ATTACKFENCE

Autonomous Cyber Defense Platform

Extended Detection and Response (XDR) Datasheet

A perpetrator needs only a small opening...

It is up to the cybersecurity teams to ensure that ramparts of the organization are well defended.

AttackFence® Extended Detection and Response (XDR) solution provides comprehensive context-linked visibility, detection and, response using multiple telemetry sources – Endpoint, Application Data and Network.

Cybersecurity teams need the ability to respond swiftly to incidents. With a single-pane-of-glass view across all data-sources, AttackFence® Autonomous Cyber Defense offers activity view right up to the application and user level using Windows™ or LINUX® based agents and in-depth view of critical business applications by ingesting log-data into its data-lake.

The outcome is a full 360-degree visibility and easy understanding of events to speed up triage.

AttackFence® XDR has built-in integration with leading Network and Endpoint Protection Platforms to support a single-click response ability that prohibit further onset of risky events.

Leveraging the console's retrospective analysis capability, one can easily perform in-depth forensic analysis and incident response thus maximizing the platform's utilization and eliminating the need for their analysts to work on multiple platforms when time is critical.

Analyse

Intelligent correlation of contextualized alerts from multiple control points using Machine Learning

Prioritize

Dynamic risk scoring and prioritization through event linking, threat intelligence and MITRE ATT&CK™ mapping

Accelerate

Reduced Mean Time to Respond(MTTR) owing to streamlined automated response through multiple integrations

Solution Highlights

Sensors
- Network
- Endpoint (Agent & Agentless)
- Application Logs

Performance
Network – up-to 40Gbps
Event-rate – 500,000 EPS

Threat Detection
- Signatures, Behavior-based
- Real-time Threat Intel
- Statistical Anomaly, AI/ML

Response Integrations
- Direct via Endpoint agent
- EPP, UTM & NGFW
- SOAR
- AD, L2/L3 Network gear

Services
- Incident Response
- MDR (via partner)
- 24x7 Support

ATTACKFENCE

Autonomous Cyber Defense Platform

Scalability & Availability	Method
Redundant Deployment	Supported. Active-Standby for Network Sensor
Throughput scalability	Supported. Using an external Network Packet Broker to cascade multiple sensors
Endpoint Agent/Agentless	Supported. Multiple endpoint managment stations

Service & Support	Using/For
24x7 Support	E-mail and Telephonic
Professional Services	Solution sizing, systems architecture, implementation & commissioning
Engineering Services	Incident Response and Infrastructure Integration
Managed Services	Managed Detection & Response (via partner)

Reach us:
connect@attackfence.com | +91 9818855853

ATTACKFENCE
Autonomous Cyber Defense Platform

AttackFence Techlabs Pvt. Ltd.
426,428, Tower A,
Spaze I-tech Park, Sector 49,
Sohna Road, Gurugram-122018

www.attackfence.com

About AttackFence

We are a cybersecurity product company offering XDR [Extended Detection and Response] solution. Superior effectiveness of our solution emanates from our leveraging knowledge of attacker behavior during different phases of an attack. The solution provides comprehensive visibility across network, endpoint, cloud workloads, containers and SaaS for improved profiling and compliance. Multi-pronged analytics approach based on MITRE ATT&CK™ framework and Machine Learning algorithm mesh enables the solution to detect even stealthiest of malware. Deployment can be on-premises, 100% in the cloud or hybrid. Our XDR's Detection based on attacker's behavior and swifter response via integrations with existing security and infrastructure components would make you more effective against cyber-threats while keeping TCO low.

©Copyright 2023 AttackFence Techlabs Pvt. Ltd. All Rights Reserved. AttackFence is a registered trademark of AttackFence Techlabs Pvt. Ltd.