Firewalls), NGFW, and vulnerability management,are inadequate to fully protect run-time applications — leaving global brands,government organizations & healthcare institutions in constant jeopardy.

Consider the following challenges for MongoDB applications on-prem or in the clouds:

- Deployments without administrative password and authentication, no network access control for database and misconfiguration in MongoDB security layer
- No network access control for database. No firewall rules for port blocking or restricting access on standard MongoDB ports e.g. TCP 27017
- Distributed and scale-out applications create vulnerabilities due to large amounts of application communications
- Current signature or behavior-based solutions require policy-based configurations, are complex to implement and generate too many false positives
- No mechanism to stop lateral movement of the threats

2016
In the US
888
Breaches
62% Stolen
BY OUTSIDERS

Most recent data breaches involved lateral or application-wide spread, and loss of PII, PCI, HIPPA data.

Avocado Solution for Securing MongoDB Applications

One-Touch Application Segmentation for Security and Compliance

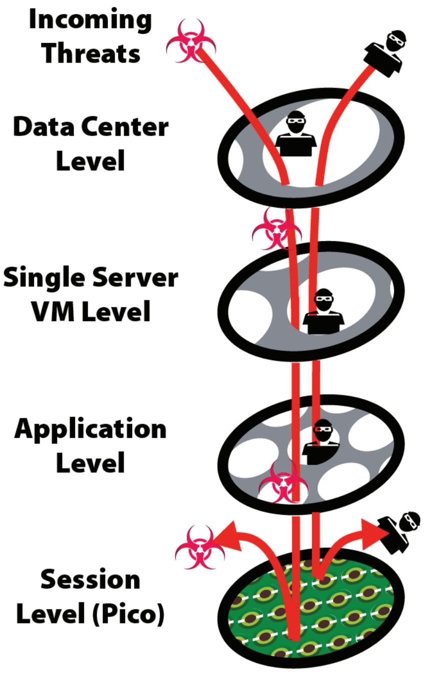
- Auto-Discovery
- Pico-Segments
- Applications Self-Protect

- Auto-Discovers & Secures Application Instances by:
  - Forming Pico-segments (one of the lowest possible units in the metric system) of application instances
  - Catalogs applications and their unique digital DNA
- Pico-Segments Create a Secure Layer Around Applications:
  - No requirement to encrypt the entire payload
  - Enables applications to self-protect
  - Single segmentation may include apps from multiple clouds

- Deterministic in Nature
- Produces Zero False Positives

- Deterministic Security Protects Applications:
  - High resolution dynamic application segmentation
  - Zero false-positives
- Application Data Protection Plug-in:
  - Provides real-time, deterministic security around applications
  - No policy configuration for most of the installation

Attack Surface Reduction



Real-Time, Deterministic Detection

- Threat detection at the lowest possible attack surface i.e. application socket descriptor
- No human intervention
- One-touch segmentation at the smallest attack surfaces
- No payload encryption required

Effortless Deployment

- DevOps friendly, integrated with Chef, Puppet, OpenShift and CloudFoundry
- No policies to configure
- No code changes
- No re-compiliation or re-linking
- Auto-discovery & security configuration
- Removes shadow IT challenges

Real-Time Threat Visualization

- Application session level security event visualization
- Collects detailed forensic & log information for compliance and auditing
- Integrated with SIEM (Splunk) and ITSM (ServiceNow)

Deterministic Application Security

Spoof-Proof Application Security & Data Protection

Avocado Solution's Key Components

Avocado Solution provides platform agnostic deployment to Bare Metal, VMs, Containers or Server-less application architecture. By design, it can massively scale to protect application instances in data centers, private, public, and hybrid clouds; spanning your needs as you grow.
Two primary drivers that work to provide you spoof-proof protection are as following:

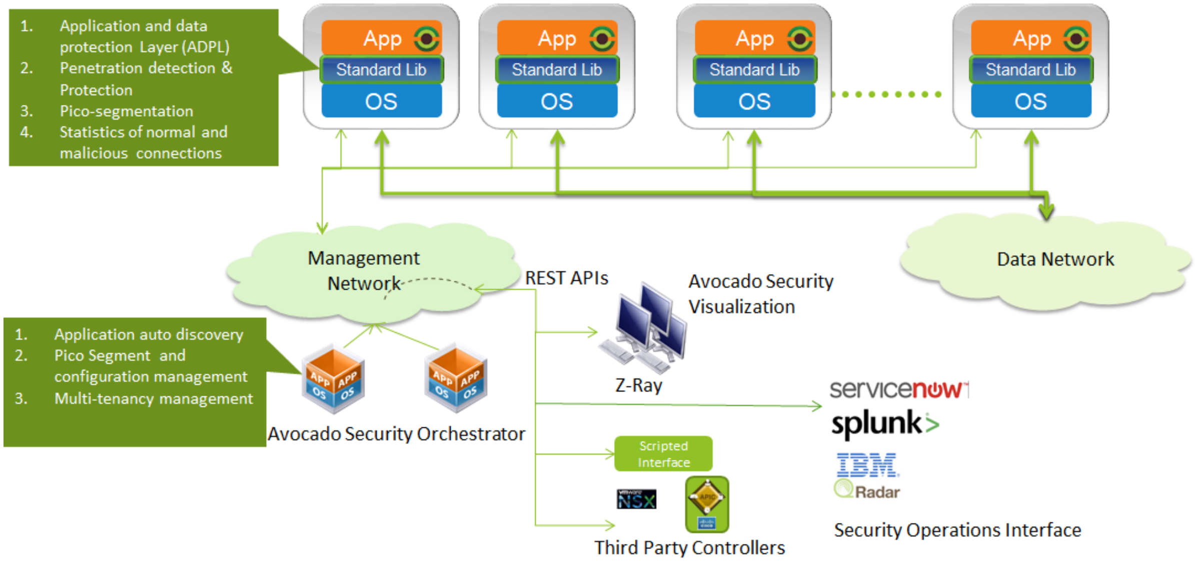
1

Application and Data Protection Plug-In
Security enforcement point that also collects malicious activities statistics and forensics from APTs.

2

Orchestrator
Performs application auto-discovery , auto-configuration and segmentation while providing complete programmability through RESTful APIs and a scripted interface, for DevOps automation and integrations with 3rd party controllers.

Avocado Platform Details



1. Application and data protection Layer (ADPL)
2. Penetration detection & Protection
3. Pico-segmentation
4. Statistics of normal and malicious connections

1. Application auto discovery
2. Pico Segment and configuration management
3. Multi-tenancy management

Avocado Systems™

MongoDB Application Protection on Any App, Any Platform, Any Cloud

Secured Applications Everywhere

- » Secures applications running bare metal, virtual, container or server-less app architecture
- » Across any data center, private, public, or hybrid clouds

Stops Threat Spreads (APTs, Malware, Ransomeware, NoSQL attacks, etc.)

- » Applications are Pico-segmented down to individual processes on workloads
- » All unauthorized connection attempts are auto-blocked

Minimizes Policy Creation

- » Dynamic One-Touch application segmentation from traditional policy based segmentation

Zero False-Positives

- » Threats are identified deterministically
- » Using mathematical algorithms
- » Resulting in zero false-positives

Enables you to meet Compliance Requirements

- » PCI, HIPAA, and other compliance requirements are easier to meet via application segmentation

Detects & Eliminates Pre-existing APTs or Malware in Real-Time

- » Catches an APT's first attempt to communicate with protected application
- » Kills APT's processes instantly in real-time
- » Auto-creates a service ticket with ServiceNow™ ITSM solution

Removes Shadow IT Challenges

- » Discovers unauthorized applications or ShadowIT elements for IT management
- » Reduces IT intervention
- » Substantial time and cost savings

Real-Time Visualization

- » Real-time communications between work loads, within and across applications display via interactive graphical maps
- » Threats are identified, mitigated, and displayed
- » Logs are sent to any SIEM solution such as Splunk or IBM Q-Radar

Platforms Supported

Linux Workloads

Ubuntu 14.04, 15.10. 16.04
Red Hat 7.x
SuSE Linux 11
CentOS 7.x

Windows Workloads

Windows Server 2012-R2
Windows Server 2016

Databases

Oracle 12c
MongoDB 3.x
MySQL 5.7.x
Hbase 1.1.3

Environments

Any hypervisor (VMware 6+, Hyper-V, KVM, Xen) in any cloud
Bare-metal servers
Containers
Server-less architecture
Private data centers
Any public clouds

(e.g. MongoDB Atlas, AWS, Microsoft Azure, Google Cloud Platform, Oracle Cloud, Rackspace Cloud)

Containers

Docker 1.1.x
Windows 2016

MONGODB WORLD'17 {SPONSOR}

Avocado Systems™

www.avocadosystems.net

Deterministic Application Security