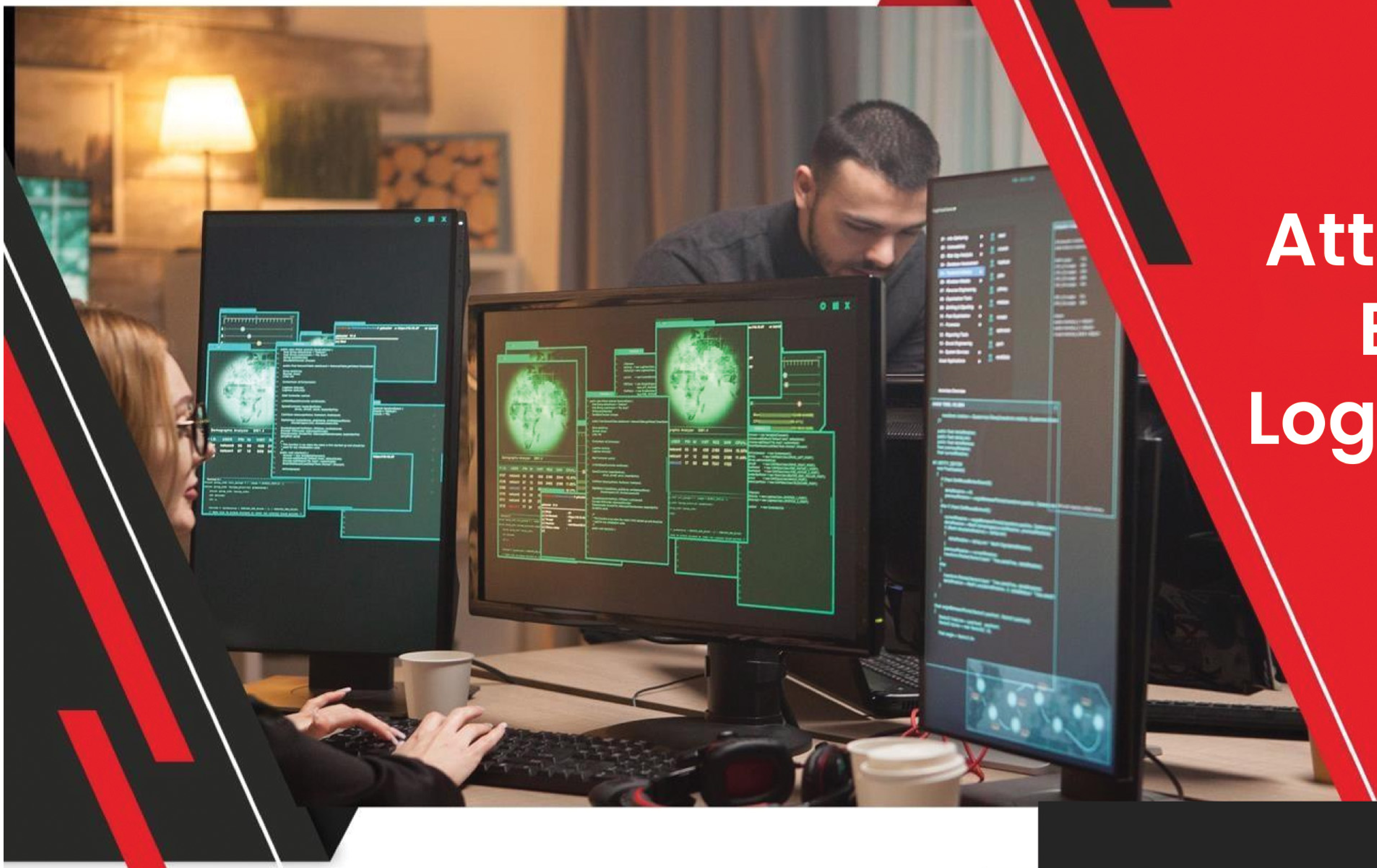
ATTACKFENCE
Autonomous Cyber Defense Platform



AttackFence Enterprise Log Manager

Making an IT or cybersecurity decision is often a complicated process. An important element in accomplishment of data-driven decision is the information being generated by currently deployed systems, applications and, tools themselves.

Gathering that data and making sense of it is a cumbersome process often rift with analysis fatigue and lack of adequate tools to help collect, normalize, prioritize & examine available data.

AttackFence® Enterprise Log Manager is an easy to implement solution for such needs. It is capable of ingesting, segregating and, storing incoming messages at throughput up to 100,000 events/second. Using an in-built data grouping algorithm, the solution identifies frequent patterns and anomalies to improve turnaround time for informed decision-making. The data-grouping algorithm finds its use among Cybersecurity, Business Analysts, Finance, IT and, Network teams to detect issues, identify capacity and security gaps with the objective of eliminating analysis fatigue and improving quality of outcome.

The Enterprise Log Manager dashboard is built with minimalistic design concept offering relevant insights and analysis at user fingertips. AttackFence User-Experience services enable customers maximize their investment by requesting for custom dashboards to suit their unique business needs.

Complying with CERT-In directive becomes extremely simple through Enterprise Log Manager. Required logs can be sent to CERT-In promptly using Enterprise Log Manager instead of businesses deploying expensive man-hours to comply, hence saving huge cost.

Solution Highlights

Log Management

- Standards-based TCP/UDP Syslog server
- Ingest structured, semi-structured or even unstructured logs in different formats like clear-text, csv, JSON, XML, CEF, W3C, etc.
- Hierarchical storage for faster search and retrieval
- Log-rotation and Log-retention policy enforcement

Performance

- Throughput: up-to 100,000 messages/second

Enrichment Integration

- Open-Source/Commercial Threat-Intel
- Custom Integrations

Services

- User-Experience Services for custom dashboards
- Engineering Services for Integration with Fraud/Risk Management Databases
- Professional Services to identify patterns and anomalies using a combination of expressions and rules

Solution Components	Capacity
Log Collector	100,000 Events/Second
Storage	10TB inbuilt
Collection Mechanism	Standards-based SYSLOG TCP/UDP

Scalability & Availability	Method
Storage Expansion	Supported. Integration with SAN/NAS/DAS
Increase Throughput	Supported. Using Load-balancer or Proxy

Service & Support	Details
24 x 7 Support	E-mail & Telephonic
Professional Services	Sizing, Implementation & Consulting, Data-grouping algorithm customization
User Experience Services	Dashboard/Analytics customization
Engineering Services	Integration with open-source/commercial enrichment data sources, and with binary log source integration

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.