DATA SHEET

FortiClient Forensic Service

Analysis of cyber security events in a FortiClient deployment.

FortiClient Forensic Service provides analysis to help endpoint customers respond to and recover from cyber incidents. For each engagement, forensic analysts from Fortinet's FortiGuard Labs will assist in the collection, examination, and presentation of digital evidence, including a final, detailed report. FortiClient subscriptions that include Forensic Services entitle the customer to call on these forensic experts whenever an event happens, offloading internal teams and accelerating investigations by analysts deeply familiar with the tools of endpoint security.

FEATURES

Collection

Collecting disk artifacts and memory snapshots that may be relevant to the investigation. Collections are conducted securely via a remote agent with minimal customer interaction.

Examination

Examining file system contents, processing log files, and extracting statistical results to prioritize high value items for analysis.

Analysis

Analyzing targeted digital evidence to determine the initial attack vector, establish timeline of malicious activity, and identify the extent of compromise.

Reporting

Synthesizing the findings in a high-level executive summary with details on remediation recommendations.

Forensic Service Value

The service helps identify and mitigate potential risks including:

- Affected applications, networks, systems, and user accounts
- Malicious software and vulnerabilities
- Indicators of Compromise
- Root Cause Analysis
- Lateral Movement

Benefits

- Advanced skills and expertise of FortiClient product experts
- Faster analysis of events
- Detailed analysis of the digital evidence
- Initial attack vector, timeline of activity, and extent of compromise
- Remediation steps

SERVICE HIGHLIGHTS

Report and recommend actions

The report will provide details on the attack timeline and the root cause analysis. The report will include an executive summary explaining the major findings of the investigations, including the key takeaways and recommendations. The body of the report delves into each type of analysis performed (as outlined in previous question) as well as highlighting the Indicators of Compromise, list of affected computers and user accounts (when appropriate).

Respond and recover from cyber incidents

The Forensic Service adds value by helping clients respond to and recover from cyber incidents. Forensic analysis reveals how a malicious actor breached the network and identifies all affected systems. The delivery of threat intelligence and remediation recommendations can help an enterprise to quickly move back to normal day-to-day business.

Identify current and past attacker activity

With the Forensic Service, past attacker activity can be identified. Typically, forensic analysis is conducted on endpoints that have been identified as potentially or confirmed compromised. A sophisticated timeline can be created to identify when malicious files first appeared on disk, and if and when certain sensitive files were accessed by a malicious actor. Correlated the timeline with event logs would show when a malicious actor logged into the system, and when they moved laterally.

Tailor a comprehensive analysis

The type of analysis is tailored depending on the necessity of the case. Depending on the operating system, the available artifacts will differ. For the Windows operating system, the type of analysis can be any combination of the following:

- Persistence Analysis
- Program Execution
- Shell Item Forensics
- Windows Event Log Analysis
- Timeline Analysis
- Browser Application Forensics
- Memory Forensic
- Malware Analysis

Collect broad ranging artifacts

To conduct the above mentioned analyses, a number of system artifacts are collected.

- Registry Hives
- Prefetch Files
- System Resource Usage Database
- Jump List and LNK Files
- Event Log files
- Browser History
- Windows Recycle Bin
- Memory Snapshot

ORDER INFORMATION

	SKU	DESCRIPTION
PER ENDPOINT		
VPN/ZTNA Agent plus FortiGuard Forensics Subscription	FC1-10-EMS05-537-01-DD	FortiClient VPN/ZTNA Agent Subscriptions (EMS hosted by FortiCloud) plus FortiGuard Forensics with FortiCare Premium for 25 endpoints.
	FC2-10-EMS05-537-01-DD	FortiClient VPN/ZTNA Agent Subscriptions (EMS hosted by FortiCloud) plus FortiGuard Forensics with FortiCare Premium for 500 endpoints.
	FC3-10-EMS05-537-01-DD	FortiClient VPN/ZTNA Agent Subscriptions (EMS hosted by FortiCloud) plus FortiGuard Forensics with FortiCare Premium for 2000 endpoints.
	FC4-10-EMS05-537-01-DD	FortiClient VPN/ZTNA Agent Subscriptions (EMS hosted by FortiCloud) plus FortiGuard Forensics with FortiCare Premium for 10 000 endpoints.
ZTNA/VPN, EPP/ATP Plus Forensics	FC1-10-EMS05-538-01-DD	FortiClient VPN/ZTNA Agent and EPP/APT Subscriptions (EMS hosted by FortiCloud) plus FortiGuard Forensics with FortiCare Premium for 25 endpoints.
	FC2-10-EMS05-538-01-DD	FortiClient VPN/ZTNA Agent and EPP/APT Subscriptions (EMS hosted by FortiCloud) plus FortiGuard Forensics with FortiCare Premium for 500 endpoints.
	FC3-10-EMS05-538-01-DD	FortiClient VPN/ZTNA Agent and EPP/APT Subscriptions (EMS hosted by FortiCloud) plus FortiGuard Forensics with FortiCare Premium for 2000 endpoints.
	FC4-10-EMS05-538-01-DD	FortiClient VPN/ZTNA Agent and EPP/APT Subscriptions (EMS hosted by FortiCloud) plus FortiGuard Forensics with FortiCare Premium for 10 000 endpoints.
Managed FortiClient Plus Forensics	FC1-10-EMS05-539-01-DD	Managed FortiClient VPN/ZTNA Agent and EPP/APT Subscriptions (EMS hosted by FortiCloud) plus FortiGuard Forensics with FortiCare Premium for 25 endpoints.
	FC2-10-EMS05-539-01-DD	Managed FortiClient VPN/ZTNA Agent and EPP/APT Subscriptions (EMS hosted by FortiCloud) plus FortiGuard Forensics with FortiCare Premium for 500 endpoints.
	FC3-10-EMS05-539-01-DD	Managed FortiClient VPN/ZTNA Agent and EPP/APT Subscriptions (EMS hosted by FortiCloud) plus FortiGuard Forensics with FortiCare Premium for 2000 endpoints.
	FC4-10-EMS05-539-01-DD	Managed FortiClient VPN/ZTNA Agent and EPP/APT Subscriptions (EMS hosted by FortiCloud) plus FortiGuard Forensics with FortiCare Premium for 10 000 endpoints.
PER-USER LICENSE		*Check for availability before ordering
ZTNA/VPN Plus Forensics	FC2-10-EMS05-557-02-DD	FortiClient VPN/ZTNA Agent plus FortiGuard Forensics Subscription for 100-499 Users. Includes EMS hosted by FortiCloud with FortiCare Premium.
	FC3-10-EMS05-557-02-DD	FortiClient VPN/ZTNA Agent plus FortiGuard Forensics Subscription for 500-1999 Users. Includes EMS hosted by FortiCloud with FortiCare Premium.
	FC4-10-EMS05-557-02-DD	FortiClient VPN/ZTNA Agent plus FortiGuard Forensics Subscription for 2000-9999 Users. Includes EMS hosted by FortiCloud with FortiCare Premium.
	FC5-10-EMS05-557-02-DD	FortiClient VPN/ZTNA Agent plus FortiGuard Forensics Subscription for 10 000+ Users. Includes EMS hosted by FortiCloud with FortiCare Premium.
ZTNA/VPN, EPP/ATP Plus Forensics	FC2-10-EMS05-558-02-DD	FortiClient VPN/ZTNA and EPP/ATP Agent plus FortiGuard Forensics Subscription for 100-499 Users. Includes EMS hosted by FortiCloud with FortiCare Premium.
	FC3-10-EMS05-558-02-DD	FortiClient VPN/ZTNA and EPP/ATP Agent plus FortiGuard Forensics Subscription for 500-1999 Users. Includes EMS hosted by FortiCloud with FortiCare Premium.
	FC4-10-EMS05-558-02-DD	FortiClient VPN/ZTNA and EPP/ATP Agent plus FortiGuard Forensics Subscription for 2000-9999 Users. Includes EMS hosted by FortiCloud with FortiCare Premium.
	FC5-10-EMS05-558-02-DD	FortiClient VPN/ZTNA and EPP/ATP Agent plus FortiGuard Forensics Subscription for 10 000+ Users. Includes EMS hosted by FortiCloud with FortiCare Premium.
Managed FortiClient Plus Forensics	FC2-10-EMS05-556-02-DD	Managed FortiClient plus FortiGuard Forensic Subscription for 100-499 Users. Includes VPN/ZTNA Agent, EPP/APT, Deployment Assistance, Endpoint Monitoring Service, Forensics and FortiClient Cloud with FortiCare Premium.
	FC3-10-EMS05-556-02-DD	Managed FortiClient plus FortiGuard Forensic Subscription for 500-1,999 Users. Includes VPN/ZTNA Agent, EPP/APT, Deployment Assistance, Endpoint Monitoring Service, Forensics and FortiClient Cloud with FortiCare Premium.
	FC4-10-EMS05-556-02-DD	Managed FortiClient plus FortiGuard Forensic Subscription for 2,000-9,999 Users. Includes VPN/ZTNA Agent, EPP/APT, Deployment Assistance, Endpoint Monitoring Service, Forensics and FortiClient Cloud with FortiCare Premium.
	FC5-10-EMS05-556-02-DD	Managed FortiClient plus FortiGuard Forensic Subscription for 10,000+ Users. Includes VPN/ZTNA Agent, EPP/APT, Deployment Assistance, Endpoint Monitoring Service, Forensics and FortiClient Cloud with FortiCare Premium.

FCFF-DAT-R01-20220713