AVOCADO SYSTEMS

Protecting Financial Services Applications with AppXDR

Cyber criminals are constantly looking to infiltrate financial systems. Once inside, they create more backdoors and move laterally. Avocado AppXDR stops these Advanced Threats before they can do damage.

At A Glance

Native runtime protection for workloads, apps, and APIs
Applies zero-trust down to the process level, allows only approved operations, even on trusted systems.

High security efficacy with near zero false positives
Local machine learning enables policies to be enforced directly on the protected systems.

High performance
Light weight plugin architecture requires minimal resources.

Automated application threat modeling
Discovery, dependency mapping, and threat exposure details in minutes.

Operational efficiency
Real-time threat detection and mitigation with virtually zero false positives eliminates alert fatigue and improves SOC efficiency.

It has been alleged that when the notorious 1950's American bank robber Willie Sutton was asked why he robbed banks, his response was simply "because that is where the money is." The same is true today, however, modern criminals no longer need to rob banks at gun point. Instead, they rely on sophisticated cyber-attacks. Using automation, they have virtually unlimited scale and no shortage of targets.

Digital Transformation Expands the Attack Surface

Digital transformation initiatives are top priorities as financial services organizations look to improve the customer digital experience. The effort to attract new and keep existing customers by delivering additional value has resulted in more application services and micro-services being developed with greater pace and agility.

This surge in application services has significantly expanded both the internal and external attack surfaces. Distributed and interconnected applications mean there is no longer a single security enforcement control point. Whether compromised directly or through lateral movement from existing malware, the individual components are ripe targets.

Avocado Systems helps financial organizations to defend the expanded workload attack surface. Avocado AppXDR technology provides virtually impenetrable run-time application security. The AppXDR has visibility and security controls at the smallest attack level – at the application and the application sub-processes. Workloads are actively protected without the need for centralized threat analytics that leave critical windows of vulnerability for attackers to do their damage.

Reduce Open Banking Risk

Open Banking continues to gain traction within financial institutions around the globe. Driven by customer demand for integrated financial services, Open Banking enables consumer banking information to be available and shared with other institutions (via APIs). Open Banking enables connected services that enhance existing consumer experiences such as real-time payments and account information services. Open Banking also unlocks tremendous potential for new revenue streams.

Avocado AppXDR

Deep Application Visibility

- Continuous and comprehensive application visibility.
- Feeds telemetry to SIEM and XDR engines.
- Automates dependency mapping and threat modeling.

Advanced Threat mitigation

- Stops Advanced Threats from moving laterally.
- Blocks malicious activity, even by trusted processes on trusted systems.

Zero Trust policy enforcement

- Applies Zero Trust principles down to the individual application process level.

Governance controls

- Built-in controls to help address regulatory and industry compliance requirements such as PCI-DSS, GLBA, and PSD2.

APIs are at the heart of Open Banking and are used to connect services for the exchange of financial data. Because these APIs are "open," they are also exposed to attack, fraud, and abuse by cyber criminals. Perimeter-security for APIs such as API Gateways and Web Application Firewalls can help to protect exposed APIs; however, sophisticated attackers can often bypass these edge-only controls. Because most API communications that pass through the gateway have been authenticated, and subsequently trusted, a single compromised API workload puts all connected workloads at risk.

Avocado AppXDR helps protect APIs by applying "zero trust" security controls around the API workload. These controls provide a local virtual ring fence around each API component and its subprocesses that locally analyzes each interaction, automatically blocking abnormal and malicious requests. This approach ensures that even if one API workload is compromised, an ecosystem partner API for example, it cannot laterally move throughout the API ecosystem to spread the infection. This helps financial institutions to keep sensitive data well protected and to address Open Banking security regulation requirements such as the EU's Second Payment Services Directive (PSD2).

Application Threat Modeling In Minutes

Traditional threat modeling, an arduous and manual process, has provided limited value because of its cost and lengthy time to complete. Making it worse, the output is out of date before it is even completed. Avocado AppXDR technology helps to simplify and automate Threat Modeling. Using deep application visibility, it collects application dependencies and comprehensive data exchange telemetry. The result is detailed logical threat models diagrams, containing complete application mappings and insights on potential attack vectors.

About Avocado Systems

Avocado Systems focuses on protecting applications and workloads from advanced cyber threats. The patented AppXDR™ 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.