ENDGAME.

SOLUTION BRIEF

ENDGAME REFLEX™

Reflex is the first technology that moves customized protection within reach of IT Operations – a simple language, an IDE that allows rapid and thorough testing against a comprehensive history of enterprise user behavior and endpoint configurations, and a host-based execution engine that eliminates the time between detection and response, addressing the 'breakout window' across enterprise networks.

Nobody knows an organization's environment better than its IT security team. Software deployment tools, networking and routing nuances, threat models, operational IT tasks, change controls, and more, prove that there are many things that make one infrastructure infinitely unique compared with another. Yet security vendors try to solve the same problems for every organization in the same way. The most aggressive of preventions are disabled and often hidden, to avoid the deluge of false positives. Detections are suppressed until cloud services can analyze the stream of events and identify an attack, stopping potential alert fatigue and hiding inaccuracy, yet opening a threat window for adversaries to exploit.

REFLEX = EXTENSIBLE QUERY RULES + RESPONSE ACTIONS

The compromises made by some security vendors help them deliver "just good enough" for some customers, at the expense of efficacy and visibility for all customers.

Where SIEMs, SOARs and even UEBAs have failed to deliver against the promise of improved detection and response by correlating events from multiple sources, Endgame Reflex fires in the right place, on the endpoint instead of a data lake, but more importantly it fires at the right time - instantly.

Endgame's autonomous agent already imparts the defensive experience and adversary knowledge of Endgame's world-class threat research team. With out-of-the-box preventions and detections covering the breadth and depth of the MITRE ATT&CK matrix, Endgame was found to be the leader in the inaugural MITRE ATT&CK evaluation which simulated an attack by APT3 - a threat group that researchers have attributed to China's Ministry of State Security.

With Endgame Reflex, customers can take full advantage of both their IT security team's tribal knowledge and the most accurate vendor authority provided by Endgame's award winning pre-built rules. Security analysts can create new rules from scratch or extend one of Endgame's pre-built rules, and once the criteria is matched, the Reflex response executes.

REFLEX ELIMINATES THE TIME BETWEEN DETECTION AND RESPONSE

Almost identical to Endgame's pre-built preventions and detections, Endgame Reflex uses two components:

1. A FULLY CUSTOMIZABLE DETECTION RULE, BUILT USING EQL.
2. AN ACTION TO TAKE IN RESPONSE TO THE RULE FIRING.

Security analysts can craft new EQL queries or extend an existing EQL query, and once the criteria is matched, the Reflex response is executed.

WHAT IS EQL?

Event Query Language is an extensible, open-source language built in-house at Endgame to express relationships between security-relevant events. We designed it to be generic, apply to multiple use cases, and avoid reliance on any particular architecture. Powering Endgame's high confidence detections, EQL is used to perform basic searching, and gives hunt teams the tooling necessary to easily sift through massive amounts of data. EQL has a minimal learning curve where rules are written and read in plain English.

REFLEX IMPLEMENTS REAL-TIME ENFORCEMENT

Endgame has a unique approach to endpoint data collection, implementing a zero-trust model when it comes to extracting information from the OS. Most vendors focus on gathering a subset of the easy to get (but easy to tamper with) events streamed from Event Tracing for Windows (ETW). Endgame gathers, enriches, stores, and protects the endpoint activity data itself. Building custom rules against the same trusted data leads to more high-fidelity, high confidence detections that fit the organizations unique needs.

Customized endpoint detection capabilities have traditionally been wholly manual, reactive, and restricted to searches of offline data, due to the risk of poorly designed queries overwhelming the security analyst with false positive alerts. With Endgame's tamper-proof data bringing unrivalled accuracy, and autonomy that does not require cloud-services to impart authority, Endgame Reflex is ideal for implementing the real-time enforcement of security controls and the real-time detection of suspicious and malicious activity.

To ensure that Endgame Reflex performs the expected response to an exact set of defined behaviors, the rule-building IDE includes two key safeguards:

- First, the EQL rule is examined and validated in real-time, as the security operator types – removing the burdensome tasks of making a change, saving, and testing to ensure correct syntax.
- Second, the rule can be tested against historical data already collected from endpoints, without creating any new alerts or generating any responses. Testing against historical data reduces the chance of false positives by showing exactly what action would have been taken if the rule was in Endgame Reflex before then.

Endgame Reflex runs in-line on the endpoint, with no need for human interaction or confirmation, to stop adversaries before they have the chance to cause damage or loss. Reflex allows operations teams to deploy controls enforcing security policies and risk, compliance and governance items such as PCI-DSS, HIPAA, and more.

EXAMPLES

FIG.1 | An example of an EQL query to detect adversary behavior over a period of time.

FIG.2 | Create EQL queries from scratch or by extending from Endgame's existing library.

FIGURE 1

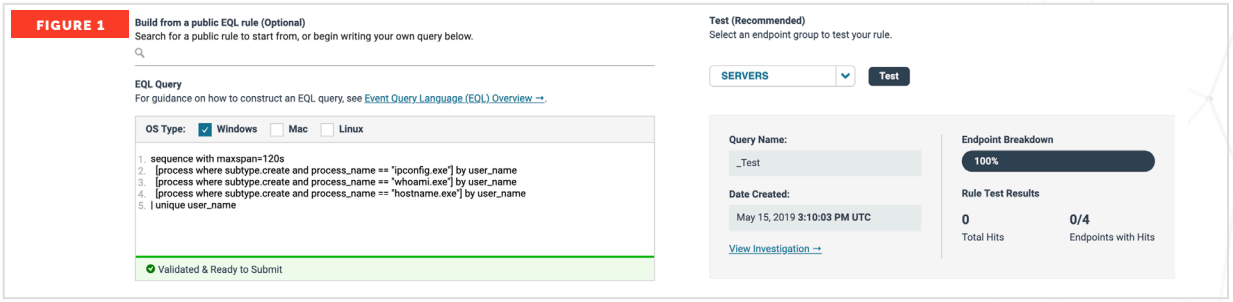

FIGURE 2

ABOUT ENDGAME

Endgame makes military-grade endpoint protection as simple as anti-virus. Leveraging the industry's most advanced machine learning technology, Endgame enables security operators of any skill level to deliver full-force protection, stopping everything from ransomware, to phishing, and targeted attacks. Endgame is the only endpoint security platform to offer a unique hybrid architecture that delivers both cloud administration and data localization that meets all industry, regulatory, and global compliance requirements. The US military as well as the world's largest commercial organizations rely on Endgame to protect their people, technology and mission, globally. For more information, visit **www.endgame.com.**