

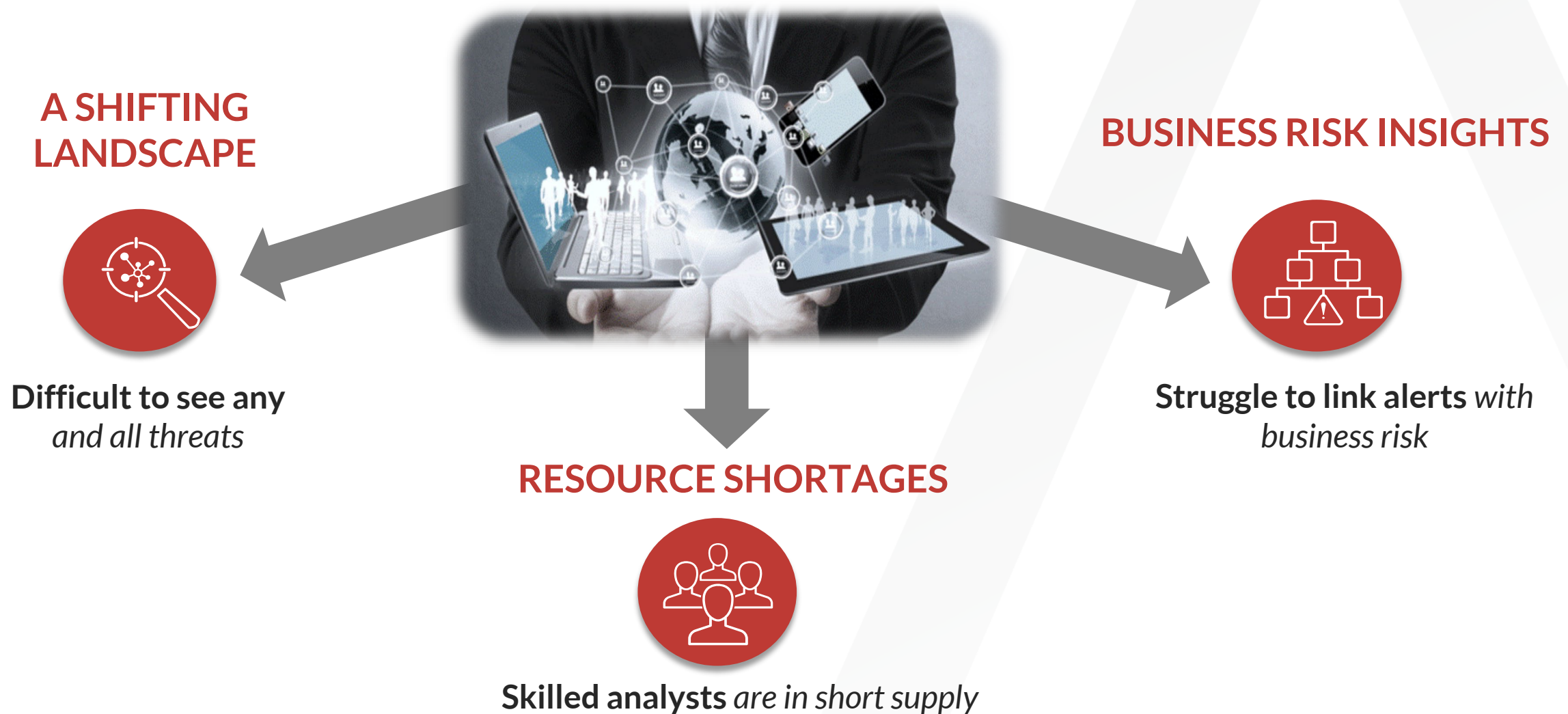


BEYOND THE SIEM RSA NETWITNESS®

*Accelerated Threat Detection & Automated Response,
from the Endpoint to the Cloud*

Bernard Montel : Regional PreSales Manager

SECURITY OPERATIONS CHALLENGES



RSA'S EVOLVED SIEM WORKS WITH YOU TO SOLVE THOSE CHALLENGES



Visibility and Early Detection

Transform raw data into actionable insights

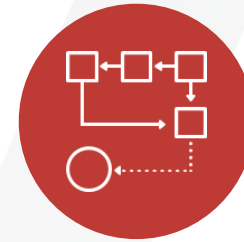
Analyze Big Data sets with business context to identify potential threats



Quickly Investigate and Assess

Validate Incidents and realize true impact and scope risks

Behavioral & Machine Learning Analytics for comprehensive detection and forensics



Effective Threat Remediation

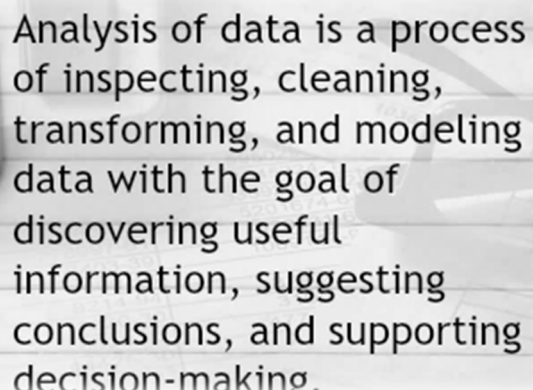
Act and Mitigate before threats become breaches

Integrated Platform enables optimized response

“RSA’s Evolved SIEM helped us **reduce our response times** dramatically and realize the scope of a threat, delivering a comprehensive view into our network risks and threats.”

MANAGER OF SECURITY OPERATIONS GROUP, Global Software Vendor

Investigate & Assess *with Advanced Analytics*



Analysis of data is a process of inspecting, cleaning, transforming, and modeling data with the goal of discovering useful information, suggesting conclusions, and supporting decision-making.



**Fast and
Accurate
Investigations!**

“With RSA NetWitness Platform we can detect advanced malware and security incidents on the perimeter, and use the platform to register and handle them all. **It's the backbone of our security analytics center.**”

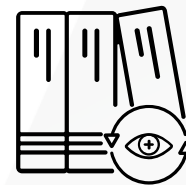
- RASMUS THEEDE, CORPORATE VP GROUP SECURITY, KMD



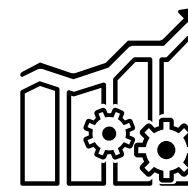
**Correlate multiple data
sources**



**User and Entity
Behavior Analytics**

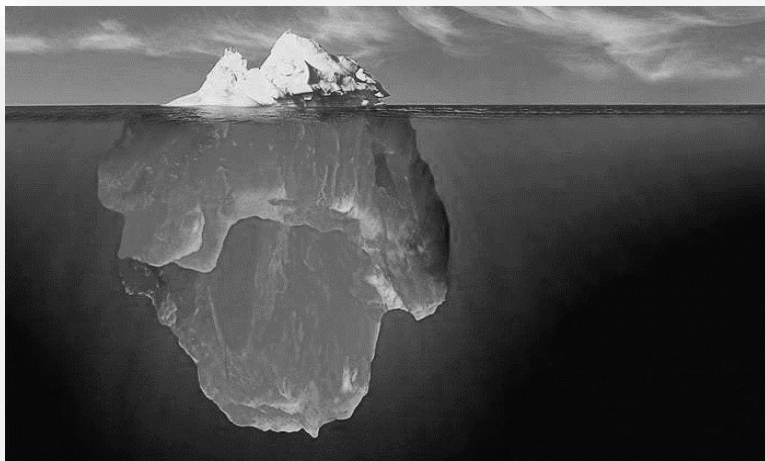


**Out-of-the-box threat
intelligence**



**Machine learning &
data science**

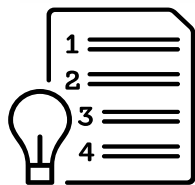
Effective Threat Remediation *to prevent threats from becoming breaches*



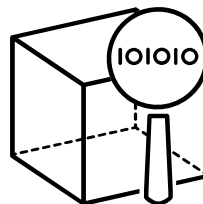
**Assess and
Remediate the
full threat!**

“RSA’s fast and comprehensive response to advanced attacks **enables us to mitigate threats before they can do any damage** to our business.”

Yumiko Matsubara, Security Architecture Manager, Recruit Technologies Co., Ltd.



Accelerate and automate incident triage



Focus on the threats that matter most



Orchestrated SOC response with business context

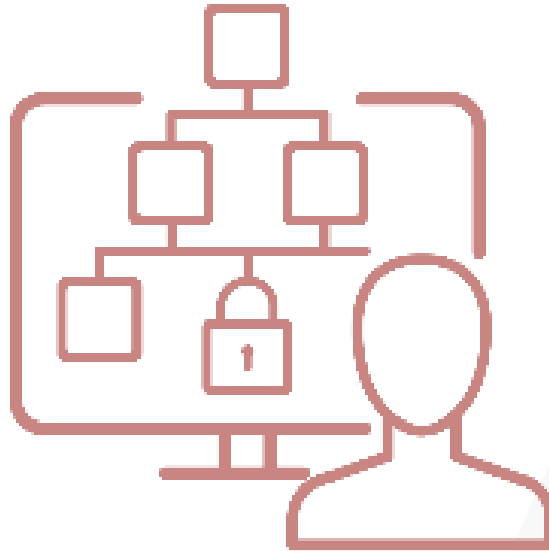
RSA'S EVOLVED SIEM



SOLUTIONS INCLUDED AT NO CHARGE TO RSA NETWITNESS PLATFORM CUSTOMERS

■ RSA NetWitness Endpoint Insights

- Lightweight endpoint agent
- Adds context to accelerate threat detection & response
- Delivers timely insights into endpoint hosts via scans
- Simplifies Microsoft Windows Logs collection



■ RSA NetWitness UEBA Essentials

- Content Pack with user-focused rule set
- Provides high confidence, high fidelity detection of user- and entity-based threats
- Correlates multiple data sources to identify anomalous or suspicious user behavior

What do Industry Analysts and our Customers say about RSA NetWitness Platform?

RSA NAMED A LEADER IN 2018 GARTNER MAGIC QUADRANT FOR SIEM

See why Gartner® recognized RSA as a leader in its latest Magic Quadrant report for SIEM providers.

“A single vendor that integrates capabilities including core SIEM, network monitoring and analysis, EDR, and UEBA”.



“RSA’s fast and comprehensive response to advanced attacks

enables us to mitigate threats before they can do any damage to our business.”

Yumiko Matsubara, Security Architecture Manager, Recruit Technologies Co., Ltd.

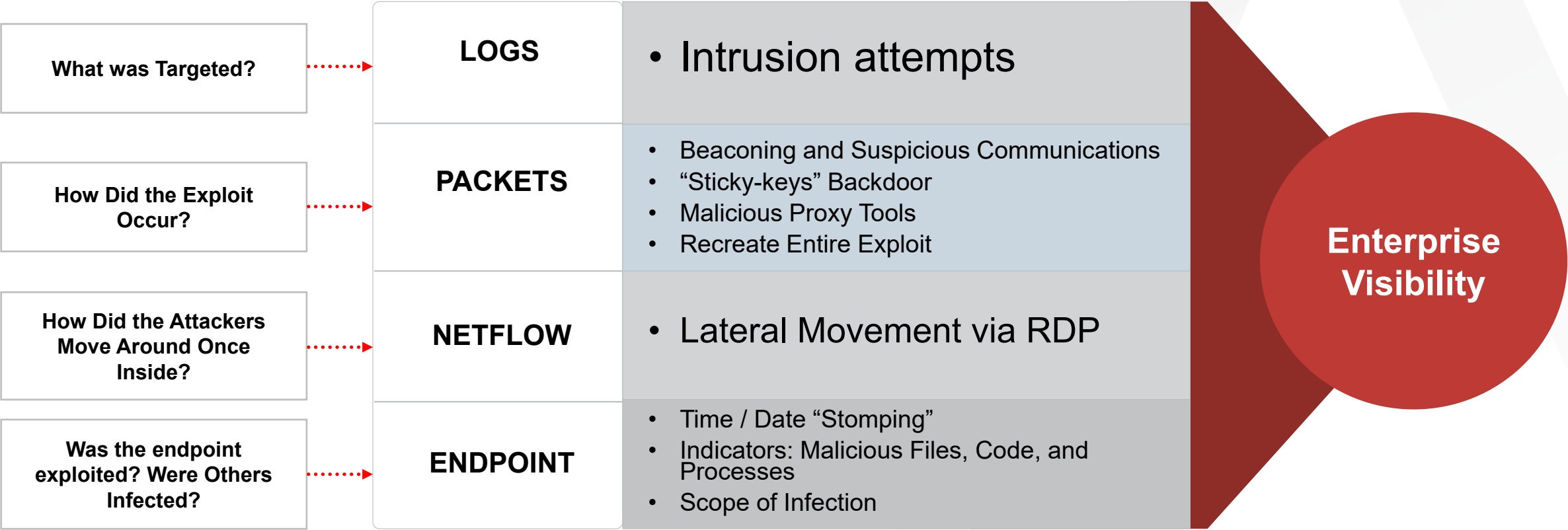
RECRUIT
Recruit Technologies Co., Ltd.

RSA NETWITNESS PLATFORM CONCEPTS

META DATA

CORE COMPONENTS

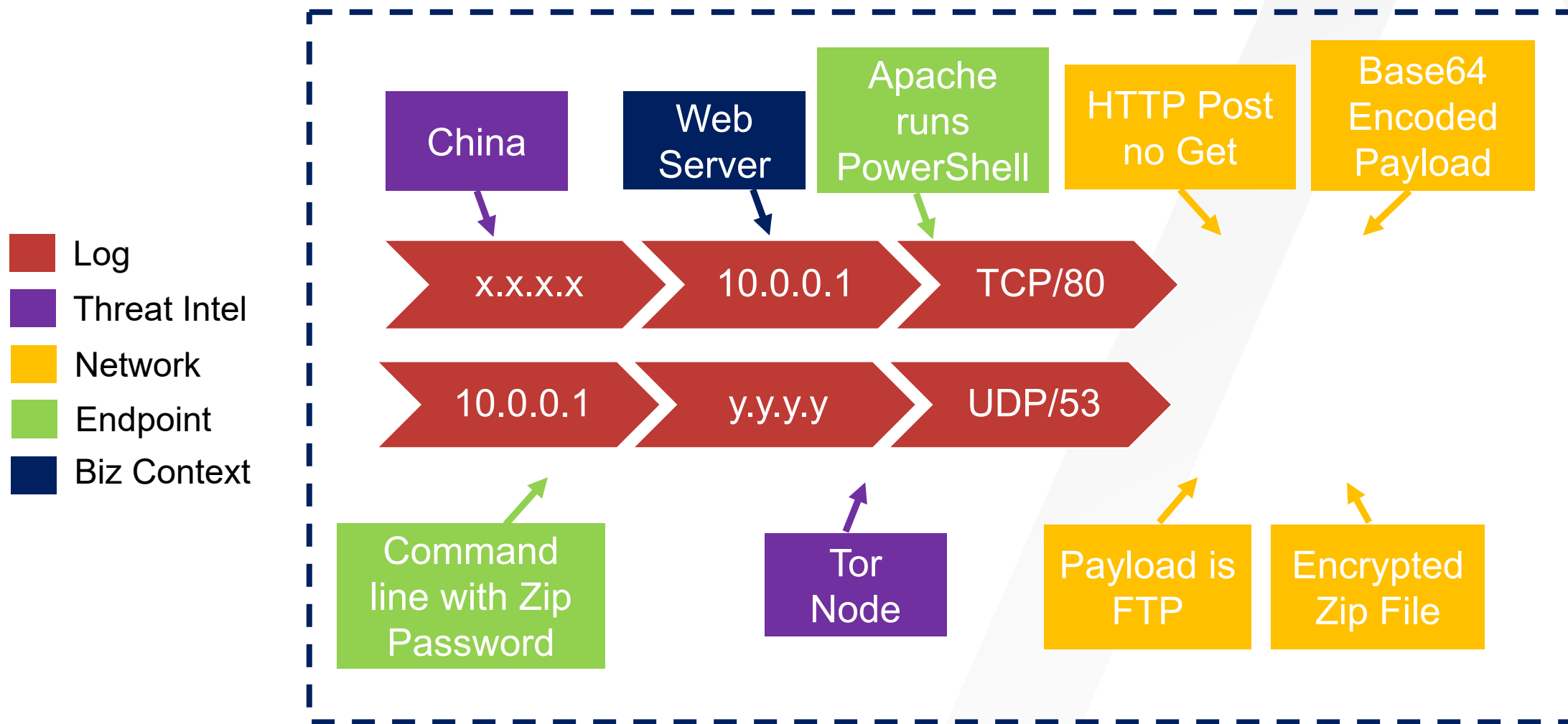
Full Visibility and Context



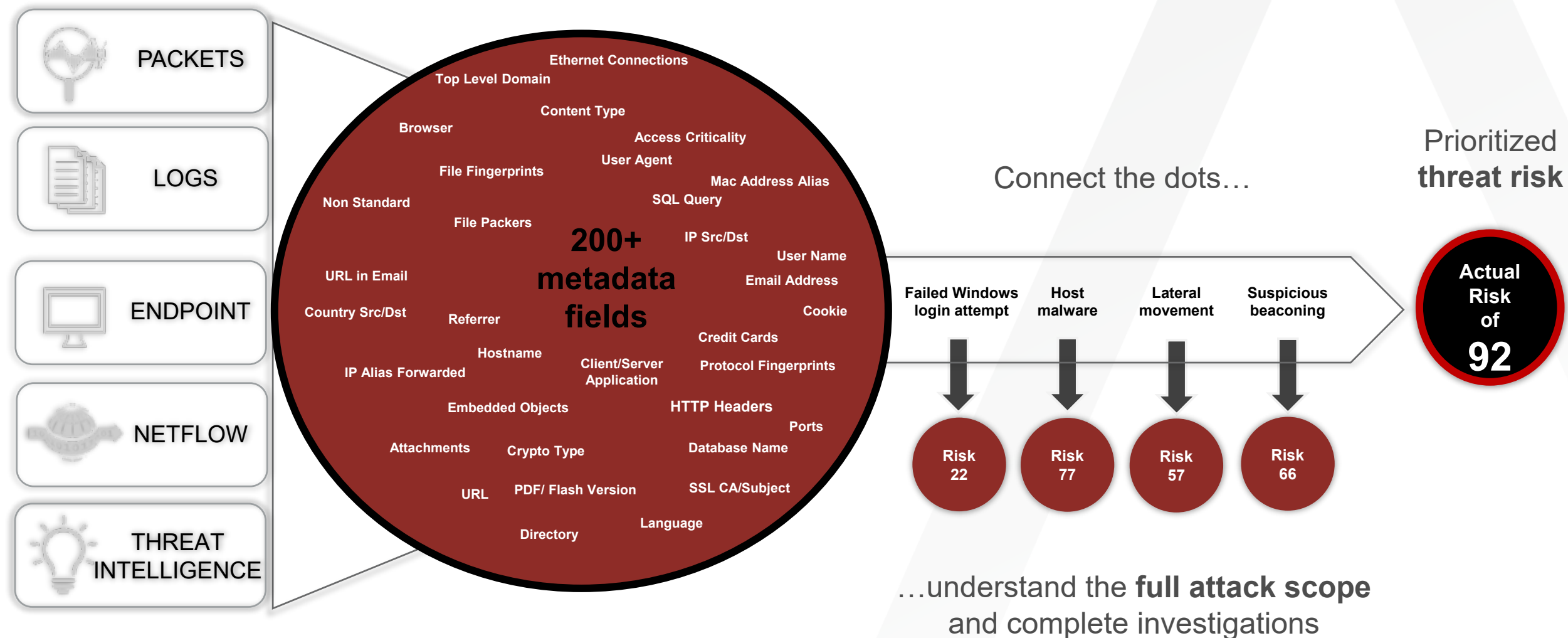
RSA NetWitness Suite Consumes and Normalizes ALL Available Threat Data
to Deliver Faster, More Accurate Risk Analysis.

METADATA

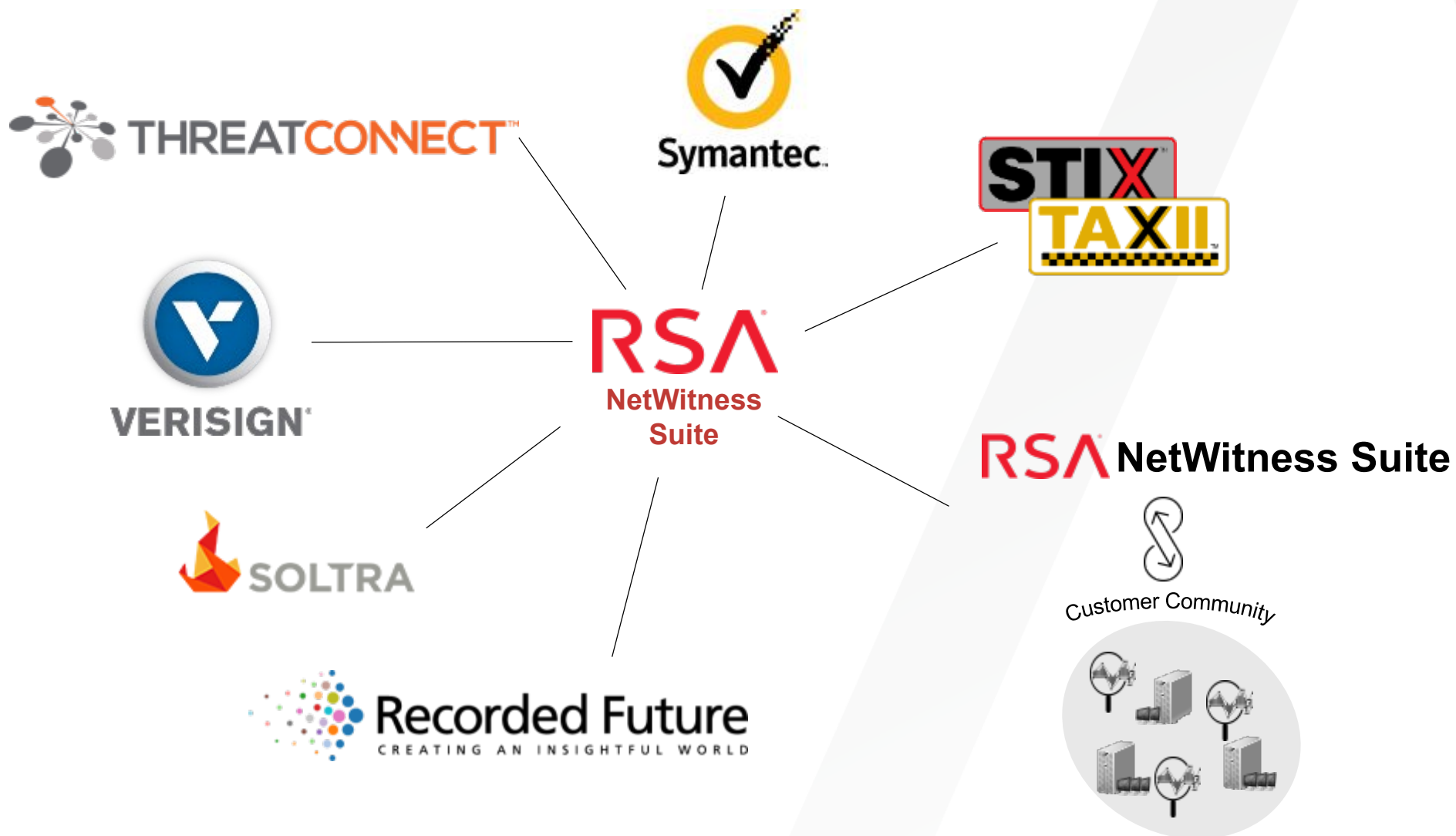
IT'S THE STORY BEHIND THE DATA



RSA'S UNIQUE APPROACH TO DETECTING THREATS



LEVERAGE MULTIPLE THREAT INTEL SOURCES

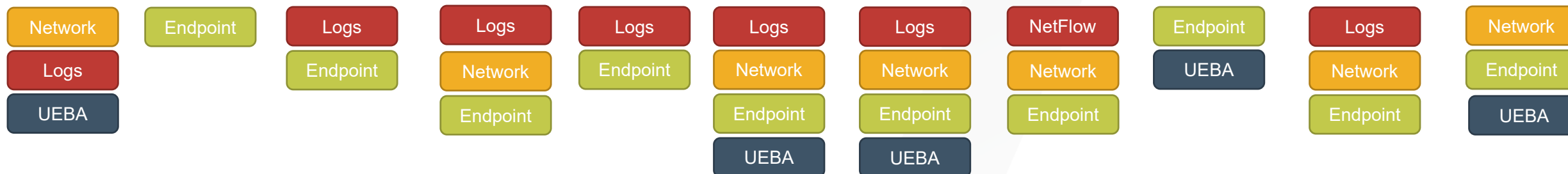


MITRE ATT&CK FRAMEWORK

RSA NETWITNESS PLATFORM MAPPING

Attack stages detecting according [MITRE ATT&CK framework](#) using RSA NetWitness components

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Spearphishing Attachment	Command Line Interface	Create Account	Process Injection	Rundll32	Brute Force	Account Discovery	Remote Desktop Protocol	Data Staged	Data Encrypted	Data Encoding
Drive-by Compromise	PowerShell	New Service	New Service	File Deletion	Credential Dumping	Network Service Discovery	Remote File Copy	Data from Local System	Data Transfer Size Limits	Remote File Copy
Valid Accounts	Scheduled Tasks	Registry Run Keys	Web Shell	Timestamp	Account Manipulation	System Service Discovery	SSH Hijacking	Data from Removable Media	Exfiltration over Command and Control Channel	Custom Cryptographic Protocol



RSA'S EVOLVED SIEM



- **A Single, Unified Platform** for All Your Data
- **Integrated** Threat and Business Context
- **Automated** User Behavior Analytics
- **Smart and Fast** Investigations
- **Orchestrated** Actions
- **Flexible, Scalable** Architecture
- **End-to-End** Security Operations

The background is a vibrant red with a complex pattern of small, dark red dots arranged in a grid. Overlaid on this grid are numerous thin, dark red lines that radiate from the center towards the edges, creating a sense of depth and movement. The overall effect is a dynamic, high-tech aesthetic.

RSA[®]