ForeScout® Research and Intelligent Analytics Program

Data Security Document

October 1, 2017

Updated for CounterACT 7.0.0 SP 3.0.1 with Device Profile Library 2.0.1

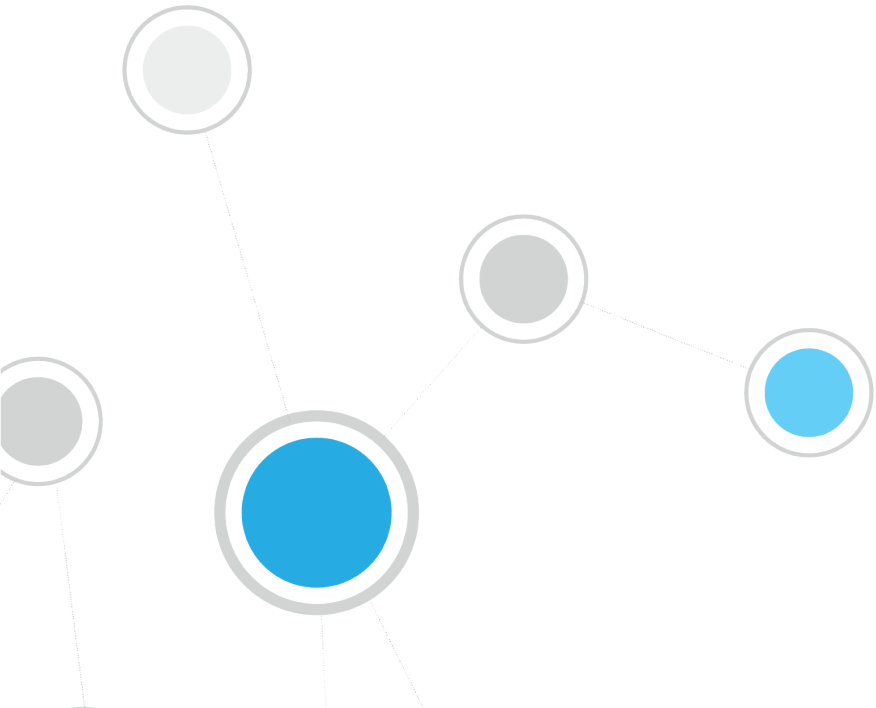


Table of Contents

About the ForeScout Research and Intelligent Analytics Program

The goal of the ForeScout Research and Intelligent Analytics Program (the 'Program') is to improve the classification and posture assessment capabilities of ForeScout CounterACT® for all ForeScout customers.

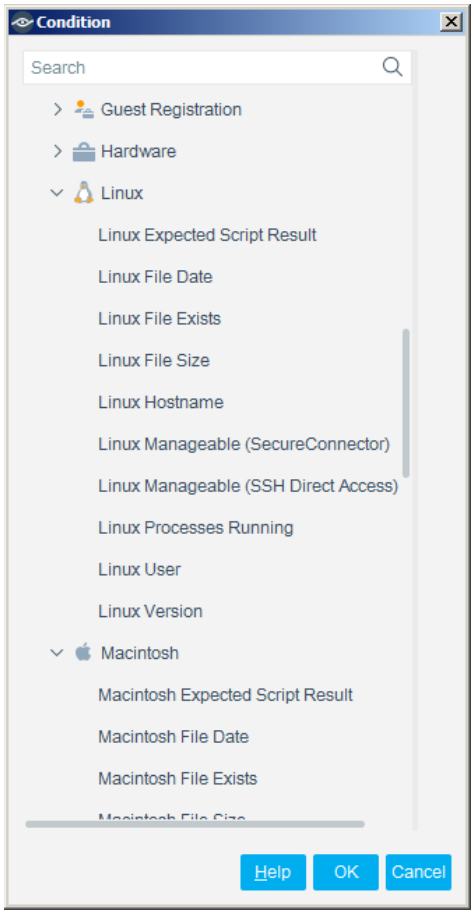
Collecting endpoint data from customers enables ForeScout to use machine analytics as well as human researchers to improve the quality of its classification capabilities. This both improves the accuracy of existing classification profiles, and better enables the creation of new profiles. Ongoing research constantly improves CounterACT's ability to assess endpoint posture based on the analysis of the data collected.

Program Details

CounterACT's internal database keeps track of the endpoints in your environment and the properties belonging to each endpoint. A 'property' is a name-value pair that describes a given attribute relating to that endpoint. Each CounterACT deployment is unique in terms of the environment in which it runs, the plugins and modules that are installed, the version of the software running and the network access given to the product. The set of properties that CounterACT tracks for each endpoint differs between environments, and may even differ for endpoints within a given environment.

In general, customers can see which properties CounterACT can resolve in their environment by looking at the conditions available when creating or editing a policy condition. The actual properties that are resolved depend on the CounterACT configuration.

Along with the specific properties utilized by CounterACT policy conditions, some properties may be automatically resolved. The following shows a sample of policy conditions that may be available in your environment:



Under the Program, you may allow CounterACT to share certain data about your endpoints and their properties with ForeScout.

Data Sanitization

CounterACT sanitizes the data it collects before uploading it to ForeScout's research servers. The data consists of certain CounterACT properties for all endpoints discovered by CounterACT in your environment. The properties that are uploaded do not contain any Personally Identifiable Information (PII) of the endpoint users in your environment. Additionally, ForeScout takes great effort to help ensure that any host property data that could identify your organization is either removed or anonymized prior to upload. ForeScout does not store any data that can identify your organization, except for an authentication token unique to your environment which is stored securely offline.

CounterACT properties are divided into the following three groups:

Group	Upload Status	Property Description	Examples
PII	**Never Uploaded**	Properties that contain information about the user of the endpoint.	User, Email, Last Name, Guest User Name

Group	Upload Status	Property Description	Examples
Sensitive Data	**Anonymized Prior to Upload**	Properties that may reveal sensitive information about your environment. See Properties Anonymized before Upload and Additional NetFlow Properties Anonymized before Upload.	IP Address, MAC Address, Hostname and internal DNS properties
Generic Data	**Uploaded 'As Is'**	Properties that do not contain Sensitive Data, but can be used to characterize endpoints for the purposes of classification. See Properties Uploaded 'As Is' and Additional NetFlow Properties Uploaded 'As Is'.	Linux Version, Windows Cloud Application Installed, DHCP Vendor Class, Manual Classification

Data Anonymization Process

For properties in the 'Sensitive Data' group, CounterACT employs an anonymization process prior to uploading the data to ForeScout's research servers. The process works as follows:

- All IP addresses discovered by CounterACT are re-enumerated such that each endpoint is given a unique 'fake' IP address. This 'fake' IP address is maintained in order to identify and track the endpoint data post-anonymization. Those outside your CounterACT environment cannot use these 'fake' IP addresses to reverse engineer the actual IP addresses of the endpoints in your environment.
- The last 12 bits of MAC addresses are removed. These addresses are then re-enumerated such that the last 12 bits of the first endpoint are set to value '1', the next endpoint to value '2', etc. The first 36 bits of MAC addresses are maintained so that this portion of the MAC address can be used to identify the NIC vendor, which is useful for classification.
- Actual hostnames and DNS names of endpoints in your environment are not uploaded; however, metadata may be extracted from the names and uploaded. For example, if an endpoint's name starts with 'dc', the metadata might note a possible indication of a Domain Controller (due to the common practice of naming conventions). This information is useful in classifying the endpoint as a Windows server.

Upload Methodology

When CounterACT is ready to upload the data, the data is sanitized, anonymized and compressed, and then uploaded to ForeScout's research servers. If you have a CounterACT Enterprise Manager, the data is uploaded via the Enterprise Manager; otherwise your standalone CounterACT Appliance uploads the data. CounterACT employs mutual authentication to help ensure that it uploads data to ForeScout's servers only, and not to another site that may attempt to spoof it.

Server Details

The Program is hosted by Amazon Web Services ('AWS'). The server that your Enterprise Manager or standalone Appliance connects to is ds.forescout.com, and all connections are over HTTPS (port 443/TCP).

Upload Frequency

Each standalone Appliance or Enterprise Manager will attempt to upload data in bulk every 24 hours. If an upload fails for any reason, no attempts will be made to upload the content until the following day.

Bandwidth Used

The amount of data uploaded from your environment to ForeScout is dependent on the following major factors:

- The number of endpoints in your environment. The more endpoints, the greater the amount of data.
- Which plugins and modules you have installed. Although not all host properties are uploaded, in general, the more host properties that are resolved for your endpoints, the greater the amount of data to be uploaded.

The following table provides an estimated baseline of how much bandwidth is used per upload, which depends on the number of endpoints discovered by CounterACT and the number of properties to be uploaded. The table assumes an average of 14 uploaded properties per endpoint. See Appendix I – List of Uploaded CounterACT Properties for a complete list of properties that may be uploaded.

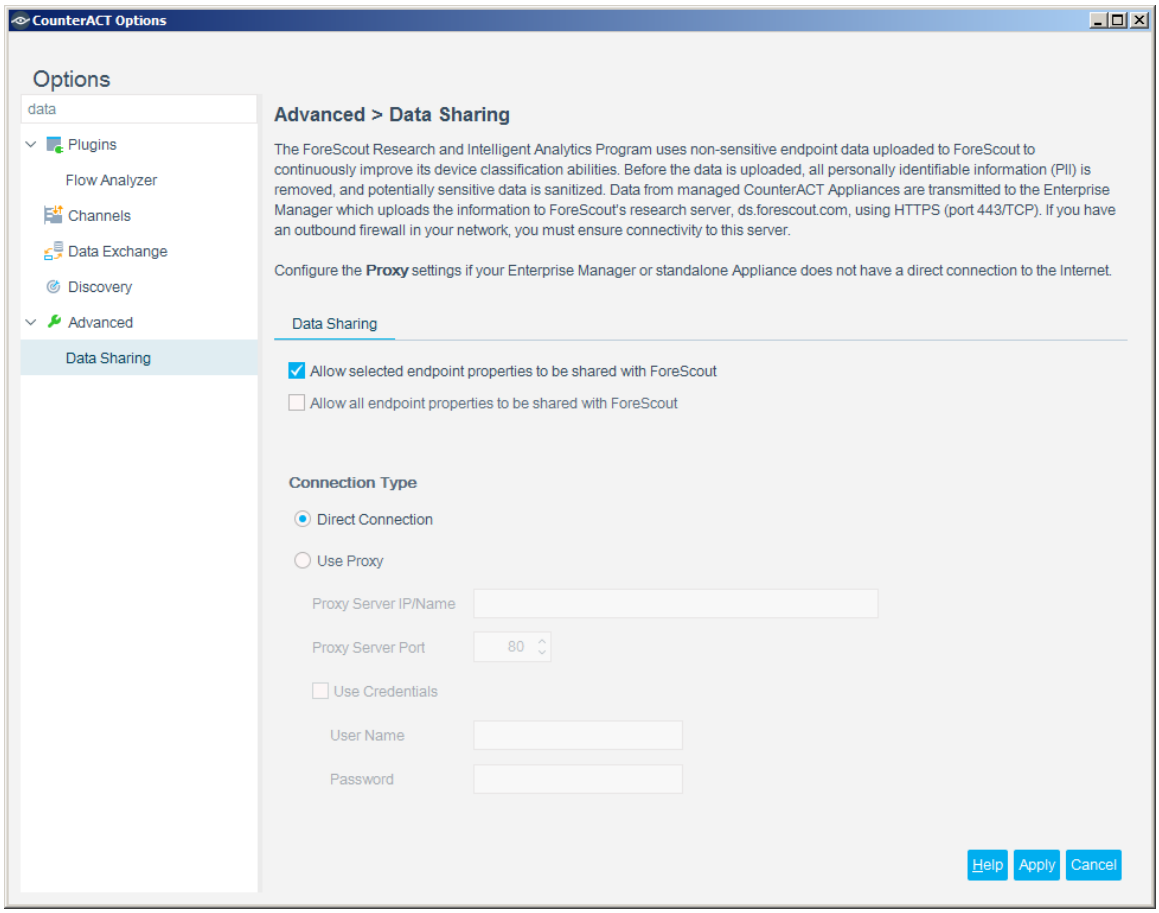
Number of Endpoints Managed by the Appliance	Bandwidth Used per Upload
1	4KB
10	5KB
100	18KB
1,000	152KB
10,000	1.68MB

Data Storage Security

All data uploaded as part of the Program is encrypted using a combination of RSA-1024 and AES-256 encryption, and can only be decrypted by a dedicated team of ForeScout researchers.

Controlling Your Data

You may opt in and opt out of the Program at any time via the *Advanced > Data Sharing* pane in the Options dialog of your CounterACT Console. Changes take effect as soon as you click the Apply button. If you opt out, any data that was previously uploaded prior to your opt-out will remain in the Program, but CounterACT will not upload any additional data.



The first checkbox, *Allow selected endpoint properties to be shared with ForeScout*, allows CounterACT to share only a subset of properties with ForeScout. The second checkbox, *Allow all endpoint properties to be shared with ForeScout*, allows CounterACT to share additional properties with ForeScout. Currently, this includes sampled, statistical network traffic flow information. This additional data is used to develop more advanced classification and posture assessment profiles which may be delivered to customers in future versions of CounterACT.

Appendix I – List of Uploaded CounterACT Properties

The properties listed below are provided by various plugins and extended modules within CounterACT. Some of the properties are hidden. Not all of them necessarily exist in your environment. The list covers the complete whitelist of properties that will be uploaded to the Program if they exist in your environment.

Properties Uploaded 'As Is'

The following properties contain generic information that CounterACT will upload ‘as is’.

Property Name	Internal Name
Admission	adm
AirWatch Applications	aw_DeviceAppsResult
AirWatch Compromised Status	aw_IsCompromised
AirWatch Model	aw_Model
AirWatch OS Version	aw_OperatingSystem
AirWatch Platform	aw_Platform
Applications Installed	application
Classification Method	cl_type
Classification Method (Classification Version 3)	cl_type3.0
Classification Rule	cl_rule
Classification Rule (Classification Version 3)	cl_rule3.0
Classified by Action	operator_classified
classify_action_result	classify_action_result
Device Interfaces	device_interfaces
Device is DHCP Relay	is_dhcp_relay
Device is DHCP Server	is_dhcp_server
Device is NAT	nat
DHCP device class	dhcp_class
DHCP device OS	dhcp_os
DHCP options fingerprint	dhcp_opt_fingerprint
DHCP request fingerprint	dhcp_req_fingerprint
DHCP Vendor Class	dhcp_vendor_class
DNS Event	dnsniff_event
ePO Host Nac Health Status	epo_host_nac_health_status
External Classification	extcls

Property Name	Internal Name
External Device Connected (By Class)	external_class_device
External Network Function	external_netfunc
FireEye HX Network Info	fireeye_hx_host_network_info
FireEye HX OS Info	fireeye_hx_host_os_info
FireEye HX Threat Detections	fireeye_hx_detected_ioc
FireEye NX Threat Detections	fireeye_detected_ioc
Host is online	online
HTTP User Agent	ebanner_http
Linux Version	linux_operating_system
MAC Prefix	mac_prefix32
Macintosh Applications Installed	mac_app_installed_detected
Macintosh Version	mac_operating_system
Macintosh-OS Version	va_mac_os
Malicious Event	malic
Manual Network Function	operator_netfunc
matched_fingerprints	matched_fingerprints
Member of Group	in-group
Microsoft Applications Installed	product
Microsoft Vulnerabilities	vulns
Miscellaneous Events	misc_events
MobileIron Android Device Rooted	mi_android_rooted
MobileIron iOS Device JailBroken	mi_ios_jailbroken
MobileIron Manufacturer	mi_manufacturer
MobileIron Model	mi_model
MobileIron Platform	mi_platform
Network Function	va_netfunc
Network Function (Classification Version 3)	va_netfunc3.0
NIC Vendor	vendor
Nmap-Banner (Ver. 5.3)	nmap_banner5
Nmap-Banner (Ver. 7)	nmap_banner7
Nmap-Network Function(Ver. 5.3)	nmap_netfunc5
Nmap-Network Function(Ver. 7)	nmap_netfunc7
Nmap-OS Fingerprint(Ver. 5.3)	nmap_def_fp5
Nmap-OS Fingerprint(Ver. 7)	nmap_def_fp7
Number of IP Addresses	host_ips

Property Name	Internal Name
Open Ports	openports
Open Ports Delay	openportsdelay
Operating System	os_classification
os_classify_action_result	os_classify_action_result
Function	prim_classification
Recent appliances	recent_apps
Service Banner	banner
Splunk Alerts	splunk_alerts
Splunk Last Alert	splunk_last_alert
Suggested Operating System	suggested_os_classification
Suggested Function	suggested_prim_classification
Switch Port Name	sw_port_desc
Switch Port PoE Connected Device	sw_port_poe_desc
Switch Port PoE Power Consumption	sw_port_poe_power
Switch Port VLAN	sw_port_vlan
Switch Port Vlan Group	sw_port_vlan_group
Switch Port Voice Device	sw_port_voice_device
Switch Port Voice VLAN	sw_port_voice_vlan
Switch Ports Host ACL Locations – Enforced	sw_port_acl_restricted_locations
Switch Vendor	sw_vendor
Switch Virtual Interface	sw_virtual_interface
Switch VoIP Port	sw_voip_port
System Description	sw_netfunc_os
TCP/IP Syn Ack Fingerprint	p0f_sa_fingerprint
TCP/IP Syn Fingerprint	p0f_fingerprint
Traffic seen	engine_seen_packet
Vendor and Model	vendor_classification
Virtual Machine Guest Health	vmware_guest_health
Virtual Machine Guest OS	vmware_guest_os
Virtual Machine Peripheral Devices	vmware_vm_peripherals
VMware Server OS Type	vmware_server_os_type
VMware Server Product ID	vmware_server_product_line_id
VMware Server Product Name	vmware_server_product_name
VMware Server Vendor	vmware_server_vendor
VMware Server Version	vmware_server_version

Property Name	Internal Name
Windows Services Running	Service
Windows Version	va_os
Windows Version Fine- tuned	va_os_comp
Wireless Device (Banner)	access_point
WLAN AP Location	wifi_ap_location
WLAN AP Name	wifi_ap_name
WLAN Association Status	wifi_client_status
WLAN CTP Vendor	wifi_vendor
WLAN Detected Client Type	host_os
WLAN Managing Controller	wifi_ap_wlc
WLAN Network Function	wireless_netfunc_role
WLAN SSID	wifi_ssid
XenMobile MDM Managed	zdm_register_status
XenMobile Model	zdm_model
XenMobile OS Build	zdm_SYSTEM_OS_BUILD
XenMobile OS Version	zdm_SYSTEM_OS_VERSION
XenMobile Platform	zdm_SYSTEM_PLATFORM
XenMobile Product Name	zdm_PRODUCT_NAME
XenMobile Software Inventory	zdm_softwareInventory

Properties Anonymized before Upload

All sensitive information in the following properties will be anonymized before being uploaded to ForeScout.

Property Name	Internal Name
ClearPass Wireless Controller	clearpass_wireless_controller
DHCP Server Address	dhcp_server
IP Address	ip
Last known IP Address	lost_ip
MAC Address	mac
Sessions as Client	client_session
Sessions as Server	server_session
Switch IP	sw_ip
Switch IP and Port Name	sw_ipport_desc
Switch Location	sw_location
Virtual Machine Guest Network Adapters	vmware_guest_nic_info

Property Name	Internal Name
Virtual Machine Guest Primary IP	vmware_guest_ip
VMware vCenter Server IP	vmware_vcenter_ip

Additional NetFlow Properties Uploaded 'As Is'

The following additional properties contain generic information that CounterACT will upload ‘as is’ if you select *Allow all endpoint properties to be shared with ForeScout*.

Property Name	Internal Name
NetFlow Inbound Bits Per Second (daily)	flow_in_bps2
NetFlow Inbound Bits Per Second (hourly)	flow_in_bps1
NetFlow Inbound Bits Per Second (per minute)	flow_in_bps0
NetFlow Inbound Idle Time Percentage (daily)	flow_in_idle2
NetFlow Inbound Idle Time Percentage (hourly)	flow_in_idle1
NetFlow Inbound Idle Time Percentage (per minute)	flow_in_idle0
NetFlow Inbound Packet Size (daily)	flow_in_pktlen2
NetFlow Inbound Packet Size (hourly)	flow_in_pktlen1
NetFlow Inbound Packet Size (per minute)	flow_in_pktlen0
NetFlow Inbound Packets Per Second (daily)	flow_in_pps2
NetFlow Inbound Packets Per Second (hourly)	flow_in_pps1
NetFlow Inbound Packets Per Second (per minute)	flow_in_pps0
NetFlow Outbound Bits Per Second (daily)	flow_out_bps2
NetFlow Outbound Bits Per Second (hourly)	flow_out_bps1
NetFlow Outbound Bits Per Second (per minute)	flow_out_bps0
NetFlow Outbound Idle Time Percentage (daily)	flow_out_idle2
NetFlow Outbound Idle Time Percentage (hourly)	flow_out_idle1
NetFlow Outbound Idle Time Percentage (per minute)	flow_out_idle0
NetFlow Outbound Packet Size (daily)	flow_out_pktlen2
NetFlow Outbound Packet Size (hourly)	flow_out_pktlen1
NetFlow Outbound Packet Size (per minute)	flow_out_pktlen0
NetFlow Outbound Packets Per Second (daily)	flow_out_pps2
NetFlow Outbound Packets Per Second (hourly)	flow_out_pps1
NetFlow Outbound Packets Per Second (per minute)	flow_out_pps0
NetFlow Sessions as Client (DNS)	netflowtool_client_session_dns
NetFlow Sessions as Server (DNS)	netflowtool_server_session_dns

Additional NetFlow Properties Anonymized before Upload

These additional properties will be uploaded to ForeScout if you select *Allow all endpoint properties to be shared with ForeScout*. All sensitive information in these properties will be anonymized before being uploaded.

Property Name	Internal Name
NetFlow Sessions as Client	netflowtool_client_session
NetFlow Sessions as Server	netflowtool_server_session

Legal Notice

Send comments and questions about this document to: documentation@forescout.com

2017-10-01 11:04