



Finding **threats** on your network faster.

Firebug in the Mitre Framework

Connecting Firebug, Engage, and Att&ck

This document will discuss Firebug’s current use cases and how they integrate with the Mitre cybersecurity frameworks, specifically Mitre Engage and Mitre Att&ck. We will first outline the sample use cases for Firebug, then the Mitre Engage Framework and where Firebug sits inside it, and then we will dive deeper to identify where Firebug can provide additional visibility with regards to the Att&ck framework.

Summary Mapping

■ : Coverage ■ : Partial Coverage

Engage Positioning

Prepare	Expose		Affect			Elicit		Understand
Plan	Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate	Analyze
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring ■	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis ■	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

Att&ck Positioning - Part 1

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs
Gather Victim Network Information (5)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)	Create Account (3)	Domain Policy Modification (2)	Direct Volume Access
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Escape to Host	Execution Guardrails (1)
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	Exploitation for Defense Evasion
Search Victim-Owned Websites			System Services (2)	External Remote Services	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)
			User Execution (3)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hide Artifacts (9)
			Windows Management Instrumentation	Implant Internal Image	Process Injection (11)	Hijack Execution Flow (11)
				Modify Authentication Process (4)	Scheduled Task/Job (6)	Impair Defenses (9)
				Office Application Startup (6)	Valid Accounts (4)	Indicator Removal on Host (6)
				Pre-OS Boot (5)		Indirect Command Execution
				Scheduled Task/Job (6)		Masquerading (7)
				Server Software Component (4)		Modify Authentication Process (4)
				Traffic Signaling (1)		Modify Cloud Compute Infrastructure (4)
				Valid Accounts (4)		Modify Registry
						Modify System Image (2)
						Network Boundary Bridging (1)
						Obfuscated Files or Information (6)
						Pre-OS Boot (5)
						Process Injection (11)
						Reflective Code Loading
						Rogue Domain Controller
						Rootkit
						Signed Binary Proxy Execution (13)

: Coverage : Partial Coverage

Att&ck Positioning - Part 2

Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Adversary-in-the-Middle (2) ■	Account Discovery (4) ■	Exploitation of Remote Services ■	Adversary-in-the-Middle (2) ■	Application Layer Protocol (4) ■	Automated Exfiltration (1) ■	Account Access Removal
Brute Force (4) ■	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3) ■	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores (5) ■	Browser Bookmark Discovery	Lateral Tool Transfer ■	Audio Capture	Data Encoding (2) ■	Exfiltration Over Alternative Protocol (3) ■	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2) ■	Automated Collection ■	Data Obfuscation (3) ■	Exfiltration Over C2 Channel ■	Data Manipulation (3) ■
Forced Authentication	Cloud Service Dashboard	Remote Services (6) ■	Browser Session Hijacking	Dynamic Resolution (3) ■	Exfiltration Over Other Network Medium (1) ■	Defacement (2) ■
Forge Web Credentials (2) ■	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2) ■	Exfiltration Over Physical Medium (1) ■	Disk Wipe (2) ■
Input Capture (4) ■	Cloud Storage Object Discovery	Software Deployment Tools ■	Data from Cloud Storage Object	Fallback Channels ■	Exfiltration Over Web Service (2) ■	Endpoint Denial of Service (4) ■
Modify Authentication Process (4) ■	Container and Resource Discovery	Taint Shared Content ■	Data from Configuration Repository (2) ■	Ingress Tool Transfer ■	Scheduled Transfer ■	Firmware Corruption
Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material (4) ■	Data from Information Repositories (3) ■	Multi-Stage Channels ■	Transfer Data to Cloud Account ■	Inhibit System Recovery
OS Credential Dumping (8) ■	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol ■		Network Denial of Service (2) ■
Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive ■	Non-Standard Port ■		Resource Hijacking
Steal or Forge Kerberos Tickets (4) ■	Network Service Scanning ■		Data from Removable Media	Protocol Tunneling ■		Service Stop
Steal Web Session Cookie	Network Share Discovery		Data Staged (2) ■	Proxy (4) ■		System Shutdown/Reboot
Two-Factor Authentication Interception	Network Sniffing		Email Collection (3) ■	Remote Access Software ■		
Unsecured Credentials (7) ■	Password Policy Discovery		Input Capture (4) ■	Traffic Signaling (1) ■		
	Peripheral Device Discovery		Screen Capture	Web Service (3) ■		
	Permission Groups Discovery (3) ■		Video Capture			
	Process Discovery					
	Query Registry					
	Remote System Discovery					
	Software Discovery (1) ■					
	System Information Discovery					
	System Location Discovery (1) ■					
	System Network Configuration Discovery (1) ■					
	System Network Connections Discovery					
	System Owner/User Discovery					
	System Service Discovery					
	System Time Discovery					
	Virtualization/Sandbox Evasion (3) ■					

■ : Coverage ■ : Partial Coverage

Firebug Use Cases

Firebug is by design an active network cyber security tool, and as such works best in a threat hunting environment with threat hunting workflows. At its most basic form, Firebug is a threat hunting lead generator with specific focus on abnormal or unusual network traffic, specifically with relation to behaviours (and protocols) that are related to lateral movement and early stage internal reconnaissance. Firebug's unique method of handling network data also means that it does not limit its detection capability to attacks, it is also useful in exposing unwanted user behaviour and overall misconfigurations. Firebug's sample use cases are indicative of this lead-generation concept and workflow, and such a capability precludes simple association of use cases with Att&ck framework strategies (as Firebug does not detect these, it provides a platform to hunt them down, ie it allows an analyst to expose those threats and identify where on the killchain attackers are).

General Use Case

Firebug in general is used to provide:

- Information on security relevant issues inside client networks from the perspective of the hosting network tap.
- The ability to identify abnormal and potentially unwanted usage of lateral movement protocols (SMB, WinRM, LDAP)
- The ability to identify issues in outbound traffic regardless of the existence of outbound firewall policy (or more likely the lack thereof)

These in turn provide:

- Visibility of network issues (misconfigurations, attackers, insider threat) from a security standpoint.
- The ability to identify, classify, and react to abuses and misuses of machines and protocols (ie, bad user behaviour) inside selected networks.
- The ability to identify, classify, and react to outbound events (ie exfiltration, beaconing, unwanted service usage, etc) in selected networks regardless of firewall capability.

These activities through both Firebug's statistic engine and the simple fact that it gives focused attention to network events aligns with Firebug's placement in the Expose elements of the Engage matrix, specifically in Collection and Detection (see Mitre Expose below). The broad detective capability of Firebug allows for more subtle abuses of machines and protocol that go undetected by policy driven or tool detecting threat model security applications. Specific targets here are attackers trying to remain undetected by performing off-the-land attack styles.

Unwanted Service Detection Use Case

Firebug can be used to identify unwanted and unusual service usage inside selected networks. For example:

- Firebug was deployed between BYOD network and internet gateway in Client network
- Client did not have good visibility of outbound traffic from BYOD network
- Client had reason to believe users were using VPN/remote access software to bypass policy
- Firebug was able to detect these from a combination of unusual profile (VPN), rare usage (remote access), and target destinations (abnormal geolocations).
- Reporting was able to allow the client to rectify these issues.

Firebug was able to detect this due to the pDNS capability inside Firebug acting in concert with the statistical deviation detection system at Firebug's core. The behaviour of users using VPN and remote access software was detectable due to their rarity when compared with usual user actions. The fact that domains the remote access tools used were associated with known services was leveraged to extract these events from the Firebug log output. Firebug performs in similar fashion when used to detect attacker behaviour via IOC FQDNs (see Beaconing and IOC detection below). Firebug collects user actions, associates them with the used DNS queries via the pDNS system, and then forwards them as logs as the statistical detection system dictates. This allows for refined and targeted event generation for abnormal behaviour that correlates with DNS entries. This exists across both the Network Monitoring and Network Analysis cells in the Engage Matrix (see Mitre Engage).

Beaconing and IOC Detection

Firebug can be used to identify actor beaconing, exfiltration, and C2 traffic by virtue of its unusual nature and confirmed by known IOCs. One such example is the following:

- Firebug was deployed between Client VPN and Client core network.
- Firebug detected abnormal HTTPS behaviour emanating from the VPN network and passing outbound in the direction of the core switch.
- Firebug was able to identify the remote endpoint FQDN and generate events accordingly.
- Events were correlated with external threat intelligence data and remote FQDN was found to be a known IOC of known threat (in this case a C2 server)
- Event was then acted on, affected machines were identified from event data and isolated, and mitigation steps were taken.

In this case the attacker had not yet begun using the C2 connection, it was still in a beaconing phase. This behaviour however was different enough from HTTPS traffic in the VPN network that Firebug was able to identify its novelty and need to generate events for it. This allowed defenders to take corrective action before the attacker was able to perform further actions.

IR/Post IR Lateral Movement Detection

Firebug’s rapid time to normalisation allows for drop-in deployments of the system into compromised environments. Firebug has been used in IR scenarios to provide leads in the investigation process as part of a reactive threat hunting scenario. One such example is the following:

- Firebug was deployed in the DMZ network of Client affected (and compromised by) Log4Shell attack.
- Firebug was able to rapidly provide data on potential lateral movement, common talkers, and any LDAP protocol abuses (in Log4Shell’s case, outbound LDAP).
- Firebug allowed the investigative team to rapidly identify and classify DMZ to broader network communications of concern.
- Firebug ultimately gave Client confidence at the end of engagement that the network had been secured from the immediate threat and that no further lateral movement was at that point occurring.

Mitre Engage

The Mitre Engage Framework (found here <https://engage.mitre.org/matrix>) is a framework that covers the Active Cyber Security strategic cycle. It covers the three main pillars of the Active process, identifying attackers early in the environment, actively engaging attackers in the environment in both direct and indirect methods, and crafting a realistic set of countermeasures to ensure attackers engage with decoys and countermeasures and provide maximum intelligence on their goals and tactics. It also covers the bookending steps in the Active cycle, including preparation for attacks and post attack analysis.



The Engage Matrix

The Engage Matrix displays the relationships between the various Strategic and Engagement Goals, Approaches, and Activities. Goals are found at the top row of Engage. Each Approach and Activity is assigned to a goal. Approaches are the next row down. All Activities are assigned to an Approach. Finally, Activities make up the remaining entries in Engage. Strategic Actions can be found in the far right and far left columns of Engage. Engagement Actions can be found in the central columns. By bookending Engagements Actions with Strategic Planning and Analysis, we hope that MITRE Engage™ will help organizations better plan and implement real-world adversary engagement strategies and advance the cybersecurity ecosystem.

For a full exploration of the various components of MITRE Engage™, click here.

Legend	
Engagement Actions Taken Against Your Adversary	White
Strategic Actions Taken to Support Operational Strategy	Gray

Prepare	Expose		Affect			Elicit		Understand
Planning	Collection	Detection	Prevention	Direction	Disruption	Reassurance	Motivation	Analysis
Define Exit Criteria	API Monitoring	Decoy Artifacts and Systems	Baseline	Decoy Artifacts and Systems	Decoy Artifacts and Systems	Application Diversity	Application Diversity	Distill Intelligence
Develop Threat Model	Network Monitoring	Detonate Malware	Hardware Manipulation	Detonate Malware	Isolation	Artifact Diversity	Artifact Diversity	Hotwash
Persona Creation	Software Manipulation	Network Analysis	Isolation	Email Manipulation	Network Manipulation	Burn-In	Detonate Malware	Inform Threat Model
Strategic Goal	System Activity Monitoring		Network Manipulation	Migrate Attack Vector	Software Manipulation	Email Manipulation	Information Manipulation	Refine Operation Activities
Storyboarding			Security Controls	Network Manipulation		Information Manipulation	Personas	
				Peripheral Management		Network Diversity	Network Diversity	
				Security Controls		Peripheral Management		
				Software Manipulation		Pocket Litter		

Firebug falls into the first of the three pillars, Expose, for early detection of malicious actors on the network via active threat hunting and intelligence usage. Firebug performance fits into both Network Monitoring activities (for collection of network data) and Network Analysis activities (for determination of network anomalies requiring investigation). Firebug can be classified as an “internal intelligence” system, as it provides intelligence on network events from selected networks that, when combined with additional intelligence and threat hunting, can provide a potent cyber security capability beyond passive automated response tools.

The screenshot shows the MITRE Engage web interface. At the top is a dark blue navigation bar with the MITRE Engage logo and various menu items like 'Getting Started', 'Matrix', 'Goals', 'Approaches', 'Activities', 'ATT&CK® Mapping', and 'Resources'. A search bar is on the right. Below the navigation bar is a light green banner with a welcome message and a feedback email address. The main content area has a breadcrumb trail 'Home > Activities' and a heading 'Network Monitoring'. Below the heading is a sub-heading 'Monitor network traffic in order to detect adversary activity.' followed by a paragraph describing network monitoring. A 'Details' sidebar on the right shows 'ID: EAC0002', 'Type: Engagement', 'Goals: Expose', and 'Approaches: Collection'. Below this is a table with two columns: 'ATT&CK® Tactics' and 'Adversary Vulnerability Presented'. The table lists three rows of tactics and their corresponding vulnerabilities. At the bottom of the page is a dark blue footer with the MITRE logo, copyright information, and links for 'Privacy Policy', 'Terms of Use', 'Connect with Us', and '@MITREcorp'.

Each of these activities break down into a series of attacker vulnerabilities, or ways the attacker exposes themselves to a defender.

These are aligned with a series of Att&ck framework attacker tactics, like for example the Command and Control tactic. These are the activities in general that describe attacker kill chains in broad strokes.

MITRE | ATT&CK

[Matrices](#)
[Tactics](#)
[Techniques](#)
[Data Sources](#)
[Mitigations](#)
[Groups](#)
[Software](#)
[Resources](#)
[Blog](#)
[Contribute](#)

ATT&CKcon 3.0 will be March 29, 30 2022 in McLean, VA! Submit to our CFP by 11/23 [here](#)

TACTICS

- Enterprise
- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact
- Mobile

Home > Tactics > Enterprise > Command and Control

Command and Control

The adversary is trying to communicate with compromised systems to control them.

ID: TA0011
 Created: 17 October 2018
 Last Modified: 19 July 2019
[Version Permalink](#)

Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

Techniques

Techniques: 16

ID	Name	Description
T1071	Application Layer Protocol	Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.
	.001 Web Protocols	Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.
	.002 File Transfer Protocols	Adversaries may communicate using application layer protocols associated with transferring files to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.
	.003 Mail Protocols	Adversaries may communicate using application layer protocols associated with electronic mail delivery to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.
	.004 DNS	Adversaries may communicate using the Domain Name System (DNS) application layer protocol to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.
T1092	Communication Through	Adversaries can perform command and control between compromised hosts on potentially disconnected networks using removable media to transfer commands from system to system. Both systems would need to be compromised, with the likelihood that an Internet-connected system was compromised

Each of these directly incorporate techniques of the Att&ck framework itself, the final state of the Engage to Att&ck mapping. These mappings do not identify which Att&ck strategies an active solution or strategy “detects” or “covers”, but rather which locations in the Att&ck kill chain each element can expose. This is important in the threat hunting methodology, as the approach is to identify where an attacker may be in the kill chain from events that are necessarily broader than what can be matched to any given Att&ck technique or subtechnique. In short: We’re not interested in detecting specific techniques, we’re trying to expose their user’s existence.

Mitre Att&ck

For completeness, we have attached below a table that presents an Engage to Att&ck passthrough that gives a broad level understanding of how Firebug “maps” from one to the other. This should give some idea of what Firebug is capable of doing from an Att&ck standpoint, and where it can fit into your security architecture.

Attack Framework Mapping

ENGAGE Activity	ATT&CK Tactic	ATT&CK Element	Covered?	How?
Network Monitoring // Network Analysis	Command & Control	T1701 App Level Protocols	Yes	Firebug can detect sustained abnormal uses of protocols, even when encrypted
		T1132.002 Data Encoding: Non-Standard	Partial	Can detect deviations from normal protocol behaviour
		T1001.001 Data Obfuscation: Junk Data	Yes	Can detect deviations from normal protocol behaviour
		T1001.003 Data Obfuscation: Protocol Impersonation	Yes	Can detect deviations from normal protocol behaviour
		T1568 Dynamic Resolution	Yes	Firebug is inherently agnostic about source and destinations, consistent abnormal behaviour is still detectable.
		T1573 Encrypted Channel	Partial	Firebug can detect abnormal uses of encrypted channels, though not what they are being used for
		T1008 Fallback Channels	Partial	Firebug is inherently agnostic about source and destinations, consistent abnormal behaviour is still detectable.
		T1105 Ingress Tool Transfer	Yes	Firebug can detect abnormal file transfers.
		T1104 Multi Stage Channels	Yes	Firebug is inherently agnostic about source and destinations, consistent abnormal behaviour is still detectable.
		T1095 Non-Application Layer Protocol	Yes	Firebug works on the IP Protocol and catches all abnormal traffic above IP.
		T1571 Non-Standard Port	Partial	Firebug can detect when standard ports are being used inappropriately, as may

				occur when a standard port is being used for a non-standard protocol
		T1572 Protocol Tunnelling	Yes	Firebug can detect tunnelling in DNS, ICMP, and HTTPS.
		T1219 Remote Access Software	Yes	Firebug has detected unauthorised uses of TeamViewer and similar, and can be used to detect such.
		T1102 Web Service	Partial	Firebug can detect abnormal usage of web services, but cannot detect use if the ringfence regularly uses web service in similar fashion
Network Monitoring	Lateral Movement	T1210 Exploitation of Remote Services	Yes	Firebug can detect the change in behaviour of remote services as they are compromised
		T1570 Lateral Tool Transfer	Yes	Firebug can detect abnormal file transfers.
		T1563 Remote Session Hijacking	Yes	Firebug can detect abnormal use of sessions, even when the session has been persistent for some time
		T1021 Remote Services	Yes	Firebug can detect the change in behaviour of remote services as they are used abnormally
		T1072 Software Deployment Tools	Yes	Firebug can detect the change in behaviour of remote services as they are used abnormally
		T1080 Taint Shared Content	Partial	Firebug can detect abnormal behaviour, so if the shared content now behaves differently Firebug can detect the change.
Network Monitoring	Impact	T1498 Network DoS	Yes	Firebug can detect volumetric DoS and DDoS attacks.
Network Monitoring // Network Analysis	Collection	T1557 Adversary in the Middle	Yes	Firebug can detect when attackers are impersonating services like SMB to perform AitM attacks.
		T1119 Automated Collection	Partial	Bulk data replication over networks is detectable by Firebug
		T1039 Data from Network Shared Drive	Yes	Firebug can detect abnormal file transfers.
Network Monitoring	Defense Evasion	T1197 BITS Jobs	Yes	Firebug can detect abnormal file transfers.

		T1562.004 Disable or Modify System Firewall	Yes	Firebug can detect violations of firewall policy due to abnormality of non-policy behaviour
		T1562.007 Disable or Modify Cloud Firewall	Yes	Firebug can detect violations of firewall policy due to abnormality of non-policy behaviour
		T1599 Network Boundary Bridging	Yes	Firebug can detect violations of firewall policy due to abnormality of non-policy behaviour
		T1027.006 HTML Smuggling	Partial	Firebug can detect abnormal usage of HTTP/S
		T1542.005 TFTP Boot	Partial	Firebug can detect abnormal file transfers.
		T1207 Rogue Domain Controller	Yes	Firebug can detect abnormal SMB/LDAP actors, and new
Network Monitoring // Network Analysis	Exfiltration	T1020 Automated Exfiltration	Partial	Bulk data replication over networks is detectable by Firebug
		T1048 Exfiltration over Alternative Protocol	Yes	Firebug can detect abnormal file transfers.
		T1041 Exfiltration over C2 Channel	Yes	Firebug can detect abnormal file transfers.
		T1567 Exfiltration over Web Service	Yes	Firebug can detect abnormal file transfers.
		T1029 Scheduled Transfer	Yes	Firebug can detect abnormal file transfers.
		1537 Transfer Data to Cloud Account	Yes	Firebug can detect abnormal file transfers.

Document History

Document Version	Author Name	Comment	Date
0.1	Stefan Prandl	Initial Version	Tuesday, 16 November 2021
1.0	Stefan Prandl	Added Table	Tuesday, 23 November 2021
2.0	Stefan Prandl	Added Use Cases	Thursday, 7 April 2022
2.1	Stefan Prandl	Added Summary	Friday, 8 April 2022