AVOCADO SYSTEMS

Detect and Respond to Advanced Threats

Threats find a way in – that's a cybersecurity fact of life. It's critical to instantly detect threats, locally mitigate to *contain the risk and stop the spread*

Avocado Security Platform

Process Level Zero Trust
Block threats from trusted sources at the deepest level.

Stops Attacks the First Time
Catches attackers "in the act" without signatures or prior knowledge.

Autonomous Protection
Localized ML closes the security gaps without tuning or policy updates.

Prevents Lateral Movement
Runtime controls interrupt attack kill chains before damage is done.

Deep Visibility & Telemetry
Continuous observability down to the process level for real-time protection.

Automated App Threat Modeling
Discovery, dependency mapping, and threat exposure in minutes.

Operational Efficiency
No tuning, policy updates, false positives, or alert fatigue.

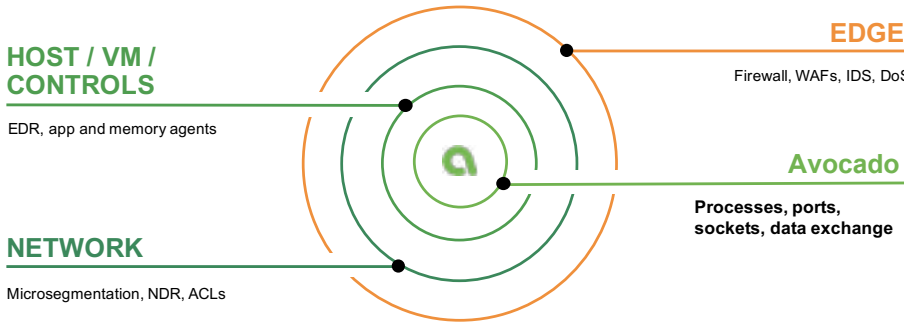
Built-in Governance Controls
Simplifies compliance with PCI-DSS, GLBA, HIPAA, and other standards.

The relentless wave of cyberattacks is getting worse because it's working. Attackers have the upper hand by utilizing difficult to detect advanced threats that circumvent existing security controls. If we continue to fight today's advanced attacks with yesterday's tools, we will keep losing with disastrous results.

Avocado Systems brings a new approach to stopping cyberattacks in their tracks. The solution takes on attackers where it matters most, in run-time at the application process level. It definitively detects attacks and stops them in real-time, before they spread throughout the network and become catastrophes.

Apply Zero Trust at the Process Level

Advanced Threats always find a way in. The precursors to the next attack are likely already inside your network. Perimeter controls are not enough. It's time to apply zero-trust principles throughout the entire environment, even to trusted systems. According to NIST, "zero trust security models assume that an attacker is present in the environment." AppXDR is the first solution to apply zero trust security down to the application process level. With Avocado you can detect and stop attacks in the act, and take immediate, automatic action, before damage is done.



Avocado operates at the deepest level and catches threat other controls miss.

Detect and Stop Lateral Movement

While threats may already be inside, what's critical is stopping the lateral spread to other systems, which turns isolated events into organizational and ecosystem disasters.

Avocado Systems

Eliminate Attack Windows

Localized machine learning and enforcement eliminates attack windows left by other solutions that rely on centralized threat analysis.

Build Better, More Secure Apps

No "shift" required, integrate native runtime security into workloads during development. Avocado provides DevSecOps friendly integration with any deployment design.

High Performance at Scale

Minimal performance impact and does not require changes to application code or heavy app agents. Avocado uses a lightweight OS plugin, deployed in user space, without privileged access to the OS kernel.

Fast Deployment

Embedded app security accelerates deployment. The onboard machine learning automatically generates policies without time-consuming manual policy creation or continuous tuning.

Avocado detects attacks early in the 'kill chain' and prevents unauthorized lateral movement between application workload systems. This effectively isolates threats and prevents attacks like ransomware from achieving their goals.

Automate High Efficacy Security Controls

Avocaod delivers autonomous security that doesn't requires manual intervention to be effective. Powered by machine learning, zero trust polices are automatically created and deliver local, autonomous protection without reliance on a centralized risk analysis engine. This provides high efficacy security, reduces operational costs, and eliminates constant, tedious updates.

Deep Visibility & Continuous Telemetry

The solution provides the deepest levels of application visibility, with continuous runtime observability. Deep forensic-level telemetry inspects application processes and data exchanges to ensure they don't become conduits for spreading threats. The same detailed telemetry can be fed directly to SIEM and XDR engines to provide a deep, rich data set for incident analysis by SOC teams.

Advanced Application Threat Modeling in Minutes

Traditional threat modeling is too slow, expensive and impractical. Avocado makes threat modeling fast and easy. With deep application visibility, it collects comprehensive details on dependencies and data exchanges. Avocado integration with leading threat modeling tools, such as OWASP's Threat Dragon, enables the application data to be imported to automatically to generate logical threat model diagrams with detailed application dependencies and associated threat data. This optimizes your security team's efforts to focus security controls where they are needed most and to address any coverage gaps.

Out-of-box Governance Controls

Avocado both improves security and simplifies compliance. A wide range of built-in in policy controls include PCI-DSS, GLBA, HIPAA and other standards.

About Avocado Systems

Avocado Systems focuses on protecting app and workloads from advanced cyber threats. The patented technology combines Zero Trust principles with machine learning, continuous observability, and autonomous run-time security. Avocado solutions enable organizations to efficiently threat model workloads, effectively manage risk, and enforce governance policies all while keeping pace with innovation.