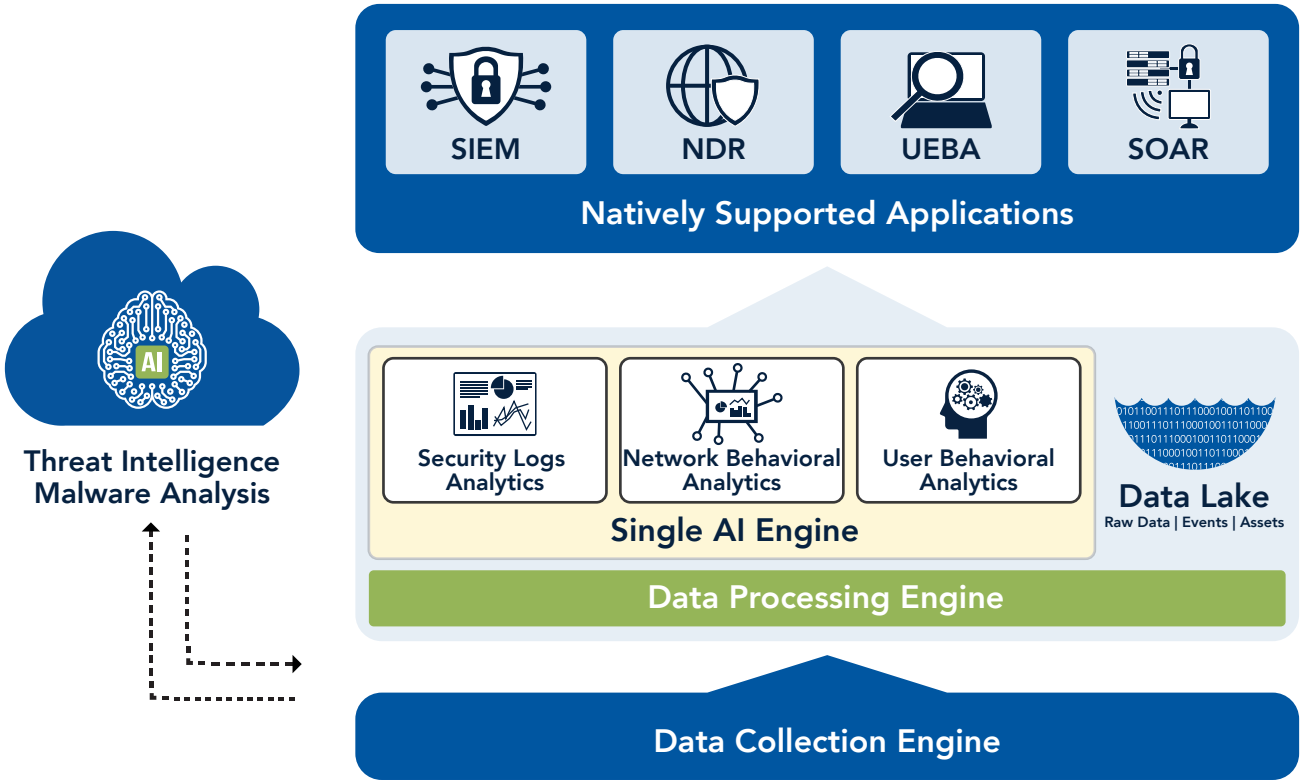
MANAGED NEXTGEN SIEM POWERED BY OPEN XDR

Too much data, not enough action. Today's SIEMs are not able to effectively weed through the vast amount of data nor deliver accurate and actionable alerts. As a result, analysts spend more time looking for incidents than on remediation or preventing them occurring again.

Enter XDR. Using Machine Learning, large amounts of data are instantly analyzed and correlated, resulting in the important alerts filtering to the top. With the right data, analyst spend time investigating true incidents. Through extended integration capabilities, remediation and orchestration with other security tools is possible from one interface, manually or automated. BriteProtect combines, XDR with SIEM, NTA, UEBA and SOAR to give customers the functionality they need today, in one easy to use interface.



Brite People.
Brite Solutions.

COLLECT THE RIGHT DATA

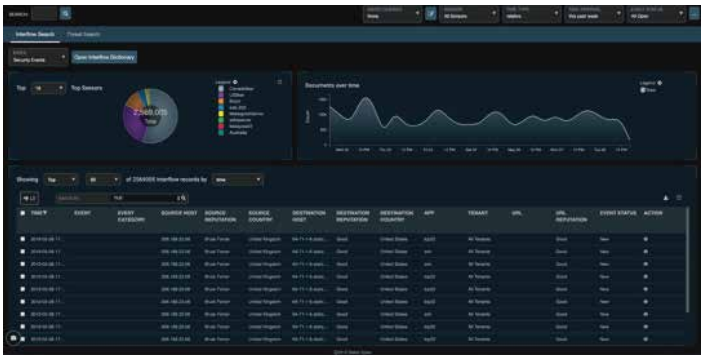
BriteProtect's XDR platform has data collection at its core. We solve the challenges of having too much data, not enough data or no context to data by normalizing data as it enters the system. Then, the data is reduced, enriched with other telemetry and fused into one record to provide context to what is actually occurring.

DETECT THE REAL THREATS

By mapping out over 50,000 detections of known and unknown behaviors against the cybersecurity kill chain, BriteProtect's XDR platform acts as an early warning detection system. Unlike other solutions in the market, BriteProtect has complete kill chain detection because of the its rich data collection and correlation.

INVESTIGATE PROBLEMS

The search for the unknown is as important as the detection of the unknown. Brite's team of analysts search through the rich dataset for malicious activity by creating simple and complex queries. These queries can then be saved and turned into custom visualizations and automatic reports or notifications.



AUTOMATIC RESPONSE

Automatic and appropriate response is critical when ensuring a secure environment. An event can automatically trigger the creation of a trouble ticket with its built-in case management system, trigger email, Slack and restful API alerts, automatically send out POF reports and signal firewalls to take appropriate actions. Additionally, with orchestration plugins for SIEMs, XDR detections can automatically trigger playbooks to enact.

MANAGED BY BRITE'S TEAM OF EXPERTS

The Brite team takes on the burden of daily monitoring, management and response to mitigate alert fatigue and missed critical events. Now, your team will then have the bandwidth to focus on strategic initiatives.

See just what we can take off your plate:

- Appliance Set-up
- Configuration
- 24/7 Log Investigation & Analysis
- Proactive Threat Hunting
- Normalization of Data
- Correlation of Data
- Playbook Development
- Automated Incident Response
- Software & Firmware Updates
- Subscription Updates
- Policy Review & Updates

Gain superior security and orchestration with XDR managed by the Brite team

Brite

Technology and people are at the core of everything we do. Brite is committed to proactively protecting communities and organizations through innovative technology solutions delivered by our talented team. We recommend thoroughly evaluated industry-leading technologies and pair them with proven processes to assist our clients in effectively achieving their goals and objectives.

At Brite, **good enough is never enough**.

www.Brite.com
1.800.333.0498
SalesInfo@Brite.com