Introducing Elastic Endpoint Security

endgame.com/blog/technical-blog/stopping-olympic-destroyer-new-process-injection-insights

October 15, 2019

Editor's Note — August 19, 2020: The Elastic Endpoint Security and Elastic SIEM solutions mentioned in this post are now referred to as Elastic Security. The broader Elastic Security solution delivers endpoint security, SIEM, threat hunting, cloud monitoring, and more.

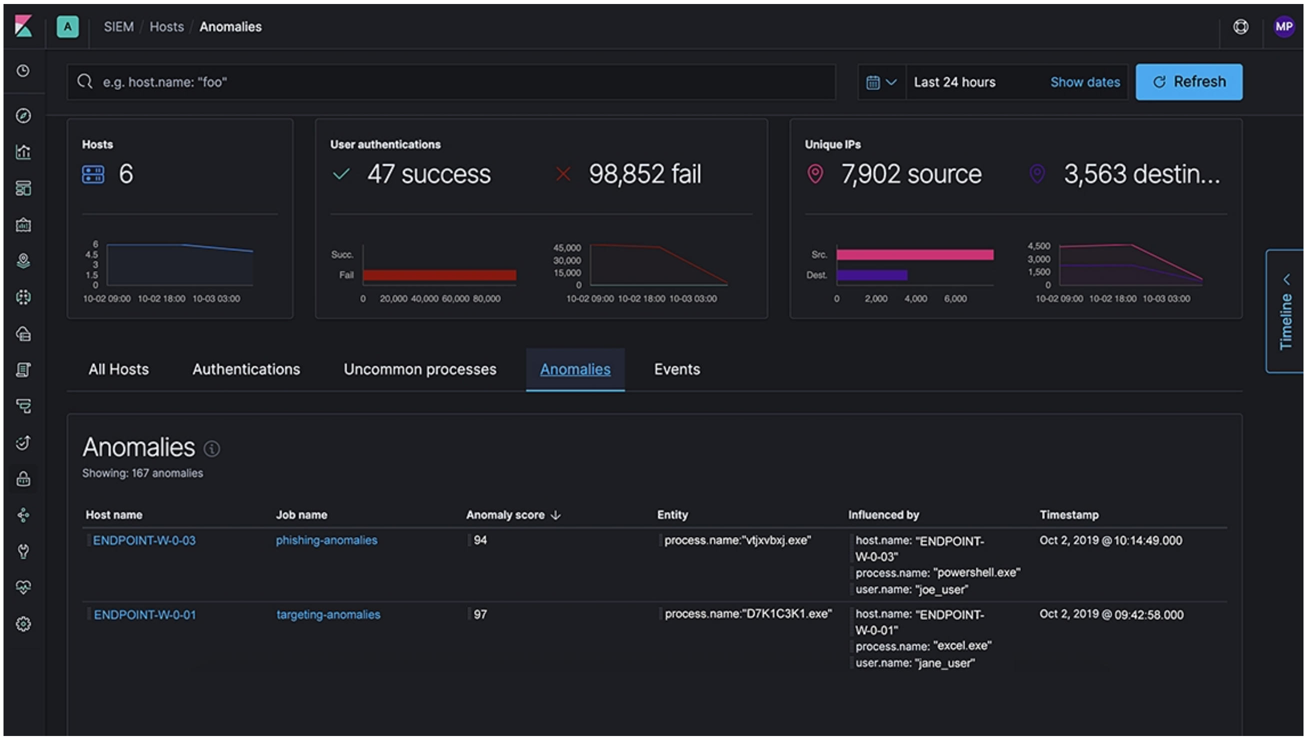
Today we are excited to announce the introduction of Elastic Endpoint Security, based on Elastic's acquisition of Endgame, a pioneer and industry-recognized leader in endpoint threat prevention, detection, and response based on the MITRE ATT&CK™ matrix. Elastic is combining SIEM and endpoint security into a single solution to enable organizations to automatically and flexibly respond to threats in real time, whether in the cloud, on-premises, or in hybrid environments. Also announced today, Elastic is eliminating per-endpoint pricing.

"Two key trends in endpoint security — the importance of a strong analytics back-end and the rise of the MITRE ATT&CK framework as a lingua franca — help make the case for greater emphasis on threat hunting and incident response use cases," said Fernando Montenegro, Principal Analyst at 451 Research. "Elastic's acquisition of Endgame fits well within these trends, and the combination of SIEM and endpoint security should enable organizations to pursue efficiencies around those use cases."

Endgame has been validated by numerous independent testing organizations, including NSS Labs, SE Labs, MITRE, and others as having both the strongest preventions and detections available. This was recently illustrated by its performance in the AV Comparatives Independent Anti-Virus Test, where Endgame demonstrated exceptional protection against real-world threats, preventing 99.7% of malware with no cloud connectivity required.

Additionally, Elastic Endpoint Security brings one of the strongest sources of endpoint security data, raw endpoint event data, and alerts to the Elastic Stack, joining the existing logging, security, APM, and infrastructure event collection. With the average threat dwell time exceeding 100 days, shipping, scaling, and storing data efficiently in Elasticsearch makes searching through all of this disparate security-related data practical, easy, and fast. Accordingly, endpoint security is a natural fit for the Elastic Stack to provide prevention against threats and the fastest detection and response to stop attacks at the earliest stages possible.

“Users deserve more from the tools they deploy. That’s why we are providing immediate value today through the simplicity of a single stack to search, store, analyze, and secure your data,” said Shay Banon, founder and chief executive officer of Elastic. “This is an exciting step toward realizing our vision for applying search to multiple use cases, as we are now able to offer users the best threat hunting solution with the best endpoint protection.”



Anomalies

Showing: 167 anomalies

Host name	Job name	Anomaly score ↓	Entity	Influenced by	Timestamp
ENDPOINT-W-0-03	phishing-anomalies	94	process.name:"vtjxvbxj.exe"	host.name: "ENDPOINT-W-0-03" process.name: "powershell.exe" user.name: "joe_user"	Oct 2, 2019 @ 10:14:49.000
ENDPOINT-W-0-01	targeting-anomalies	97	process.name:"D7K1C3K1.exe"	host.name: "ENDPOINT-W-0-01" process.name: "excel.exe" user.name: "jane_user"	Oct 2, 2019 @ 09:42:58.000

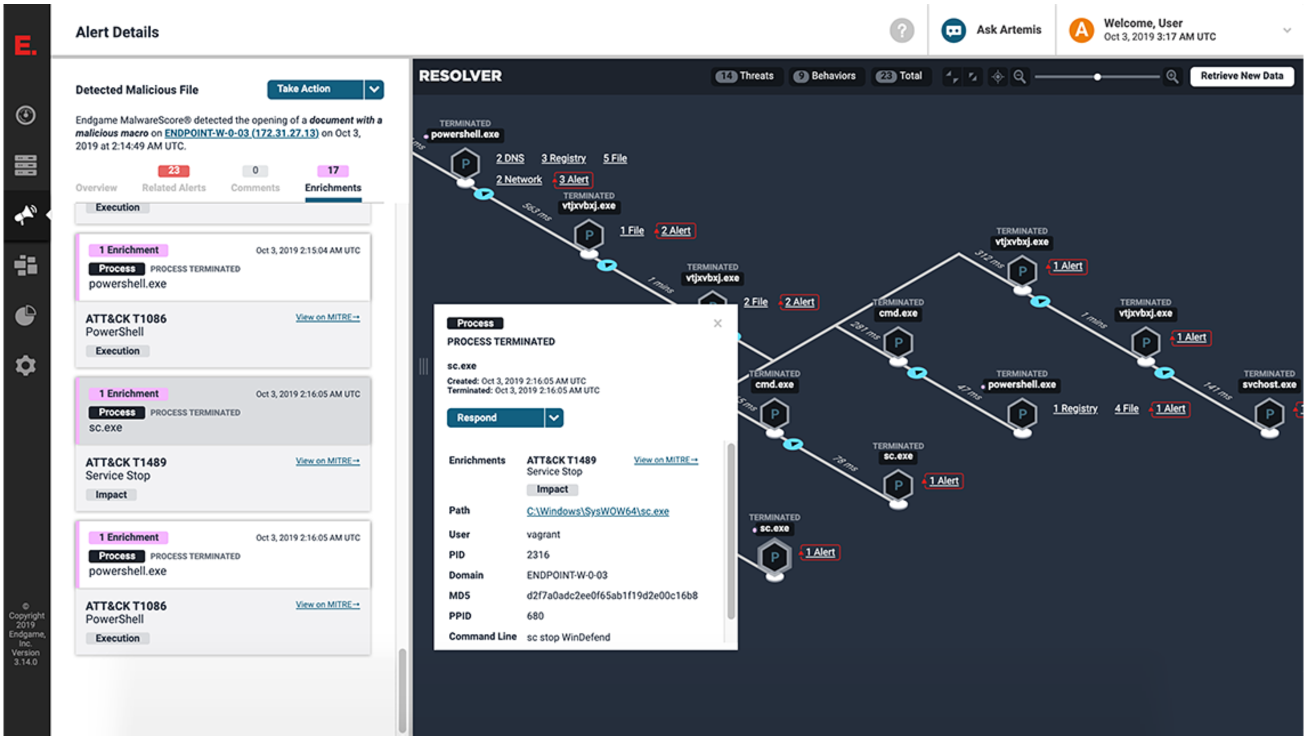
Our journey into SIEM and endpoint security

Tools working in isolation can’t safeguard an organization, and the data that those tools collect isn’t actionable without a centralized management console. Security teams are faced with siloed data, slow query times, and compromised analysis that lacks relevance and context. Organizations already know they need to work in real time; they need to ingest and store all types of data in a way that is unbounded; and they need to produce relevant results and automatically operationalize them into existing and new security workflows.

Nearly two years ago, we embarked on a mission to help organizations evolve their security efforts. While the Elastic Stack has been adopted and is used as a security solution for use cases like threat hunting, fraud detection, and security monitoring, we wanted to make it even easier for users to deploy our products for security. We first worked in collaboration with our community to develop the Elastic Common Schema (ECS) to provide an easy way to normalize data from disparate sources from network and host data. Then we launched Elastic SIEM, the world’s first free and open SIEM... but we didn’t stop there.

Now, when you deploy a data collection agent for Elastic SIEM, you can protect the endpoint simultaneously and remove the inefficiency of multiple solutions that can’t respond in time to prevent damage and loss.

“Stopping attacks as early as possible is the goal. That requires the best preventions and the highest fidelity detections on the endpoint. The combination of Endgame’s leading endpoint protection technology with Elastic SIEM creates an interactive workspace for SecOps and threat hunting teams to stop attacks and protect their organizations,” said Nate Fick, formerly CEO of Endgame and now general manager of Elastic Security.



Detected Malicious File

Endgame MalwareScore® detected the opening of a *document with a malicious macro* on ENDPOINT-W-0-03 (172.31.27.13) on Oct 3, 2019 at 2:14:49 AM UTC.

23 Related Alerts · 0 Comments · 17 Enrichments

Execution

1 Enrichment — Oct 3, 2019 2:15:04 AM UTC
Process PROCESS TERMINATED
powershell.exe
ATT&CK T1086 PowerShell — View on MITRE→
Execution

1 Enrichment — Oct 3, 2019 2:16:05 AM UTC
Process PROCESS TERMINATED
sc.exe
ATT&CK T1489 Service Stop — View on MITRE→
Impact

1 Enrichment — Oct 3, 2019 2:16:05 AM UTC
Process PROCESS TERMINATED
powershell.exe
ATT&CK T1086 PowerShell — View on MITRE→
Execution

Process
PROCESS TERMINATED
sc.exe
Created: Oct 3, 2019 2:16:05 AM UTC
Terminated: Oct 3, 2019 2:16:05 AM UTC

Enrichments	ATT&CK T1489 Service Stop View on MITRE→ Impact
Path	C:\Windows\SysWOW64\sc.exe
User	vagrant
PID	2316
Domain	ENDPOINT-W-0-03
MD5	d2f7a0adc2ee0f65ab1f19d2e00c16b8
PPID	680
Command Line	sc stop WinDefend

The end of endpoint pricing

In addition to combining the world’s first free and open SIEM with the best endpoint protection technology, Elastic is eliminating per-endpoint pricing.

“Why should users need to count the number of devices they need to protect? Or choose how many days of threat intelligence data they can afford to retain?” added Banon. “We want organizations to have the best protection, use it everywhere, and not be penalized with per-endpoint pricing.”

Elastic customers pay for resource capacity for any solution they use — Elastic Logs, APM, SIEM, App Search, Site Search, Enterprise Search, and now Endpoint Security — with a consistent and transparent pricing framework. This ensures organizations can capture maximum value from their data. With Elastic Endpoint Security, customers get full protection for as many endpoints as they need, and full data collection and shipping without having to compromise.

Security leaders comment on Elastic Endpoint Security

Texas A&M University, Andrew Stokes, Assistant Director and Information Security Officer

“We value speed of response and the ability to learn from and analyze our historical data. Elastic Endpoint Security has dramatically dropped our mean time to remediate from seven days to 30 minutes over legacy antivirus, and the Elastic Stack has provided an unparalleled way to store, analyze, and react to data well beyond any competitor in the market. Combining Elastic Endpoint Security and the Elastic Stack into a single, intelligence-led platform will further simplify and automate our security operations.”

Optiv, Anthony Diaz, Divisional Vice President, Emerging Services

"Elastic is bringing together the integration of a next-generation SIEM, robust visualization engine and a best-in-class endpoint product all backed by the world's leading search technology. This combination provides a foundation for enterprises to combat the growing complexity of cyber threats. Elastic's vision for bringing together these components in an open ecosystem is a revolutionary, yet practical idea that helps organizations of all sizes maximize all of their data to manage their cyber security needs."

Infotrack, Sebastian Mill, Chief Technology Officer, Global Development

“At InfoTrack, we’ve come to realize just how valuable endpoint data can be for gaining visibility into our operations and making sure our infrastructure remains secure. Toward these goals, our innovation team has already been scoping Auditbeat into our environments, but introducing Elastic Endpoint Security takes it to a whole new level. We are intrigued by the ability to stop threats with Elastic Endpoint Security while pairing security event data with some Elastic machine learning-powered anomaly detection. It will be a killer setup."

SANS Institute, John Pescatore, Director, Emerging Security Trends

“When SANS surveyed SOC managers about the tools they wish new SOC hires were skilled in the Elastic (ELK) Stack was one of the top ones mentioned. The components of the ELK stack are used both by SOC analysts and application developers. Having strong EDR capability integrated into the endpoint side of the standard packages deployed by DevOps and CI/CD pipelines can be a real game changer in visibility, detection and prevention of cyber attacks.”

Resources

If you want to see Elastic Endpoint Security in action and hear more about our developments, please join us at one of our Elastic{ON} Tour stops in the US, EMEA, or Asia Pacific.