RSA

THREAT-AWARE AUTHENTICATION

DRIVE INTELLIGENT ACCESS DECISIONS AND RICH RESPONSE ACTIONS ENRICHED WITH DENTITY INSIGHTS AND THREAT CONTEXT TO REDUCE DIGITAL RISK

In an era of ever-expanding attack surfaces, protecting against threat actors has become an increasingly complex activity. The variety of attack types, from commodity malware, insider threats and crimeware to state-sponsored exploits, hacktivists and terrorists, makes things even more complicated. Acting quickly and efficiently with consistency and precision, once a compromise has been identified, is key for security teams to scale and rapidly weed out false positives and provide focused indicators as opposed to open-ended siloed alerts.

- **81%** of the investigated breaches to organizations' infrastructure, sensitive data or applications originated **using compromised credentials.**
- Time-to-compromise continues to be measured in minutes, while **time-to-discovery remains in weeks or months.**
- Two-thirds (68%) of reported breaches went undiscovered for months or more.

Verizon Data Breach Investigations Reports 2017, 2018, Verizon

In reality, the average Mean Time To Detect, Investigate and Respond (MTTD/I/R) is far from being ideal for a majority of organizations, and this is where RSA NetWitness® Platform and RSA SecurID® Access join forces to deliver better risk incident response and more informed authentication decisions to manage digital risk.

The RSA NetWitness Platform enables security operations teams to detect abnormal user and machine activities inside or outside of the corporate premises, as well as network anomalies, and can share this information with RSA SecurID Access to enrich authentication policy decisions with threat intelligence, providing stronger, continuous authentication.

WHAT HAPPENS WHEN THE ATTACKER IS ALREADY IN?

INTEGRATION BENEFITS

- Visibility and insight into user activity across your environment
- Instead of blocking all users upon detection of suspicious activity, allow access for legitimate users by elevating trust with multi-factor authentication
- Take immediate action by disconnecting VPN session and requiring additional authentication
- Mitigate the risk of insider threat and data breach

With an increasingly modern, global and remote workforce, managing and monitoring user access across your hybrid IT environment is a critical security concern. For many organizations, the perimeter has shifted from the hosts at the corporate premises to identities that need access from anywhere, to any application, across all devices, at any time. Therefore, evolved means are needed for detection, investigation and response to threats.

In addition, what if the attacker was already able to access the organization's assets (using compromised credentials, for example)? How can a response action be performed? And how can we automate response without needing the security analyst to be present at that time, with an automated workflow?

In order to accomplish this, security operations tools and workflows need to be able to:

- **Automatically detect** abnormal users' behaviors
- Have **visibility** to all actions performed by the user—before, during and after abnormal behavior was identified
- **Investigate** the entire attack lifecycle and understand how widespread the compromise is
- Leverage strong, risk-based, multi-factor **authentication** for an immediate response action, driving trust elevation without the need to block legitimate user activity

RSA

AUTOMATIC BEHAVIOR-BASED DETECTION & RESPONSE

Collection and monitoring of authentication and activity logs is already available today by feeding information from RSA SecurID Access into RSA NetWitness Platform for advanced correlation and user access context. In order to react to threats in real time and to enable greater visibility, RSA expands the integration and takes an innovative approach by detecting anomalous activity with RSA NetWitness Platform, leveraging advanced machine learning, and then feeding actionable insights into RSA SecurID Access. RSA SecurID Access leverages this threat intelligence, along with business context and identity insights, in real time in order to trigger additional authentication when the risk is high. This empowers security teams with continuous authentication as an automated out-of-the-box workflow to reduce the number of alerts that might block genuine user activity and to elevate critical alerts with higher probability of being malicious.

The intersection of threat intelligence and identity insights enables informed authentication decisions that drive trust elevation and provide an alternative to blocking all access when suspicious activity is detected.

VISIBILITY

Visibility to network traffic, user activities and endpoint behaviors enables the RSA NetWitness Platform to detect threats across all terrains. RSA NetWitness integrates with hundreds of data sources to better understand the full scope of an attack.

Adding that information to the identity insights collected by RSA SecurID Access extends visibility beyond the scope of identity, supporting contiguous assessment of risk.

DETECTION

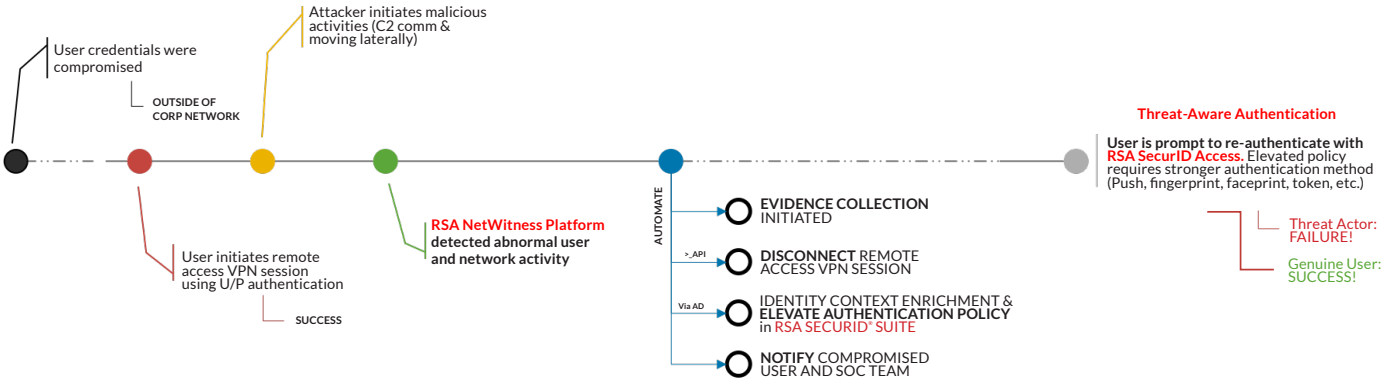
Whether a host on the network was infected, user credentials were compromised or data was exfiltrated, RSA NetWitness Platform automates threat detection, leveraging static indicators of compromise, advanced correlation, machine learning and behavior analytics, capable of pinpointing the threat and triggering an incident and workflow in RSA NetWitness Orchestrator.

ENFORCEMENT

When RSA SecurID Access is informed of high-risk activity, whether the user was in an active session that was disconnected or is about to log into an application, it will take the threat intelligence into account in the policy assessment to determine the action. For example, if the information indicates that the risk is high, this will impact the current identity assurance, which is the confidence that the user is who they claim to be. Additional authentication will be triggered. When users need to authenticate, they can use a broad variety of modern, mobile optimized authentication options such as push to approve, biometric authentication (fingerprint and face), one-time passcodes (OTPs) and SMS, as well as software and hardware tokens, leveraging strong authentication to power identity assurance. If RSA NetWitness determines that the suspicious activity is persistent and more sophisticated remediation is required, the RSA SecurID Access policy will block the user from accessing the application.

FROM ATTACK TO RESPONSE

Outside of the corporate network, users have greater chances of getting their machines infected or their information stolen either at their home network or at a public Wi-Fi. Once compromised, the attacker can gain access, move laterally and perform actions from an alleged trusted user and device. Therefore, beyond perimeter defense controls, the need to identify user, host and network anomalies is critical for detection. Upon detection of a possible attack, there is no time to spend on evidence collection, true positive validation or obtaining relevant data for investigation. An automated, scalable, consistent validation and enforcement process is required to prevent the attacker from causing damage to the organization—all without being dependent on SOC resources or a security analyst to be available in real time to take action.



HANDS-OFF SOC RESPONSE PROCEDURE

Threat-Aware Authentication empowers SOC teams to automate incident-response procedures, leveraging behavioral analytics and strong, multi-factor authentication, elevating trust instead of blocking users, and reduces Mean Time to Respond with RSA NetWitness Platform and RSA SecurID Access.

ABOUT RSA NETWITNESS PLATFORM

RSA NetWitness® Platform is an evolved SIEM and threat defense solution that empowers security teams to rapidly detect, understand the full scope of a compromise and automatically respond to the threat before damage is done. With a design that aligns business context to security risks, RSA NetWitness Platform closes the gaps of technology-only solutions and ensures that IT security is optimized to support an organization's strategic goals.

ABOUT RSA SECURID® SUITE

RSA SecurID® Access is part of the RSA SecurID® Suite, which enables your organization to accelerate business while mitigating identity risk and ensuring compliance. To address today's toughest security challenges of delivering access to a dynamic and modern workforce across complex environments, the RSA SecurID Suite transforms secure access to be **convenient** to support the modern workforce, **intelligent** to prioritize action on what matters most and **pervasive** across all access use cases.

ABOUT RSA

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection, and integrated risk management, RSA customers can thrive and continuously adapt to transformational change. For more information, visit rsa.com.

02/19, Use Case, H17320 W218280.