SOLUTION BRIEF

# Unify Detection and Response across Your Entire Network with FortiEDR, FortiNDR Cloud, and FortiGate NGFW

## Executive Summary

To avoid detection, attackers continuously evolve their techniques, often combining malicious activity with routing network traffic and using encrypted channels to exfiltrate data, making it challenging for defenders to discover and distinguish between legitimate and malicious activities. By analyzing suspicious activity from multiple perspectives, specifically network and endpoint data, security operations center (SOC) analysts gain better insights and higher-fidelity detections that shed light on unknown attacks so they can halt evolving threats quickly.

168

On average, it takes at least 168 hours for security teams to identify network threats, and many still go undetected.[1]

## Move from Siloed to Streamlined Visibility and Investigations

Investigating alerts often requires significant manual effort, working across multiple solutions searching for additional context to help prioritize and determine next steps. This results in longer investigation and response times, prolonging an attacker's ability to cause damage throughout the network.

While these arduous, time-consuming investigations are challenging enough, security teams often do not have visibility into all the devices on their network. This includes unmonitored devices that are connected to the network but may not support endpoint detection and response (EDR) agents, such as OT and IoT devices.

With the Fortinet Security Fabric platform, security teams can bring network and endpoint data together in a single console, easily using telemetry gathered by FortiEDR and FortiNDR (network detection and response) Cloud to identify threats, especially those originating at the edges of the network, enhance response efforts, and proactively address security gaps. Further, the team can easily enforce new security rules through the organization's FortiGate Next-Generation Firewall (NGFW), ultimately securing unmanaged devices and roaming endpoints quickly and more effectively. Receiving actionable, enriched telemetry from across the network decreases the time required for teams to detect and respond to potential threats and allows them to take steps to better secure the environment before an attacker can strike.

FortiNDR Cloud leverages AI/ML capabilities and behavioral and human analysis to analyze network metadata, detecting malicious behavior and anomalies across multi-cloud and hybrid environments. The technology collects and analyzes network traffic metadata across Layer 2 through Layer 7, including Domain Name System, IPs, HTTP, Remote Desktop Protocol, Server Message Block, and encrypted traffic. Metadata is retained for 365 days for retrospective analysis and threat hunting. Because metadata cannot be manipulated by an attacker, it is a reliable "source of truth" for analysts looking to discover evidence of a sophisticated attack. By pairing FortiNDR Cloud detections and FortiEDR host context, analysts gain an end-to-end view of an attacker's actions. Analysts can then isolate impacted endpoints directly from the FortiNDR Cloud console using their FortiGate NGFW or FortiEDR to streamline response.

Analysts can also use network metadata from FortiNDR Cloud to identify any device connected to the network, including unmonitored and shadow IT endpoints that are not covered by other security controls. Analysts gain additional insights into the endpoints by combining FortiNDR Cloud and FortiEDR active discovery results. When these scans are performed continuously, they provide analysts with valuable information on newly connected network devices, such as printers, cameras, and media devices. Analysts can then decide if FortiEDR should be installed on a specific endpoint and if not, adjust FortiGate NGFW rules to either closely monitor or quarantine these endpoints to block traffic.

Additionally, using this combination of Fortinet solutions through the Fortinet Security Fabric platform enables security teams to:

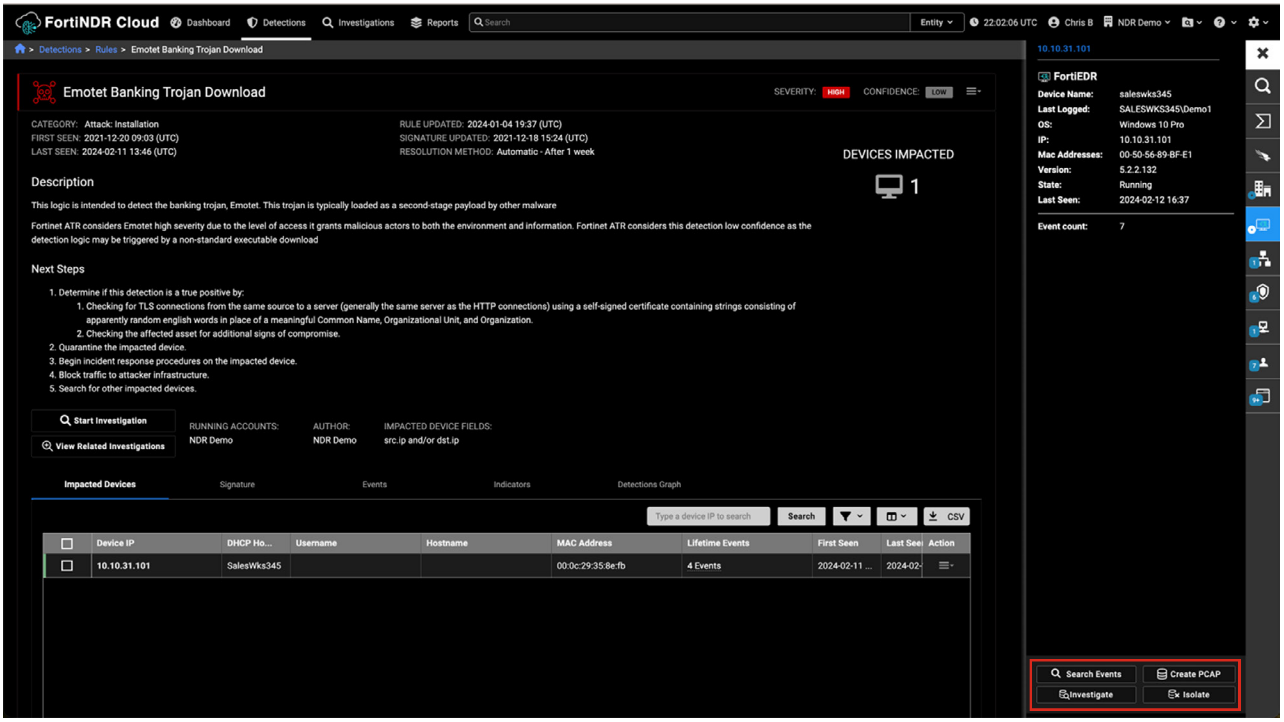
### Detect threats hiding in encrypted traffic

Attackers are increasingly finding new ways to make their malicious actions appear normal network activity. Security teams can leverage FortiGate NGFW decryption to meet this challenge and use FortiNDR Cloud to inspect SSL/TLS traffic. Combining these insights with FortiEDR data can help analysts detect and investigate various attacker activity.

When anomalous or suspicious activity is detected by FortiNDR Cloud, the FortiEDR tool can be used to isolate the attack. If there is no endpoint agent on the device where suspicious activity is suspected, teams can use FortiGate NGFW to isolate any device on the network.

### Reduce alert triage time

The integrated solution streamlines threat hunting using a single interface that allows security teams to investigate malicious and suspicious activity across the entire network, eliminating the need to manually collect information from disparate tools. For example, suppose analysts detect command and control beaconing, where FortiNDR Cloud detects malicious traffic from specific IPs/URLs. In that case, the analyst can pivot to FortiEDR or FortiGate NGFW to block all traffic to a C2 server directly from the FortiNDR Cloud console. In addition, FortiNDR Cloud retains rich network metadata for 365 days, giving analysts everything they need to conduct a comprehensive investigation. This data ensures newly discovered tools, tactics, and procedures can be retroactively investigated to discover if and when threats may have infiltrated the network.



Emotet Banking Trojan Download

CATEGORY: Attack: Installation
FIRST SEEN: 2021-12-20 09:03 (UTC)
LAST SEEN: 2024-02-11 13:46 (UTC)

RULE UPDATED: 2024-01-04 19:37 (UTC)
SIGNATURE UPDATED: 2021-12-18 15:24 (UTC)
RESOLUTION METHOD: Automatic - After 1 week

Description

This logic is intended to detect the banking trojan, Emotet. This trojan is typically loaded as a second-stage payload by other malware

Fortinet ATR considers Emotet high severity due to the level of access it grants malicious actors to both the environment and information. Fortinet ATR considers this detection low confidence as the detection logic may be triggered by a non-standard executable download

Next Steps

1. Determine if this detection is a true positive by:
    1. Checking for TLS connections from the same source to a server (generally the same server as the HTTP connections) using a self-signed certificate containing strings consisting of apparently random english words in place of a meaningful Common Name, Organizational Unit, and Organization.
    2. Checking the affected asset for additional signs of compromise.
2. Quarantine the impacted device.
3. Begin incident response procedures on the impacted device.
4. Block traffic to attacker infrastructure.
5. Search for other impacted devices.

RUNNING ACCOUNTS: NDR Demo
AUTHOR: NDR Demo
IMPACTED DEVICE FIELDS: src.ip and/or dst.ip

| □ | Device IP | DHCP Ho... | Username | Hostname | MAC Address | Lifetime Events | First Seen | Last Seei | Action |
|---|---|---|---|---|---|---|---|---|---|
| □ | 10.10.31.101 | SalesWks345 | | | 00:0c:29:35:8e:fb | 4 Events | 2024-02-11 ... | 2024-02- | ☰ |

10.10.31.101

FortiEDR

| | |
|---|---|
| Device Name: | saleswks345 |
| Last Logged: | SALESWKS345\Demo1 |
| OS: | Windows 10 Pro |
| IP: | 10.10.31.101 |
| Mac Addresses: | 00-50-56-89-BF-E1 |
| Version: | 5.2.2.132 |
| State: | Running |
| Last Seen: | 2024-02-12 16:37 |
| Event count: | 7 |

Figure 1: FortiNDR Cloud and FortiEDR integration allows analysts to isolate affected endpoints.

While SOC analysts benefit from the ability to investigate and hunt through advanced queries against retained enriched network metadata, they can accelerate response even further by running queries in parallel.

FortiNDR Cloud includes parallel hunting, which enables security professionals to coordinate threat hunting and investigation efforts across their global SOC teams. Team members can view existing queries and the results of an investigation. Further, they can pivot to predesigned queries with results ready for review. All detections are mapped to the MITRE ATT&CK framework, ensuring alignment when it comes to attacker behavior.

### Protect unmanaged OT and IoT assets

Not all network devices support the installation of an EDR agent, but the lack of an endpoint agent does not need to inhibit SOC visibility. FortiNDR Cloud detects anomalies in network devices and identifies unmanaged devices that can't support EDR agents. Combined with FortiGate NGFW, analysts can initiate remediation, such as isolating IT, OT, and IoT assets. This gives security teams complete visibility and control of all network-connected devices.

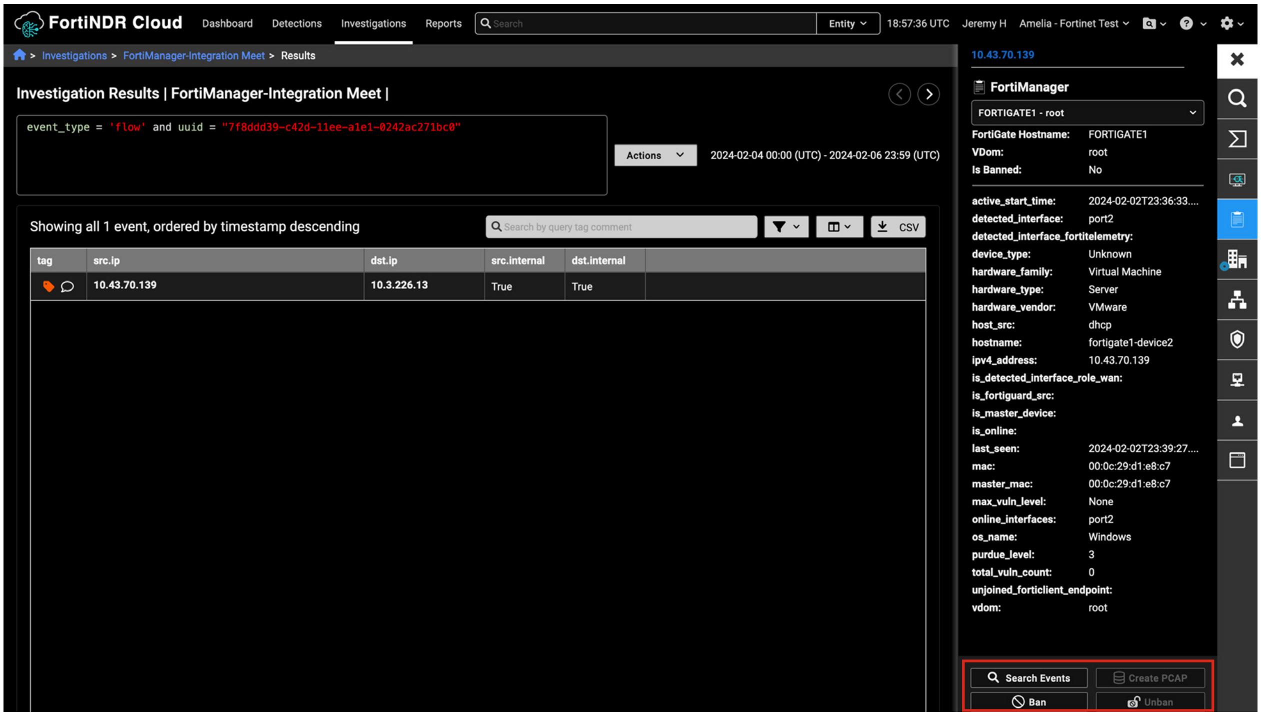
### Accelerate investigations by reducing false positives and prioritizing alerts

The FortiEDR and FortiNDR Cloud integration helps reduce false positives. When investigating suspicious communications, the analyst will be presented with endpoint data queried from FortiEDR. In cases where the endpoint process that generated the connection to a URL is a browser, which typically is not malicious activity, the information will be provided to the analyst. In cases where the process that generated the URL connection is not a browser, FortiNDR Cloud will immediately identify it as suspicious. In this scenario, the integration helps analysts distinguish between suspicious but legitimate activity, false positives, and substantiated malicious activity. An analyst can use a FortiNDR Cloud playbook to investigate all communications to the malicious URL through FortiEDR and FortiGate NGFW.

Customers reported that, on average, Fortinet EDP technologies like FortiEDR, FortiNDR, and FortiDeceptor helped them to reduce mean time to detection by 99% or more.[2]

## Leverage FortiNDR Cloud, FortiGate NGFW, and FortiEDR to Enhance Response and Stop Attacks Earlier in the Kill Chain

Integrating FortiGate NGFW, FortiNDR Cloud, and FortiEDR brings network and endpoint data together, providing security teams and threat hunters with enriched, high-fidelity detections to help expedite investigation and response. This is achieved by automatically correlating and analyzing security events from two data sources to help spot any evidence of malicious behavior early in the MITRE ATT&CK life cycle. Combining this telemetry helps teams decrease incident investigation and response time across network and cloud environments.



Investigation Results | FortiManager-Integration Meet |

```
event_type = 'flow' and uuid = "7f8ddd39-c42d-11ee-a1e1-0242ac271bc0"
```

2024-02-04 00:00 (UTC) - 2024-02-06 23:59 (UTC)

Showing all 1 event, ordered by timestamp descending

| tag | src.ip | dst.ip | src.internal | dst.internal |
|---|---|---|---|---|
| | 10.43.70.139 | 10.3.226.13 | True | True |

10.43.70.139

FortiManager

FORTIGATE1 - root

| | |
|---|---|
| FortiGate Hostname: | FORTIGATE1 |
| VDom: | root |
| Is Banned: | No |
| active_start_time: | 2024-02-02T23:36:33.... |
| detected_interface: | port2 |
| detected_interface_fortitelemetry: | |
| device_type: | Unknown |
| hardware_family: | Virtual Machine |
| hardware_type: | Server |
| hardware_vendor: | VMware |
| host_src: | dhcp |
| hostname: | fortigate1-device2 |
| ipv4_address: | 10.43.70.139 |
| is_detected_interface_role_wan: | |
| is_fortiguard_src: | |
| is_master_device: | |
| is_online: | |
| last_seen: | 2024-02-02T23:39:27.... |
| mac: | 00:0c:29:d1:e8:c7 |
| master_mac: | 00:0c:29:d1:e8:c7 |
| max_vuln_level: | None |
| online_interfaces: | port2 |
| os_name: | Windows |
| purdue_level: | 3 |
| total_vuln_count: | 0 |
| unjoined_forticlient_endpoint: | |
| vdom: | root |

Figure 2: The FortiNDR Cloud and FortiGate NGFW integration allows analysts to ban affected IPs.

FortiNDR Cloud complements FortiGate NGFW by providing an additional layer of protection within the network, applying behavioral analytics to network traffic metadata (east-west and north-south traffic) to detect unknown, subtle indicators of anomalous and malicious network activity and facilitate investigation of latent and ongoing threats.

When integrated with FortiNDR Cloud, FortiGate NGFW can provide decrypted copy of inspected SSL/TLS traffic to enable investigation and detection of a broad range of MITRE ATT&CK tactics, techniques, and procedures by FortiNDR Cloud.

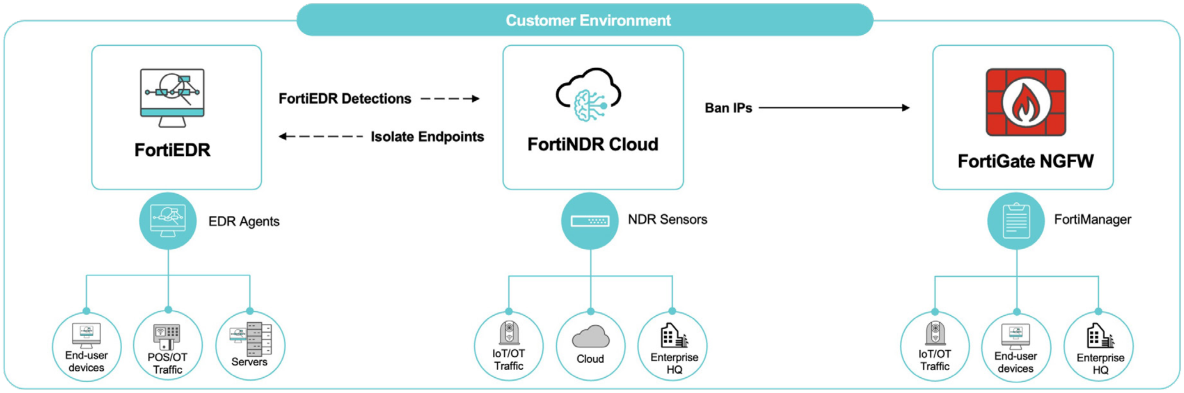


Figure 3: These integrations enable real-time network threat detection with endpoint security and NGFW attack isolation.

FortiNDR Cloud collects network traffic metadata and couples it with endpoint data from FortiEDR, providing comprehensive attack visibility and increased detection accuracy. To accelerate response, FortiNDR Cloud integrates directly with FortiGate NGFW to block malicious traffic and with FortiEDR to isolate infected devices.

FortiNDR Cloud also leverages threat intelligence from FortiGuard Labs and other leading third-party sources, resulting in early risk detection of more than 90% of the attacker tactics and techniques listed in the MITRE ATT&CK framework. Further, FortiGuard Labs threat experts continually refine ML-driven models and update detections, resulting in high-fidelity alerts and observations for faster investigations and threat hunting.

## Conclusion

The integrated solutions of the Fortinet Security Fabric platform offer unique benefits that reach far beyond simplified management. Enriched, combined telemetry decreases investigation times and streamlines remediation steps through a single interface.

FortiEDR extends the network visibility, analysis, and response capabilities of FortiGate NGFW and FortiNDR Cloud to the endpoint. FortiEDR delivers real-time, automated endpoint protection, advanced forensics, and threat hunting with orchestrated incident response across legacy and current Windows, macOS, and Linux devices. By correlating IP and domain-related network threat and anomaly detection with their endpoint-detected IOCs, SOC analysts gain an end-to-end view of an attacker’s actions, identify unmonitored endpoints, obtain contextual, enriched threat intelligence with endpoint threat hunting data, and can isolate endpoints directly from the FortiNDR Cloud console to streamline response.

[1] Aviv Kaufmann, The Quantified Benefits of Fortinet Security Operations Solutions, Enterprise Strategy Group, August 1, 2023.

[2] Ibid.

March 22, 2024 10:26 AM
2574709-0-0-EN