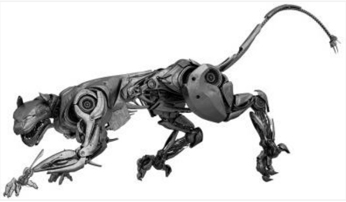
RSA ECAT

Innovative Endpoint Threat Detection



Expose More

Analyze Faster

Respond Better

AT A GLANCE

RSA ECAT helps security teams:

- Expose advanced threats that would otherwise be hidden.
- Analyze suspicious endpoint activity and confirm infections quickly.
- Determine the full scope of a compromise instantly.

KEY BENEFITS

- Reduce the time to detect and validate compromised machines
- Reduce incident investigation time with instant actionable intelligence
- Reduce attacker dwell time
- Reduce the risk of sensitive data exfiltration
- Increase visibility of endpoint activity across the enterprise to quickly gauge the magnitude of an intrusion

FIND MALWARE HIDING ON ENDPOINTS

Security teams constantly need to evolve their tactics to stay in front of attackers and the latest threats. Recently this has become much more difficult. Attackers continue to advance and use sophisticated techniques to infiltrate organizations, but they have also become more targeted in their approach. They spend significant resources performing reconnaissance to learn about organizations and to develop malware specifically to bypass traditional security technologies.

Many organizations still rely primarily on preventive, signature-based tools to try to keep these threats out, but they are no longer effective. Without the ability to quickly detect compromises, confirm infections, and take action, organizations are constantly behind the attacker, and the risk of data loss and negative business impact increases significantly.

And that's why organizations are turning to RSA ECAT. With RSA ECAT, security teams can:

- Expose advanced threats that would otherwise be hidden.
- Analyze suspicious endpoint activity and confirm infections quickly.
- Determine the full scope of a compromise instantly and take action to limit negative impact to the business.

With RSA ECAT, security teams are able to expose advanced threats faster through deep endpoint visibility and anomaly detection, quickly triage and analyze suspicious activity to confirm infections, collect the necessary information to take action to stop the threat and limit the negative impact to the business.

EXPOSE ADVANCED THREATS THROUGH SIGNATURE-LESS DETECTION

To detect and respond quickly to malware and other threats on endpoints, both servers and user systems, security analysts first need full visibility into what is happening on the endpoint. RSA ECAT gains deep visibility into the endpoint in the following ways:

- **Monitor & alert in real-time:** RSA ECAT continuously monitors endpoint activity and can alert on suspicious activity in real time, providing an early warning about potential compromises.
- **Gain an x-ray view through unique scan techniques:** RSA ECAT leverages unique scan techniques to delve deep into the inner workings of the endpoint to expose anomalies. Through per-process live memory analysis, direct physical disk inspection, and network traffic analysis, RSA ECAT identifies suspicious activity and flags it for further review. Unknown files are automatically downloaded to a central location for further analysis.
- **Collect a full inventory & profile of the endpoint in a matter of minutes with no impact to end users:** RSA ECAT collects a full inventory of everything running on the endpoint and provides the information needed to analyze and confirm infections. Endpoint scans complete 5-10 minutes, which means analysts receive the data they need quickly, making them more productive, and better able to thwart an attack in its early stages. All storage of data and the bulk of analysis are done on the server-side, which keeps the footprint of the ECAT agent small and reduces the impact to end users.
- **Automatically scan when unknown files load**: With the amount of new malware created daily and the advanced, targeted nature of many attacks, it is critical to have visibility into any new files that load across the environment in order to detect these types of attacks faster. RSA ECAT will automatically kick off a scan of a system whenever a new, unknown file loads on any endpoint. This gives fast insight into how the file behaves and impacts the system, which helps analysts quickly determine if it's malicious and take action.

WITH RSA ECAT:

Security teams are able to expose advanced threats faster through deep endpoint visibility, quickly triage and analyze suspicious activity to confirm infections, and have the necessary information to take action and limit negative impact to the business.

QUICKLY ANALYZE & CONFIRM INFECTIONS

In a typical enterprise, there are often far more issues than the security team can handle. It's imperative that the team has an effective way to identify and triage issues quickly. RSA ECAT provides security team with advanced analysis capabilities to prioritize and speed up the identification and investigation of issues. RSA ECAT has the ability to:

- **Automatically flag suspicious endpoint activity for further investigation:** By having a suspect level calculated for each file found on the endpoint and a cumulative risk score for each endpoint, RSA ECAT provides a clear visual indication of the potential threat level of endpoints and a description of the anomalous activity seen. With this crucial information right at their fingertips, security analysts can more easily triage alerts, focus their investigations and make better use of their limited resources.
- **Baseline your environment and maintain a global repository of all files found:** RSA ECAT maintains a global repository of all executable files found and IP addresses connected to across the environment. With RSA ECAT, security analysts have the flexibility to whitelist known-good (trusted) files and filter them from view during an investigation, and also blacklist known-bad files and IPs, so they will be automatically flagged if found on any endpoints. This helps to reduce the time taken for an investigation, and gives security teams the context about how many machines on which a particular file has been found, whether the file is active or dormant on a machine, and which machines have connected to a particular IP address.
- **Perform various checks of file legitimacy:** RSA ECAT performs checks to help security analysts determine if a file is malicious, including the ability to check the legitimacy of file certificates and hashes, check for known threats by incorporating YARA rules and leveraging multiple AV engines through OPSWAT Metascan, identify any code modifications made by malware, and more. RSA ECAT can also automatically pull back copies of executable files from the endpoint for additional analysis. This helps to simplify and reduce the cost of investigations.
- **Provide comprehensive visibility across endpoints, networks, & logs:** Direct integration between RSA ECAT and RSA Security Analytics provides comprehensive visibility into endpoint activity, network packets, NetFlow and logs. This enables your analysts to pivot between endpoint and network views during investigations.

SCOPE & EFFICIENTLY RESPOND TO INCIDENTS

Once an infection has been confirmed, security teams need to take targeted actions to respond. One critical aspect of effective remediation is the ability to know how far a particular infection has spread. For example, if one machine is found to be infected, what other machines across the environment are also infected? Without that visibility, organizations are left not knowing if other machines are also infected and thus the organization could still be at risk. With RSA ECAT, security teams are able to:

- **Determine the scope of compromise instantly:** RSA ECAT identifies all other endpoints that were infected, enabling security teams to instantly know how far the malware spread. By right-clicking on a malicious file, RSA ECAT will show all other machines with the same file, and security teams will know all other machines that need to be remediated.
- **Gather critical forensic data:** RSA ECAT quickly gathers critical data needed for a forensic investigation. Gathering similar forensic data with other solutions can be very resource intensive on the machines as well as time consuming to run. With RSA ECAT, analysts can easily pull full process and memory dumps, view the Master File Table (MFT), and see all modified/deleted files.
- **Remediate with precision:** RSA ECAT identifies the exact location of malicious files for precise remediation. By identifying the exact location and persistence mechanism of malicious files, security analysts can take appropriate action depending on the type of threat. RSA ECAT also has direct integration with a temporary remediation agent, which can be deployed from the ECAT console to clean known threats.

Attackers will continue to use sophisticated tactics to evade traditional perimeter and signature-based defenses, and will target organizations of all sizes, across all industries. To better defend against the constant threat of malware and reduce the risk of data loss, organizations need to increase visibility of endpoints, confirm infections faster, and take action to limit impact to the business.

ABOUT RSA

RSA's Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. Through visibility, analysis, and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud and cybercrime.

With over 30 years of industry expertise, RSA believes that our portfolio of products, services, and intelligence is better able to address today's security challenges than any other company in the industry.