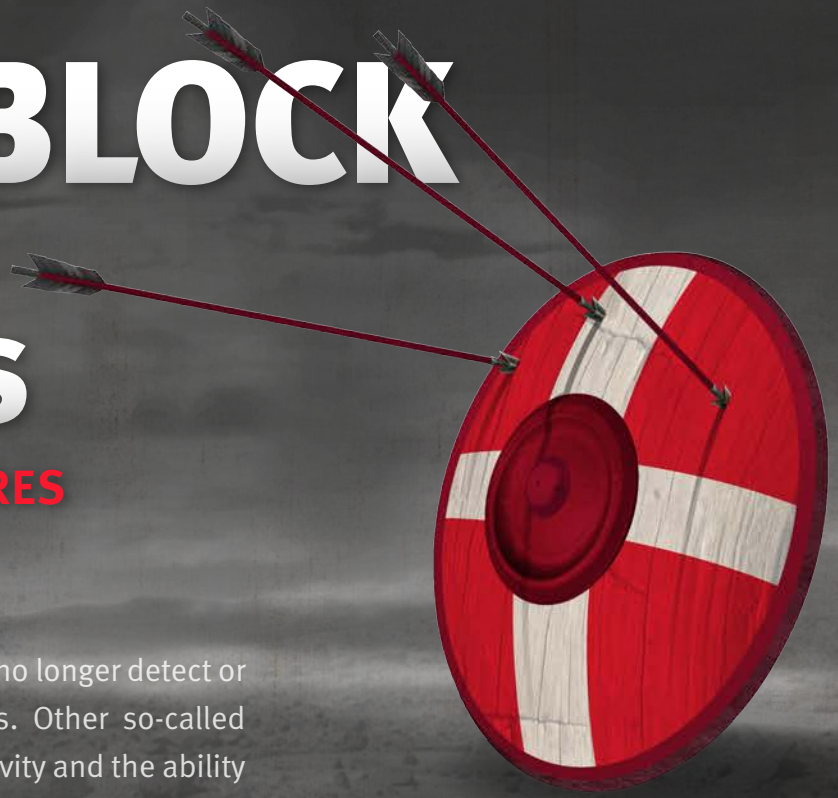

RULE YOUR
ENDPOINTS
MAXIMIZE YOUR ENDPOINT SECURITY STRATEGY
WITH THE RIGHT TECHNOLOGY
RSA

DETECT AND BLOCK ADVANCED ENDPOINT THREATS

IN REAL-TIME WITHOUT RELYING ON SIGNATURES



Traditional signature-based, preventive controls, such as antivirus, no longer detect or stop targeted malware and other sophisticated endpoint attacks. Other so-called "next generation" approaches lack deep visibility into endpoint activity and the ability to quickly alert when something seems unusual.

RSA ECAT detects and blocks suspicious endpoint activity missed by other tools by **comparing files found in memory to files on disk** and detecting the behavior of the malware, rather than a signature. RSA ECAT's ability to continuously monitor allows analysts to see and block endpoint threats in real time.

SIGNATURES DON'T WORK:

70-90% of malware samples are unique to an organization.

–*Verizon Data Breach Investigation Report 2015*

RSA

49% of enterprise organizations have experienced a successful malware-based attack over the past two years.

–Enterprise Strategy Group (ESG) Research

SEE BEYOND THE ENDPOINT WITH COMPREHENSIVE VISIBILITY

FROM THE ENDPOINT TO THE CLOUD

Alerts coming from many different sources make it difficult for security teams to prioritize investigations because siloed views of network and endpoint activity don't provide a complete picture of what's happening across the environment.

RSA ECAT shatters these security silos by providing comprehensive network and endpoint visibility when combined with RSA Security Analytics. This powerful integration **correlates endpoint data with network packet and log data**, and prioritizes investigations into one combined view for faster threat detection.

RSA

We can quickly identify other compromised systems and triaging can be done in seconds. RSA Security Analytics and RSA ECAT are two tools that our CIRC analysts cannot live without.

–James Lugabihl, Manager, EMC Critical Incident Response Center

DETERMINE THE FULL SCOPE OF A COMPROMISE

AND TAKE FAST ACTION

One of the biggest challenges after confirming a compromise is to identify other infected hosts. Security teams cannot determine the full scope of compromise without the ability to know where malware has spread.

RSA ECAT can instantly determine if a file has been seen before and learn how it behaves with automatic scans and a complete behavior tracking system. By collecting a full inventory and profile of the system, the root cause of infections can be confirmed in a matter of minutes.

RSA

RSA ECAT has helped narrow down a 12-hour analysis to 10 or 15 minutes.

–Garrett Schubert, Director, EMC Critical Incident Response Center

GET THE MOST OUT OF YOUR TEAM

By leveraging machine baselining and whitelisting to immediately remove "known-good" processes, RSA ECAT focuses security teams on suspect processes and machines. When a new, unknown files loads on the system, scans are complete in a matter of minutes, which means analysts receive all of the data they need quickly. RSA ECAT also provides **intelligent, risk-level scores based on dynamic data trained though machine learning**, highlighting anomalous activity for quick triage on the most suspicious endpoints. When combined with its built-in forensic capabilities, RSA ECAT can help reduce incident response time per host from hours to a few minutes.

RSA