RSA NetWitness Reports

This topic lists the RSA NetWitness Reports. The reports are built upon rules and lists. When you download a report, all necessary RSA NetWitness Rules and RSA NetWitness Lists are also downloaded. You may, however, need to download supporting RSA Application Rules and parsers.

Note: For content that has been discontinued, see **Discontinued Content**.

Display Name	File Name	Description	Medium	Tag
11.1-11.2 Endpoint Machine Summary Report	11.1-11.2 Endpoint Machine Summary Report	This report shows information for the machines configured to run the RSA NetWitness Endpoint agent including an OS and endpoint version summary. Training on RSA NetWitness Endpoint, including analysis of Scan Data, may be found on RSA Link: https://community.rsa.com/docs/DOC-84977. VERSIONS SUPPORTED * RSA NetWitness Endpoint 11.1 and higher DEPENDENCIES NetWitness Rules: * 11.1-11.2 Endpoint Operating Systems Summary * 11.1-11.2 Endpoint Version Summary	endpoint	assurance, compliance, corporate, risk, vulnerability management
11.1-11.2 Endpoint Scan Data Autorun and Scheduled Task Report	11.1-11.2 Endpoint Scan Data Autorun and Scheduled Task Report	This report looks for suspicious autoruns and tasks using a few key features. Autoruns/Scheduled Tasks mechanisms are often used by attackers to maintain persistence on a compromised host. This is not an exhaustive set of potentially suspicious autorun behavior, but should give an analyst visibility into some of the more common techniques leveraged by attackers. Training on RSA NetWitness Endpoint, including analysis of Scan Data, may be found on RSA Link: https://community.rsa.com/docs/DOC-84977 VERSIONS SUPPORTED * RSA NetWitness Endpoint 11.1 and higher DEPENDENCIES NetWitness Rules: * 11.1-11.2 Autoruns and Scheduled Tasks From or Referencing AppData * 11.1-11.2 Autoruns and Scheduled Tasks From Root of Program Data * 11.1-11.2 Autoruns and Scheduled Tasks Invoking Command Shell * 11.1-11.2 Autoruns and Scheduled Tasks Invoking Windows Script Host * 11.1-11.2 Autoruns and Scheduled Tasks Running Scripts * 11.1-11.2 Rarest Autorun Registry Keys	endpoint	attack phase, exploit, threat
11.1-11.2 Endpoint Scan Data File and Process Outliers Report	11.1-11.2 Endpoint Scan Data File and Process Outliers Report	This report focuses on rarity of particular process, file, and autorun features in the environment. While rarity in each of these results does not automatically imply malicious activity, it is important to analyze and justify outliers before ruling out the possibility. As certain results are determined to be benign, care should be taken to adjust the rule logic accordingly to avoid future hits. The schedule of this report should be at the same interval as your scheduled scans to avoid aggregating results across multiple scans. Training on RSA NetWitness Endpoint, including analysis of Scan Data, may be found on RSA Link: https://community.rsa.com/docs/DOC-84977 VERSIONS SUPPORTED * RSA NetWitness Endpoint 11.1 and higher DEPENDENCIES NetWitness Rules: * 11.1-11.2 Rarest Child Processes of Web Server Processes * 11.1-11.2 Rarest Code Signing Certificate CNs * 11.1-11.2 Rarest Parent Processes of cmd * 11.1-11.2 Rarest Parent Processes of powershell * 11.1-11.2 Rarest Processes Running from AppData * 11.1-11.2 Windows Process Parent Child Mismatch	endpoint	attack phase, exploit, malware, threat
11.1-11.2 Endpoint Scan Data Host Report	11.1-11.2 Endpoint Scan Data Host Report	This rule will return information about the endpoint for the configured hostname. This information could be useful when conducting an investigation into a suspect machine. Information includes autoruns, tasks, machine details, processes, services, DLLs and files. Training on RSA NetWitness Endpoint, including analysis of Scan Data, may be found on RSA Link: https://community.rsa.com/docs/DOC-84977. VERSIONS SUPPORTED * RSA NetWitness Endpoint 11.1 and higher CONFIGURATION When the Endpoint Scan Data Host Report is scheduled to run, you must enter a hostname or configure and use a NetWitness List of hostnames to return this scan data information. DEPENDENCIES NetWitness Rules: * 11.1-11.2 Autoruns and Tasks on Host * 11.1-11.2 DLLs on Host * 11.1-11.2 Files on Host * 11.1-11.2 Machine Details on Host * 11.1-11.2 Processes on Host * 11.1-11.2 Services on Host	endpoint	assurance, compliance, corporate, risk, vulnerability management
11.3 Endpoint Machine Summary Report	11.3 Endpoint Machine Summary Report	This report shows information for the machines configured to run the RSA NetWitness Endpoint agent including an OS and endpoint version summary. Training on RSA NetWitness Endpoint, including analysis of Scan Data, may be found on RSA Link: https://community.rsa.com/docs/DOC-84977. VERSIONS SUPPORTED * RSA NetWitness Endpoint 11.3 and higher DEPENDENCIES NetWitness Rules: * 11.3 Endpoint Operating Systems Summary * 11.3 Endpoint Version Summary * 11.3 Endpoint Indicators Summary * 11.3 Endpoint Indicators by Tactic and Technique * 11.3 Endpoint Indicators by Tactic * 11.3 Endpoint Indicators Analysis * 11.3 Endpoint Host State	endpoint	assurance, compliance, corporate, risk, vulnerability management
11.3 Endpoint Network Activity	11.3 Endpoint Network Activity	This report shows information for the network activity on machines configured to run the RSA NetWitness Endpoint agent. Training on RSA NetWitness Endpoint, including analysis of Scan Data, may be found on RSA Link: https://community.rsa.com/docs/DOC-84977. VERSIONS SUPPORTED * RSA NetWitness Endpoint 11.3 and higher DEPENDENCIES NetWitness Rules: * 11.3 Endpoint Module and Dynamic DNS * 11.3 Powershell to External Domain * 11.3 User Defined Domain Name Analysis	endpoint	assurance, compliance, corporate, risk, vulnerability management
11.3 Endpoint Scan Data Autorun and Scheduled Task Report	11.3 Endpoint Scan Data Autorun and Scheduled Task Report	This report looks for suspicious autoruns and tasks using a few key features. Autoruns/Scheduled Tasks mechanisms are often used by attackers to maintain persistence on a compromised host. This is not an exhaustive set of potentially suspicious autorun behavior, but should give an analyst visibility into some of the more common techniques leveraged by attackers. Training on RSA NetWitness Endpoint, including analysis of Scan Data, may be found on RSA Link: https://community.rsa.com/docs/DOC-84977 VERSIONS SUPPORTED * RSA NetWitness Endpoint 11.3 and higher DEPENDENCIES NetWitness Rules: * 11.3 Autoruns and Scheduled Tasks From or Referencing AppData * 11.3 Autoruns and Scheduled Tasks From Root of Program Data * 11.3 Autoruns and Scheduled Tasks Invoking Command Shell * 11.3 Autoruns and Scheduled Tasks Invoking Windows Script Host * 11.3 Autoruns and Scheduled Tasks Running Scripts * 11.3 Rarest Autorun Registry Keys * 11.3 Multiple Arguments for Same Task * 11.3 Multiple Filename for Task Name * 11.3 Multiple Task Name for Filename * 11.3 Rare Extension for Task * 11.3 Rarest Unsigned Service Names Across Endpoints * 11.3 Rarest Unsigned Task Names Across Endpoints * 11.3 Same Arguments for Different Task Filename * 11.3 Task Present on one Machine * 11.3 Uncommon Directory for Task * 11.3 User Created Unique Task	endpoint	attack phase, exploit, threat
11.3 Endpoint Scan Data File and Process Outliers Report	11.3 Endpoint Scan Data File and Process Outliers Report	This report focuses on rarity of particular process, file, and autorun features in the environment. While rarity in each of these results does not automatically imply malicious activity, it is important to analyze and justify outliers before ruling out the possibility. As certain results are determined to be benign, care should be taken to adjust the rule logic accordingly to avoid future hits. The schedule of this report should be at the same interval as your scheduled scans to avoid aggregating results across multiple scans. Training on RSA NetWitness Endpoint, including analysis of Scan Data, may be found on RSA Link: https://community.rsa.com/docs/DOC-84977 VERSIONS SUPPORTED * RSA NetWitness Endpoint 11.3 and higher DEPENDENCIES NetWitness Rules: * 11.3 Rarest Child Processes of Web Server Processes * 11.3 Rarest Code Signing Certificate CNs * 11.3 Rarest File Names Across Endpoints * 11.3 Rarest Parent Processes of cmd.exe * 11.3 Rarest Parent Processes of powershell.exe * 11.3 Rarest Processes Running from AppData * 11.3 Rarest Vendor of Unsigned Files Across Endpoints * 11.3 Windows Process Parent Child Mismatch	endpoint	attack phase, exploit, malware, threat
11.3 Endpoint Scan Data Host Report	11.3 Endpoint Scan Data Host Report	This rule will return information about the endpoint for the configured hostname. This information could be useful when conducting an investigation into a suspect machine. Information includes autoruns, tasks, machine details, processes, services, DLLs and files. Training on RSA NetWitness Endpoint, including analysis of Scan Data, may be found on RSA Link: https://community.rsa.com/docs/DOC-84977. VERSIONS SUPPORTED * RSA NetWitness Endpoint 11.3 and higher CONFIGURATION When the Endpoint Scan Data Host Report is scheduled to run, you must enter a hostname or configure and use a NetWitness List of hostnames to return this scan data information. DEPENDENCIES NetWitness Rules: * 11.3 Autoruns and Tasks on Host * 11.3 DLLs on Host * 11.3 Files on Host * 11.3 Machine Details on Host * 11.3 Processes on Host * 11.3 Services on Host	endpoint	assurance, compliance, corporate, risk, vulnerability management
All Risk Suspicious	All Risk Suspicious	This report lists All Risk Suspicious by Source, Destination and Session Size	log, packet	threat, identity, assurance, operations, situation awareness
All Risk Warning	All Risk Warning	This report lists All Risk Warning by Source, Destination and Session Size	log, packet	threat, identity, assurance, operations, situation awareness
Amazon VPC Traffic Flow	Amazon VPC Traffic Flow	The report provides insights on the Amazon VPC traffic flow. VERSIONS SUPPORTED 10.6.5.x and higher CONFIGURATION Configure the Amazon VPC plugin with valid credentials as per the plugin configuration document Use the latest table-map.xml DEPENDENCIES CEF log parser	log	event analysis, flow analysis, operations
Anonymous Proxy and Remote Control Activity	Anonymous Proxy and Remote Control Activity	Displays suspected use of services, clients or protocols for anonymous access or remote control activities.	log, packet	assurance, compliance, audit, operations, event analysis, situation awareness
AWS Access Permissions Modified Report	AWS Access Permissions Modified Report	10.5 and higher. Detects when Amazon Web Services (AWS) instance permissions are modified. The AWS CloudTrail log parser is a required dependency.	log	assurance, compliance, audit, identity, authorization
AWS Critical VM Modified Report	AWS Critical VM Modified Report	10.5 and higher. Detects when Amazon Web Services (AWS) critical virtual machine instances are modified. Actions detected by this module include instances being terminated, stopped and rebooted as well as modification of instance attributes and monitoring status. In order to trigger an alert, a custom feed of critical instance source IPs must be created to populate the alert meta key with the value "critical_vm". The AWS CloudTrail log parser is a required dependency.	log	assurance, compliance, audit, identity, authorization
Azure Monitoring Insights	Azure Monitoring Insights	The report provides insights on the Azure Monitor operations. VERSIONS SUPPORTED 10.6.5.x and higher CONFIGURATION Configure the Azure Monitor plugin with valid credentials as per the plugin configuration document Use the latest table-map.xml	log	event analysis, operations
BASEL II - Compliance Report	BASEL II - Compliance Report	This article introduces Basel II report templates. Basel II compliance reports are based on recommendations by bank supervisors and central bankers to improve the consistency of capital regulations internationally, make regulatory capital more risk sensitive, and promote enhanced risk-management practices among international banking organizations.	log	assurance, compliance, audit
BILL 198 - Compliance Report	BILL 198 - Compliance Report	This article introduces Bill 198 compliance reports. Bill 198 empowers the Ontario Securities Commission to develop guidelines to protect investors in public Canadian companies by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws.	log	assurance, compliance, audit
Bulk Data Transfer - Report	Bulk Data Transfer - Report	Displays events where the amount of data transferred between the Source-Destination IP pairs is over 20 Mb or 50 Mb.	packet	assurance, compliance, audit
Cleartext Authentications	Cleartext Authentications	This report displays events in which passwords were sent over cleartext using network protocols such as FTP, HTTP, POP3 and SMTP.	packet	assurance, risk, organizational hazard, operations, event analysis, protocol analysis
Encrypted Traffic	Encrypted Traffic	This report shows encrypted sessions that may warrant additional investigation by an analyst. A threat actor may use atypical protocols or ports to hide malicious activities such as data exfiltration.	log, packet	operations, situation awareness
Encrypted Traffic over Non-Standard Port	Encrypted Traffic over Non-Standard Port	Summarizes sessions containing encrypted traffic that are not on port 22, 993, 995 or 443.	packet	operations, event analysis, protocol analysis
Executables	Executables	This report presents instances of executables detected on wire. This report is broken into four sections: Executables by Domain, Country, Executables with abnormal characteristics - Suspicious and Warning	packet	operations, event analysis, file analysis
FERPA - Compliance Report	FERPA - Compliance Report	This article introduces the Family Educational Rights and Privacy Act (FERPA) compliance report templates. The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. 1232g, 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.	log	assurance, compliance, audit
FFIEC - Compliance Report	FFIEC - Compliance Report	This article introduces the Federal Financial Institutions Examination Council (FFIEC) compliance templates. The Federal Financial Institutions Examination Council (FFIEC) is a body of the United States government empowered to prescribe principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), Mergers & Acquisitions International Clearing (MAIC), and the Consumer Financial Protection Bureau (CFPB).	log	assurance, compliance, audit
File Transport Over Uncommon Protocol	File Transport Over Uncommon Protocol	Displays files transported over uncommon protocols such as ICMP and those identified as unknown. This report will ignore files transferred over common protocols of HTTP, FTP, SMTP, POP, RSYNC and TFTP.	packet	operations, event analysis, protocol analysis
FISMA - Compliance Report	FISMA - Compliance Report	This article introduces the Federal Information Security Management Act (FISMA) compliance templates.. The Federal Information Security Management Act (FISMA) is designed to ensure appropriate security controls for government information systems.	log	assurance, audit, compliance
G Suite - Activity Report	G Suite - Activity Report	The report provides insights on the G Suite - Activities. VERSIONS SUPPORTED 11.2.1 and higher CONFIGURATION Configure the G Suite plugin with valid credentials as per the plugin configuration document Use the latest table-map.xml DEPENDENCIES CEF log parser	log	event analysis, log analysis, operations
G Suite - Admin Report	G Suite - Admin Report	The report provides insights on the G Suite - Admin Activities. VERSIONS SUPPORTED 11.2.1 and higher CONFIGURATION Configure the G Suite plugin with valid credentials as per the plugin configuration document Use the latest table-map.xml DEPENDENCIES CEF log parser	log	event analysis, log analysis, operations
GLBA - Compliance Report	GLBA - Compliance Report	This article introduces the Gramm-Leach-Bliley Act (GLBA) compliance templates. The Gramm-Leach-Bliley Act (GLBA) requires companies defined under the law as "financial institutions" to ensure the security and confidentiality of this type of information. As part of its implementation of GLBA, the Federal Trade Commission (FTC) issued the Safeguards Rule, which requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure.	log	assurance, compliance, audit
Global Filtering Candidate Report	Global Filtering Candidate Report	Shows an aggregated view of traffic that is being captured in your SA deployment.Use this view to determine candidates for filtering. For instance, if the entire company reads CNN throughout the day, this report will show that usage. You could then make a decision to filter the CNN traffic from view,so that suspicious traffic becomes more noticeable.Available rules and lists cover different browsing categories, such as Ad servers, streaming sites,social networks,and so on.	log, packet	operations, event analysis, filters
GPG-13 - Compliance Report	GPG-13 - Compliance Report	Good Practice Guide 13 (GPG13) defines requirements for protective monitoring-for example, the use of intrusion detection and prevention systems(IDS/IPS)-with which local authorities must comply in order to prevent accidental or malicious data loss.	log	assurance, compliance, audit
HIPAA - Compliance Report	HIPAA - Compliance Report	The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates that providers, health plans, clearinghouses, and their business associates establish appropriate administrative, technical, and physical safeguards to protect the privacy and security of sensitive health information.	log	assurance, compliance, audit
Hunting Detail	Hunting Detail	The Hunting Pack is a set of content that derives indicators of compromise and anomalous events. See the Hunting Guide, https://community.rsa.com/docs/DOC-62341, and the Hunting Feed, https://community.rsa.com/docs/DOC-62301, for more details about the contents of the pack and the suggested investigation techniques. This report displays events that have been categorized according to the following meta keys with added contextual evidence to assist an analyst. Note: This should be run as a daily report. The amount of meta values reported may be large depending on traffic volume and running over longer time frames may result in a query timeout. - Indicators of Compromise: Possible intrusions into the network or at the endpoint that can be identified through malware signatures or IPs and domains associated with command and control campaigns - Behaviors of Compromise: Designated for suspect or nefarious behavior outside the standard signature-based detection - Enablers of Compromise: Instances of poor information or operational security. Post-mortem often ties these to the root cause - Service Analysis: Core application protocols identification and inspection - Session Analysis: Client-server communication deviations - File Analysis: A large inspection library that highlights file characteristics and anomalies	log, packet, endpoint	application analysis, attack phase, event analysis, featured, file analysis, malware, operations, threat
Hunting Summary	Hunting Summary	The Hunting Pack is a set of content that derives indicators of compromise and anomalous events. See the Hunting Guide, https://community.rsa.com/docs/DOC-62341, and the Hunting Feed, https://community.rsa.com/docs/DOC-62301, for more details about the contents of the pack and the suggested investigation techniques. This report displays a summary of the events that have been categorized according to the following meta keys: - Indicators of Compromise: Possible intrusions into the network or at the endpoint that can be identified through malware signatures or IPs and domains associated with command and control campaigns - Behaviors of Compromise: Designated for suspect or nefarious behavior outside the standard signature-based detection - Enablers of Compromise: Instances of poor information or operational security. Post-mortem often ties these to the root cause - Service Analysis: Core application protocols identification and inspection - Session Analysis: Client-server communication deviations - File Analysis: A large inspection library that highlights file characteristics and anomalies	log, packet, endpoint	application analysis, attack phase, event analysis, featured, file analysis, malware, operations, threat
Identity Management	Identity Management	Summarizes user account activity (creates, deletions, disables, modifications), group modifications, password changes and access revocations.	log	identity, accounting, operations, situation awareness
Inbound Network Traffic - Top 25	Inbound Network Traffic - Top 25	Compliance Report Template- Inbound Network Traffic - Top 25	log	operations, event analysis, protocol analysis, flow analysis
IP Profiling	IP Profiling	Summarizes activity on your network based on a list of source IP addresses.The report includes bandwidth utilization, risk alerts, threats, top destinations, OS types, browsers and clients.To use the report, create and populate the report list with source IP addresses as noted in the dependencies.	log, packet	identity, accounting, operations, situation awareness
ISO27002 - Compliance Report	ISO27002 - Compliance Report	ISO 27002 establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization. ISO 27002 is used as the foundation and technical guidelines for many international and industry compliance standards and are generally good practices for all organizations.	log	assurance, compliance, audit
Large Outbound Encrypted Sessions	Large Outbound Encrypted Sessions	Summarizes instances of HTTPS or SSH on any port where the destination is to non-RFC1918 address space that have a session size of 5MB or greater. These connections are indicative of a file transfer.	packet	assurance, risk, organizational hazard, operations, event analysis, flow analysis
Large Outbound Sessions	Large Outbound Sessions	Summarizes sessions which have a session size of 5MB or greater, those being indicative of a large file transfer from RFC 1918 to non RFC 1918 address.	packet	assurance, event analysis, flow analysis, operations, organizational hazard, risk
Lateral Movement Indicators - Windows	Lateral Movement Indicators - Windows	Report displays possible indicators of lateral movement on Windows systems.	log	action on objectives, attack phase, featured, lateral movement, threat
Malware Activity Report	Malware Activity Report	Displays traffic that has been going to a known malicious IP address or references a hostname that is known to be malicious. This could indicate an infected host on your network. The native NETWORK packet parser must be enabled. This parser is enabled by default. You will also need to have at least one of the following feeds deployed. Feeds * Investigation * RSA FirstWatch C2 Domains * RSA FirstWatch C2 IPs * RSA FirstWatch APT Domains * RSA FirstWatch APT IPs If deploying the Investigation feed, you will need at least two of the related Lua parsers. Lua Parsers * HTTP_lua OR TLS_lua * DNS_verbose_lua OR DynDNS If collecting logs you will need at least one event source with device class of web logs. This includes web proxy and security products such as Cisco WSA and SQUID. And you will need at least one event source from the following device classes: * Firewall * IDS * IPS * Netflow (rsaflow) Note: For deployments prior to 10.6.2, you will also need to configure a set of new meta keys: inv.context and inv.category. See product documentation of the Investigation Feed for more details: https://community.rsa.com/docs/DOC-62303.	log, packet	featured, malware, threat
NERC-CIP - Compliance Report	NERC-CIP - Compliance Report	The NERC CIP compliance reports are based on North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) program requirements. The CIP program coordinates NERCs efforts to improve physical and cyber security for the bulk power system of North America as it pertains to reliability. This includes standards development, compliance enforcement, assessments of risk and preparedness, disseminating critical information via alerts to industry, and raising awareness of key issues.	log	assurance, compliance, audit
Netflow - Excessive DNS Responses	Netflow - Excessive DNS Responses	10.4 or higher Log Collector required for Netflow collection protocol.Displays Excessive DNS Responses by Client and Server IP addresses. This could indicate that someone is collecting information for a possible attack.For this report to get populated, ensure that device parser "RSAFlow" for 10.3 logdecoder or "CEF" for 10.4 logdecoder is enabledand meta-keys "direction" and "Source Port (ip.srcport) " are indexed in table-map.xml and index-concentrator-custom.xml	log	operations, event analysis, protocol analysis, flow analysis
Netflow - Filtering Candidates	Netflow - Filtering Candidates	10.4 or higher Log Collector required for Netflow collection protocol.This report displays information about Network Traffic analysis. An overview of the network is presented by listing the Top Protocols, Top Applications and First Heard IPs.For this report to get populated, ensure that device parser "RSAFlow" for 10.3 logdecoder or "CEF" for 10.4 logdecoder is enabledand meta-key "direction" is indexed in table-map.xml and index-concentrator-custom.xml	log	operations, event analysis, filters, flow analysis
Netflow - TCP Resets by Source IP	Netflow - TCP Resets by Source IP	10.4 or higher Log Collector required for Netflow collection protocol.This report displays TCP Resets by Source IP addresses.Useful for determining if any devices are behaving abnormally.For this report to get populated,ensure that "RSAFLOW" LogParser for 10.3 or "CEF" LogParser for 10.4 is enabled and meta key "direction" is indexed in table-map.xml and index-concentrator-custom.xml.Also ensure that the meta-key "TCP Flags Seen (tcp.flags.seen)" is indexed index-concentrator-custom.xml	log	operations, event analysis, protocol analysis, flow analysis
Netflow - Top Communicants	Netflow - Top Communicants	10.4 or higher Log Collector required for Netflow collection protocol.Displays different types of Top Talkers via Netflow. The data in the report can be used for identifying possible sources of DoS or disruption.It can also be used to identify sources for Data Ex-filtration.For this report to get populated, ensure that device parser "RSAFlow" for 10.3 logdecoder or "CEF" for 10.4 logdecoder is enabledand meta-key "direction" is indexed in table-map.xml and index-concentrator-custom.xml	log	operations, event analysis, protocol analysis, flow analysis, situation awareness
NetWitness Administration Report	NetWitness Administration Report	10.5 and higher. This gives a summary and detail view of the NetWitness Administration - Audit events. This Report uses non-indexed keys - result and msg. They need to be indexed on Log Decoder in table-map-custom.xml and should be added to Concentrator through index_concentrator_custom.xml.	log	assurance, compliance, audit
NetWitness Respond	NetWitness Respond	The report displays a summary and detailed view of the incidents and alerts generated using NetWitness Respond. REFERENCES On RSA Link, see the NetWitness Respond Configuration and User Guides for details. VERSIONS SUPPORTED 10.6.2 and higher CONFIGURATION You must configure the Respond service and database, alert data sources and aggregation rules for this report to populate. DEPENDENCIES * Common Event Format Log Parser	log, packet	assurance, audit, compliance
Network Activity	Network Activity	This report displays summary data for top network activity for the following:Top Alias Host Destination by Session Count,Top Alias Host Destination by Source IP,Top Destination Country by Session Count,Top Destination Country by Session Size,Top Destination Country by Source IP,Top HTTPS Destination IP by Session Size,Top Network Service by Session Count	log, packet	operations, event analysis, protocol analysis, flow analysis, situation awareness
NISPOM - Compliance Report	NISPOM - Compliance Report	This article introduces the National Industrial Security Program Operating Manual (NISPOM) templates. The National Industrial Security Program Operating Manual (NISPOM) developed by the Department of Defense, sets comprehensive standards for protecting classified data. All government agencies and commercial contractors who have access to classified data are required to implement system protection processes to ensure continued availability and integrity of this data, and prevent its unauthorized disclosure. These regulations apply to systems used in the capture, creation, storage, processing, or distribution of restricted information.	log	assurance, compliance, audit
Non-Standard Traffic	Non-Standard Traffic	This report displays sessions which are categorized as unusual based on service and port usage. Sessions will either include session found on non standard port or unknown service on standard port	packet	operations, event analysis, protocol analysis
Outbound Network Traffic - Top 25	Outbound Network Traffic - Top 25	Compliance Report Template- Outbound Network Traffic - Top 25	log	operations, event analysis, protocol analysis, flow analysis
PCI-Compliance Report	PCI - Compliance Report	The Payment Card Industry (PCI) Data Security Standard applies to all payment card industry members, merchants, and service providers that store, process, or transmit payment cardholder data. Additionally, these security requirements apply to all "system components" - any network component, server, or application included in, or connected to, the cardholder data environment.	log	assurance, compliance, audit
Phishing Profile	Phishing Profile	This report summarizes data relevant to phishing.In particular it summarizes HREF header mismatches, mail traffic from top countries by frequency, top email subjects, top email addresses by frequency, top file extension of attachments by frequency.	log, packet	threat, attack phase, delivery, operations, event analysis, protocol analysis
RSA SecurID Authentication Summary	RSA SecurID Authentication Summary	This report summarizes all RSA SecurID Authentications. An incident response analyst may want to review all two-factor authentication activity over a given period of time. Each authentication type is paired with associated user, event counts and a description of each outcome. Note: You will need to index the non-standard meta key 'result' on the Log Decoder and Concentrator in order to fully populate this report. See the report documentation for more details at https://community.rsa.com/docs/DOC-43406. DEPENDENCIES: RSA Authentication Manager and User Credential Manager event source (log parser rsaacesrv)	log	featured, authentication, identity
RSA SecurID Cloud Admin and User Activity Insights	RSA SecurID Cloud Admin and User Activity Insights	The report provides insights on the SecurID admin and user events. VERSIONS SUPPORTED 10.6.5.x and higher This is supported only for the SecurID Cloud platform CONFIGURATION Configure the RSA SecurID Access plugin with valid credentials as per the plugin configuration document Use the latest table-map.xml	log	authentication, identity
Shadow IT Use	Shadow IT Use	Detects shadow IT use within the organization. At least one of the dependent application rules - organized by category of shadow IT - must be deployed to the decoder in order to populate the report. This report is dependent on the following report rules: Shadow IT Use High Risk, Shadow IT Use by Category - Event Count, Shadow IT Use by Category - Session Size, Shadow IT Use by IP Source, Shadow IT Use by BYOD. It is dependent on the following List: Watchlist by IP (optional for High Risk report). It is dependent on the following RSA Application Rules: Stealth EmailUse, Voice Chat Apps, File Sharing Apps, BYOD Mobile Web Agent Detected, Large Outbound Session. It is dependent on the following RSA Lua Parsers: http_lua, tls_lua.	log, packet	assurance, risk, organizational hazard
SOX - Compliance Report	SOX - Compliance Report	Sarbanes-Oxley Act of 2002 (SOX). Congress passed the Sarbanes-Oxley Act (SOX) in large part to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws. Section 404 of Sarbanes-Oxley not only requires companies to establish and maintain an adequate internal control structure, but also to assess its effectiveness on an annual basis.	log	assurance, compliance, audit
SSAE 16 - Compliance Report	SSAE 16 - Compliance Report	Statement on Standards for Attestation Engagements (SSAE 16) is an attestation standard issued by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) specifically geared towards addressing engagements conducted by service organizations to report on the design of controls and their operating effectiveness.	log	assurance, compliance, audit
SSH Activity	SSH Activity	Reports 2 activities:ANY ssh going to external IP addresses and ANY ssh detected over a port other than 22.	packet	operations, event analysis, protocol analysis, flow analysis
Top 10 Situational Awareness Report	Top 10 Situational Awareness Report	This report summarizes a set of "top 10" data points to provide situational awareness of traffic in your network environment. These data points include: websites by category, destination countries, destination countries by service type, destination IP addresses, search engine queries, services, uncategorized sites, websites and countries with warning or suspicious level alerts.	log, packet	threat, identity, assurance, operations, situation awareness
Top Communicants	Top Communicants	This report summarizes top communicants on your network by foreign country, protocol, outbound protocol, outbound source IP and foreign domain.	log, packet	assurance, compliance, audit, operations, event analysis, situation awareness
Traffic Flow in Azure NSG and Amazon VPC	Traffic Flow in Azure NSG and Amazon VPC	The reports provides insights on the Azure NSG and Amazon VPC traffic flow. VERSIONS SUPPORTED 10.6.5.x and higher CONFIGURATION Configure the Amazon VPC plugin and Microsoft Azure NSG with valid credentials as per the plugin configuration documents Use the latest table-map.xml DEPENDENCIES CEF log parser	log	event analysis, flow analysis, operations
User Watch	User Watch	Summarizes observed activity associated with one or more users populated in a watchlist.Activity summaries include login, logout, cleartext authentication, email and activity categorized as risk.suspicious and risk.warning.To use the report, create and populate the report lists as noted in the dependencies.	log, packet	assurance, compliance, audit, identity, authorization, operations, situation awareness