

TRUEFORT FORTRESS™

# Crowdstrike Integration Guide



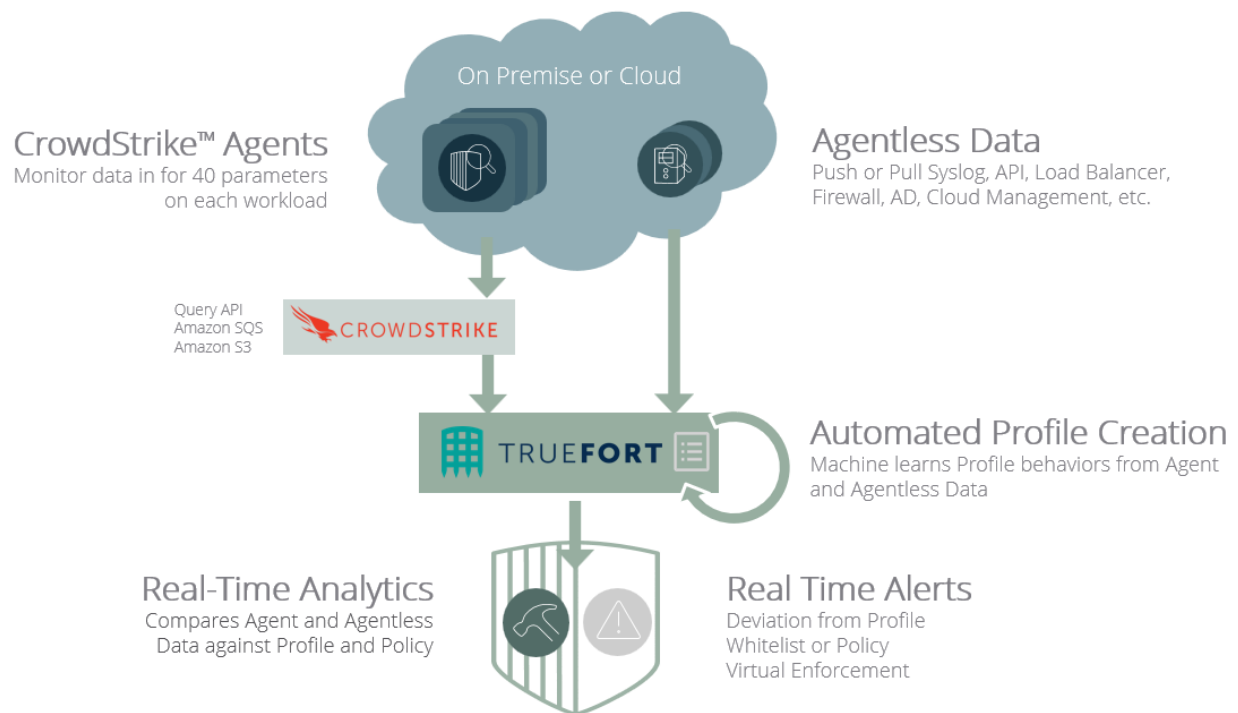
<b>CROWDSTRIKE INTEGRATION GUIDE</b>	<b>3</b>
<b>Overview</b>	<b>3</b>
<b>How ANALYTICS for CrowdStrike Works</b>	<b>4</b>
<b>Initial Steps</b>	<b>5</b>
<b>Setup Prerequisites</b>	<b>6</b>
SERVER REQUIREMENTS	6
HOST CHANGES	6
FIREWALL CHANGES	8
MISCELLANEOUS PREREQUISITES	8
TRUEFORT APPLIANCE CONFIGURATION INFORMATION	8
<b>ANALYTICS for CrowdStrike Configuration</b>	<b>9</b>
BUFFER TIME ADJUSTMENT	9
CROWDSTRIKE CONNECTION	9
CROWDSTRIKE-SPECIFIC DOMAIN AND AGENT GROUP	12
<b>Application Server Allowlisting</b>	<b>12</b>
<b>CrowdStrike APIs</b>	<b>15</b>
<b>Appendix A – Key Realm Interface Differentiators in Analytics</b>	<b>16</b>

# CROWDSTRIKE INTEGRATION GUIDE

## OVERVIEW

**TrueFort ANALYTICS for CrowdStrike™** adds comprehensive visibility and proactive detection capabilities – providing a deep understanding of applications and the environments they inhabit. This allows for the automation of complex threat detection and subsequent alert generation before valuable data can be lost. By visualizing and correlating current and historical event information, TrueFort identifies indicators of advanced threats that would otherwise go unnoticed.

CrowdStrike already gathers extensive telemetry from 40+ parameters on Windows and Linux servers to identify malware. It stores this telemetry in AWS S3 buckets. ANALYTICS clusters can access this stored data to provide continuous monitoring and real-time analytics for each workload.



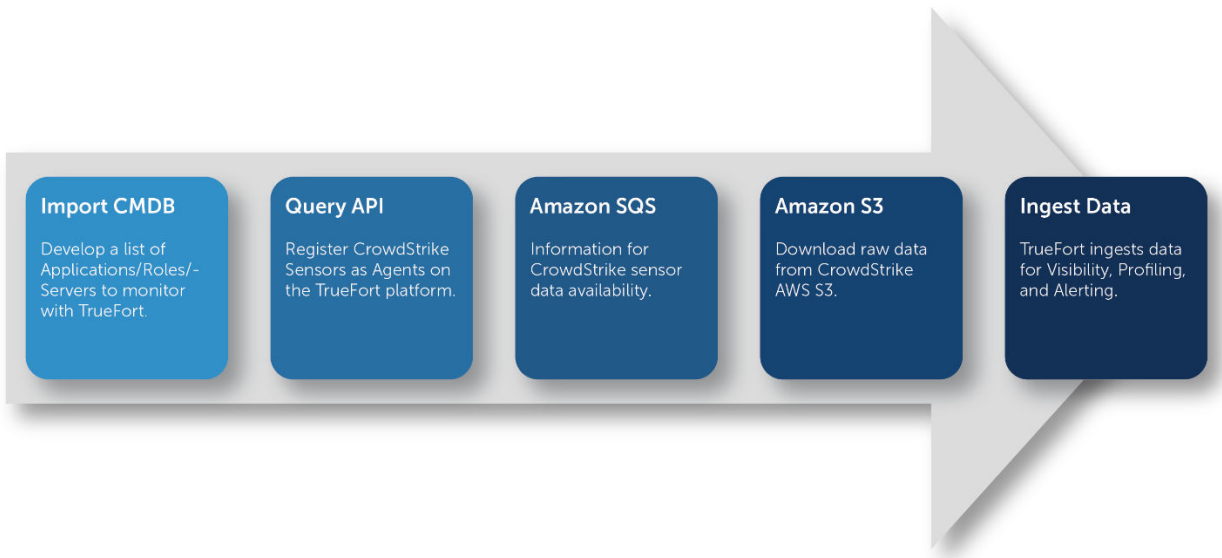
Once the initial ingestion is complete and the Application Dependency Map has been created, ANALYTICS begins profiling each workload using Machine Learning to create a baseline of accepted, normal behavior. After the profiling period is complete, ANALYTICS uses this information to analyze telemetry continually streaming in from CrowdStrike - identifying behavior that departs from the established “known good” profile.

In this way, ANALYTICS compliments and enhances CrowdStrike’s existing capabilities - further augmenting the ability to identify malicious insiders and persistent threat actors within data centers and cloud environments.

## HOW ANALYTICS FOR CROWDSTRIKE WORKS

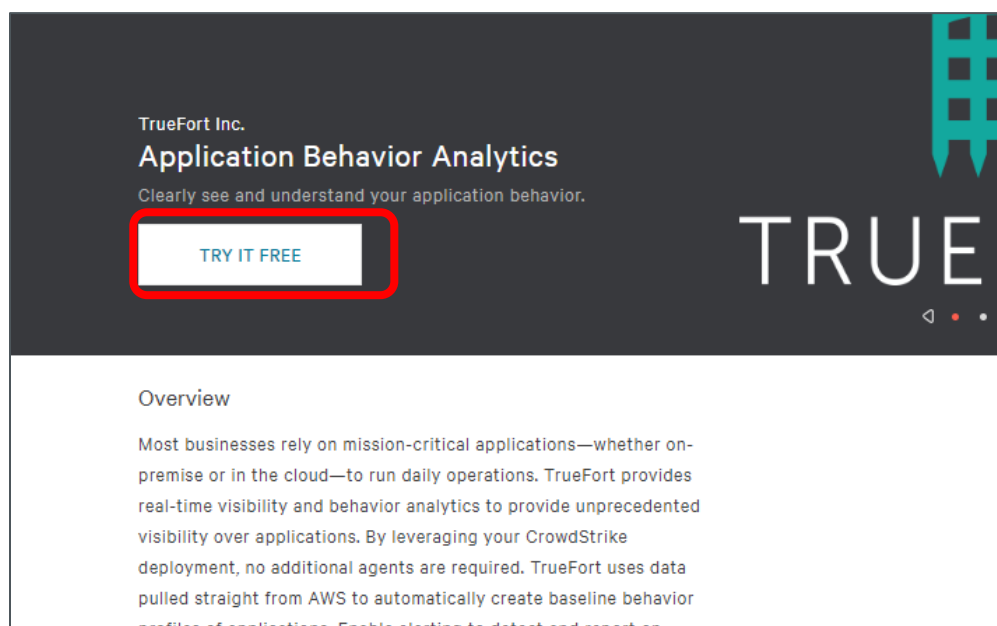
1. CrowdStrike agents send telemetry to AWS for malware/IOC analysis - storing it in an S3 bucket unique to each customer. CrowdStrike sends a message via SQS, notifying ANALYTICS that new telemetry is available for processing.
2. Via the **Falcon Data Replicator API**, ANALYTICS then collects stored telemetry related to only the application servers an organization wants to monitor. The following event-related information is collected:
  - Network
  - Processes
  - User (Identity)
  - NIC
3. ANALYTICS then analyzes the event-related information collected from the AWS cloud. This includes the **Agent ID (AID)** - the unique identifier of the CrowdStrike agent that collected and published the telemetry from a given application server.
4. ANALYTICS then calls the **Falcon Query API** to get more detail regarding each application server, using the AID to fetch server details of the specific CrowdStrike agent that published the information, such as:
  - Local IP Address
  - Local Port
  - Operating System
5. ANALYTICS then creates an agent within the ANALYTICS dashboard for that application server using the information it fetched from the Query API call.
6. If the details are provided by the customer, ANALYTICS for CrowdStrike also creates the application views under a specific organization with a corresponding region, application, and role.
7. ANALYTICS tracks metrics for each agent using the collected telemetry. At this point, an application profile can be defined either manually or via machine learning, and alerts can then be configured.





## INITIAL STEPS

The CrowdStrike-TrueFort integration process is initiated via the TrueFort listing on the **CrowdStrike Store**. Simply navigate to the listing page and select the **TRY IT FREE** button highlighted below.



Doing this provides TrueFort with the CrowdStrike and API credentials necessary for provisioning a CrowdStrike-TrueFort instance, as well as information required to connect the TrueFort instance to the CrowdStrike cloud. For more information on this process, please contact your TrueFort representative.

## SETUP PREREQUISITES

### SERVER REQUIREMENTS

ANALYTICS requires a machine with the following minimum hardware requirements:

- 16 vCPUs
- 128 GB RAM
- 1 Gb NIC

We recommend provisioning a cloud instance with the following specs:

#### AWS EC2 r5d 4xlarge instance with Persistent Storage

- 16 vCores, 128GB RAM, 2 x 300 GB EBS Volume
- RHEL 7.2 or higher

#### Azure E16 V3 and E20 Persistent SSD Storage

- 16 vCPU, 128 GiB, 512 GiB **Persistent SSD**
- RHEL 7.2 or higher

All appliance servers must have a pre-configured, IP-assigned management NIC.

### HOST CHANGES

#### ULIMIT SETTINGS

Verify that the Ulimit settings on your server are in line with the specifications detailed below.

Parameter	Value
core file size	(blocks, -c) 0
data seg size	(kbytes, -d) unlimited
scheduling priority	(-e) 0
file size	(blocks, -f) unlimited
pending signals	(-i) 772599
max locked memory	(kbytes, -l) unlimited
max memory size	(kbytes, -m) unlimited
open files	(-n) 100000

pipe size	(512 bytes, -p) 8
POSIX message queues	(bytes, -q) 819200
real-time priority	(-r) 0
stack size	(kbytes, -s) 8192
cpu time	(seconds, -t) unlimited
max user processes	(-u) 32768
virtual memory	(kbytes, -v) unlimited
file locks	(-x) unlimited

## REQUIRED PARTITIONS

Ensure that the following **seven** 50 GB partitions have been created on the cloud instance.

- /home
- /data/1
- /data/2
- /data/3
- /elastic
- /log
- /message

## REQUIRED PACKAGES

Ensure that the following packages have been installed on the cloud instance.

bash ≥ 4.0	openssh-clients ≥ 6.6	rsync ≥ 3.0.9
curl ≥ 7.29	openssh-server ≥ 6.6	sudo ≥ 1.8.6p7
iptables-services ≥ 1.4.21	postfix ≥ 2.10	sysstat ≥ 10.1.5
net-tools ≥ 2.0	python ≥ 2.7	wget ≥ 1.14
ntp ≥ 4.2.6	rpm-build ≥ 4.0	yum-utils ≥ 1.1.31
nscd ≥ 2.17		

## “BUSHIDO” SUDO USER

Each appliance that is part of a TrueFort cluster must have a “bushido” user added to the **sudo** group. Its UID must be identical across all cluster nodes.



## FIREWALL CHANGES

### PORT SETTINGS

Make the necessary firewall and proxy changes to allow user connectivity to ports **8090**, **9090**, and **9093** on the cloud instance.

### APPLIANCE-CROWDSTRIKE CONNECTION SETTINGS

Make the necessary firewall and proxy settings to allow the TrueFort appliance to connect out to the CrowdStrike cloud. This information is generated during the **Initial Steps** section of this guide.

- **api.crowdstrike.com** or **\*.crowdstrike.com**
- **SQS URL** – Provided after signing up on the CrowdStrike Store
- **S3 FQDN** – Provided after signing up on the CrowdStrike Store

## MISCELLANEOUS PREREQUISITES

The following items must be uninstalled/disabled on all TrueFort appliance servers:

- Gdb
- All wifi-related packages iw\*
- Red Hat 7 Built-In Firewall

## TRUEFORT APPLIANCE CONFIGURATION INFORMATION

The following information must also be provided to the TrueFort installation team:

### GENERAL APPLIANCE SETTINGS

- **DNS Server** – The IP address of the organization's DNS server.
- **DNS Search** – A list of domains for DNS lookups.
- **Gateway** – The IP address of the default network gateway.
- **Hostname** – Name of the machine on which the TrueFort appliance is to be configured.
- **IP Address** – IP address of the machine on which the TrueFort appliance is to be configured.
- **Netmask** – The network masking setting for the machine running TrueFort.
- **NTP Server** – The IP address or hostname of the network time protocol server to use for synchronization.

### SMTP SETTINGS

- **SMTP Server** – Email gateway for end-user email communication.
- **SMTP Port** – A specified SMTP port number for the email gateway in the event that an organization chooses not to use the default port (25).
- **SMTP User and Password** – SMTP user and password if the **"SMTP Auth (true/false)"** value is set to **"true"**.



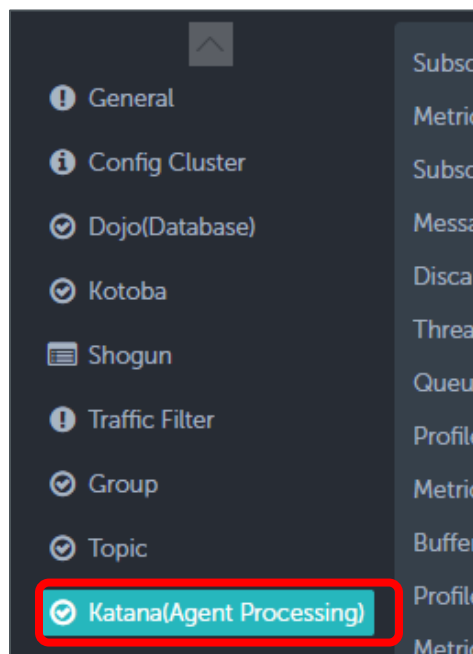
## ANALYTICS FOR CROWDSTRIKE CONFIGURATION

Initial configuration via the **TrueFort Configuration Interface** is necessary to connect the provisioned TrueFort instance with the CrowdStrike cloud. It can be accessed by navigating to <https://<Appliance IP>:9090> and logging in with your provided credentials.

### BUFFER TIME ADJUSTMENT

Before configuring a connection to CrowdStrike through this interface, ensure that the TrueFort instance's **Agent Processing Buffer Time** settings have been appropriately configured using the steps below.

1. Select the **Katana (Agent Processing)** tab located along the left-hand side of the screen.



2. Set the value of "Buffer Time (milliseconds)" to 1800000.
3. Click "Submit".

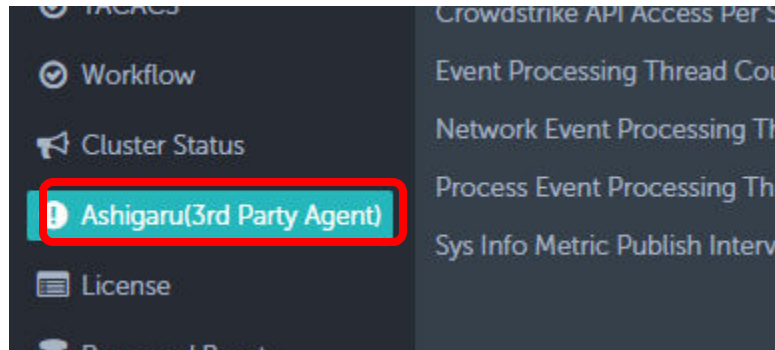
### CROWDSTRIKE CONNECTION

Initial connection to CrowdStrike can be made via one of two methods available from the Configuration Interface's **3<sup>rd</sup> Party Agent** settings – **uploading a credential file** or **manual input**.

#### UPLOADING A CREDENTIAL FILE

Customer credential files are generated during the initial steps of the CrowdStrike-TrueFort configuration process and are provisioned by TrueFort. They can be uploaded directly through the TrueFort Configuration Interface to initiate connection to the CrowdStrike cloud.

1. Select the **Ashigaru (3<sup>rd</sup> Party Agent)** tab located along the left-hand side of the screen.



2. Select the **CrowdStrike** option at the top of the screen using the provided radio button. Then, scroll down to the **Upload Credentials** section of the screen.

A screenshot of the 'Upload Credentials' section in the TrueFort Configuration Interface. At the top, there is a header 'Upload Credentials'. Below it is a large text input field. To the right of the input field are two buttons: 'Browse...' and 'Upload'. Below the input field, there is a label 'Restart Service:' followed by a checked checkbox. At the bottom right of the section, there are four buttons: 'Evaluate Login', 'Evaluate AWS', 'Submit', and 'Reset'. The interface has a dark theme.

3. Click the **Browse** button and select your provided credential file. Then, click the **Upload** button.
4. Ensure that **Restart Service** is checked.
5. Click the **Submit** button at the bottom of the screen.


## MANUAL INPUT


Alternatively, the necessary parameters can be manually defined in the absence of a credential file.

1. Select the **"Ashigaru (3<sup>rd</sup> Party Agent)"** tab located along the left-hand side of the screen.
2. Select the **CrowdStrike** option at the top of the screen using the provided radio button. This prompts the following screen:



Create Connection:


**TANIUM**


**CROWDSTRIKE**

Host:	
Query API Key:	
Password:	
Queue Url:	
AWS Credentials:	/home/bushido/components/ashigaru/credentials
Amazons3 Region:	
AWS_KEY:	
AWS_SECRET:	
SQS Message Topic:	sqsMessage
Proxy Host:	
Proxy Port:	
Proxy User:	
Proxy Pass:	
Proxy Enabled:	false
Proxy Protocol(lowercase):	
Purge Old Messages/Data:	true
Expiration Age (in ms):	3600000
Backup Data:	false
Learning Enabled:	false
Crowdstrike API Access Per Second:	250

- Configure the following required input fields.
  - Host** – falconapi.crowdstrike.com
  - Query API Key** – Falcon Query API Key
  - Password** – Falcon Query API Password
  - Queue Url** – AWS SQS Queue URL
  - AWS Credentials** – /home/bushido/components/ashigaru/credentials
  - Amazons3 Region** – S3 Bucket Region
  - AWS\_KEY** – AWS Key
  - AWS\_SECRET** – AWS Secret
  - Check Allowlist For Registering Agent** – True
  - CrowdStrike API Auth Type** – oAuth2
  - CIDs** – CIDs. Case sensitive
- Ensure that **Restart Service** is checked.
- Click **Submit**. The service will restart.



## CROWDSTRIKE-SPECIFIC DOMAIN AND AGENT GROUP

Successful connection to CrowdStrike through the TrueFort configuration interface will prompt the creation of a **CROWDSTRIKE-GENERAL** domain the TrueFort UI, with its own corresponding **Bushido Agent Group**. CrowdStrike-integrated agents will register to and appear under this Domain and Agent Group and can be managed and modified as necessary.

## APPLICATION SERVER ALLOWLISTING

Upon initial configuration, ANALYTICS will not start collecting information from the S3 bucket right away. By default, it will first search for an allowlist of servers within the S3 bucket to begin collecting telemetry from.

ANALYTICS' server allowlist requirement can be toggled off, but this is not recommended, as the sheer amount of data collected from the S3 bucket without an allowlist specified would be cumbersome.

To specify a server allowlist, use the TrueFort GUI to navigate to **"Admin > Application File Import"** and download the template sheet by clicking the **"Download"** button in the **"Export Template"** section. Use this template to configure a list of the applications in your environment to monitor with TrueFort.

Bear in mind the following while completing the template sheet:

1. On the **APPLICATIONS** tab of the import sheet, every column needs to be completed for each application entry.
  - Ensure that all entries in the **Region** column have also been defined in the **BUSHIDO REFERENCE DATA** tab.

	A	B	C	D	E	F	G
	Application Name	Organization	State	Type	Region	Team	Description
1	Sample Application	TrueFort	DEV	STATIC	North America	Bushido Admin Team	Example description.
2							
3							
4							

2. On the **SERVERS** tab, every column must be completed.
  - The **Role** and **Application Name** columns are mandatory for every server defined in this section.
  - Input the server's **FQDN** in the **IP** column.
  - The **Agent Type** for every server should be set to **"CROWDSTRIKE"**.
  - The **Domain** for every server should be set to **"BUSHIDO-GENERAL"**.


A	B	C	D	E	F
Agent Type	IP	Agent Id	Role	Application Name	Domain
CROWDSTRIKE	crowdstrike-redhat7		AD SERVER	Sample Application	BUSHIDO-GENERAL

3. The **BUSHIDO REFERENCE DATA** tab contains potential inputs for corresponding columns in the **APPLICATIONS** and **SERVERS** tabs.

A	B	C	D	E	F
State	Type	Region	Team	Domain	Agent Type
DEV	STATIC	South America	chrome_QA_DO_NOT_DELETE	BUSHIDO-GENERAL	NATIVEAGENT
UAT		Weehawken	Bushido Admin Team	BUSHIDO-GENERAL	CROWDSTRIKE
PROD		North America		PXY	TANUM
				QA	
				QA3	
				BUSHIDO-GENERAL	

4. The **ORGANIZATIONS** tab allows users to configure organization definitions and components as required.

A	B	C	D	E	F	G	H	I	J
Organization definition	Parent	Allow applications	Description	Organization	Parent organization	Type	Code	Description	
DIVISION		TRUE	QA testing	TrueFort		ORGANIZATION	001	TrueFort	
SUB-DIVISION		TRUE	QA testing	QA	TrueFort	DEPT	QA	QA Desc	
DEPARTMENT	BUSINESS UNIT	TRUE	Department	automation	QA	SUB-DEPARTMENT	QA	QA Desc	
SUB-DEPARTMENT	DEPT	TRUE	QA testing						
BUSINESS UNIT	ORGANIZATION	TRUE	Business Unit						
ORGANIZATION		TRUE	Organization						
AGENCY		TRUE	QA testing						
SUB-GROUP	DEPT	FALSE	QA testing						
TESTORG		TRUE	QA testing						
DEPT	ORGANIZATION	TRUE	QA testing						

After filling out the template, import it to the ANALYTICS appliance by clicking the  button on the **Application Import** page and selecting the completed template.

Then, click the  button. On importing the file, ANALYTICS:

- Fetches the AID of the application servers whose IP addresses are listed in the Excel file using the Falcon API and creates an allowlist of servers to be monitored
- Registers the applications, servers, and their associated information on the ANALYTICS appliance.

Once ANALYTICS is configured, it collects the following information for the specified servers that are a part of the allowlist:

- NetworkCloseIPx
- NetworkConnectIPx
- NetworkListenIPx
- NetworkReceiveAcceptIPX
- UserLogon/Logoff/UserIdentity
- FirewallXXXX

The following is an example of telemetry gathered by a CrowdStrike agent running on a server:

NetworkConnectIPV4

```
{
  "ConfigBuild": "1007.3.0006806.1",
  "ConfigStateHash": "3095529655",
  "ConnectionDirection": "0",
  "ConnectionFlags": "0",
  "ContextProcessId": "170283095539",
  "ContextTimeStamp": "1526488261.445",
  "EffectiveTransmissionClass": "3",
  "Entitlements": "15",
  "InContext": "0",
  "LocalAddressIP4": "10.179.144.11",
```

```

"LocalPort": "28881",
"Protocol": "6",
"RemoteAddressIP4": "13.68.93.109",
"RemotePort": "443",
"aid": "0d7e3ad16a0740d546d36a626f78aa44",
"aip": "47.22.68.21",
"cid": "532b3ef566b14068a416fd81b0a16acd",
"event_platform": "Win",
"event_simpleName": "NetworkConnectIP4",
"id": "8569a78a-5926-11e8-aa4e-06aef53c5872",
"name": "NetworkConnectIP4V5",
"timestamp": "1526488261672"
}

```

#### ProcessRollupX

```

{
  "AuthenticationId": "999",
  "CommandLine": "C:\\WINDOWS\\System32\\sihclient.exe",
  "ConfigBuild": "1007.3.0006806.1",
  "ConfigStateHash": "3095529655",
  "EffectiveTransmissionClass": "3",
  "Entitlements": "15",
  "ImageFileName": "\\Device\\HarddiskVolume3\\Windows\\System32\\SIHClient.exe",
  "ImageSubsystem": "3",
  "IntegrityLevel": "16384",
  "MD5HashData": "dbf290ed70b035753e62ad22e6ef0bba",
  "ParentAuthenticationId": "999",
  "ParentProcessId": "137496304121",
  "ProcessCreateFlags": "525316",
  "ProcessEndTime": "",
  "ProcessParameterFlags": "16385",
  "ProcessStartTime": "1526488261.231",
  "ProcessSxsFlags": "64",
  "RawProcessId": "1716",
  "SHA1HashData": "9ed77e9b8e1250e5624a5607de52ea4fc9069a2e",

```



```

    "SHA256HashData":
"50b0f23134dc14d19a524bacff266e87b67605a9faccaa75f85a2e431f73608",
    "SourceProcessId": "137496304121",
    "SourceThreadId": "4818542840231",
    "TargetProcessId": "170283095539",
    "TokenType": "1",
    "UserSid": "S-1-5-18",
    "WindowFlags": "128",
    "aid": "0d7e3ad16a0740d546d36a626f78aa44",
    "aip": "47.22.68.21",
    "cid": "532b3ef566b14068a416fd81b0a16acd",
    "event_platform": "Win",
    "event_simpleName": "ProcessRollup2",
    "id": "8569a45c-5926-11e8-aa4e-06aef53c5872",
    "name": "ProcessRollup2V8",
    "timestamp": "1526488261672"
}

```

ANALYTICS processes the collected information as follows:

1. From the network information, ANALYTICS fetches the aid. *i.e. "aid": "0d7e3ad16a0740d546d36a626f78aa44"*
2. ANALYTICS then runs the Falcon API to get the details of the server with the fetched AID.
3. It then checks if the corresponding server is present in the server allowlist.
4. If the server is present in the allowlist, it checks if it is registered to the ANALYTICS appliance. If not, ANALYTICS creates a static agent for the server using the information fetched via the Falcon API.
5. If the application, role, region, and organization related to the server are specified, ANALYTICS assigns agents to the specified applications with associated roles.
6. ANALYTICS then creates a profile for the CrowdStrike agent using the telemetry collected from the application servers.

## CROWDSTRIKE APIS

CrowdStrike offers multiple APIs, but ANALYTICS uses the following two APIs for collecting and processing the data:

### Falcon Data Replicator - Ingest and correlate data

Falcon Data Replicator gives security teams the ability to export complete endpoint data from the Falcon agent to their environment for independent analysis. It provides customers with the means to ingest the data from the Falcon platform into their local data warehouse and correlate it with logs collected from other sources.



### Falcon Query - Manage, investigate, and respond

The Falcon Query API allows you to upload IOCs for monitoring; obtain device information about systems with the Falcon agent installed; search for processes by indicators of attack (IOAs), IOCs, and related processes; and manage detection status.

## APPENDIX A – KEY REALM INTERFACE DIFFERENTIATORS IN ANALYTICS

The **Realm** screen provides a graphical representation of network connections being made to and from applications and workloads registered in TrueFort. However, the exact nature of these displayed connections differs when considering not only the **different flavors of TrueFort installation** but the **installed agent**, as well.

In **TrueFort Protect**, connections involving workloads with the **TrueFort Advanced Agent** installed display in real time. The colored line illustrating the connection in the **Realm** interface will appear as soon as the connection has been established and will disappear once that connection has been closed.

This is not the case in instances where TrueFort employs near-real time visibility, such as with workloads monitored by third-party solutions integrated with **TrueFort Analytics**.

In TrueFort's **CrowdStrike Integration**, the Realm screen illustrates **network connections that were initiated within the past 1 hour cycle**, as only **ACCEPT** and **INITIATED** events are detected. This is **not** a real-time display and will show **all** connections initiated within the cycle, regardless of whether the connection was closed or not in the interim.

