FirstNet
EDR as a Service

Real-Time Endpoint Protection, Detection and Automated Response

FirstNet's EDR as a Service delivers real-time, automated endpoint protection with orchestrated incident response across workstations and servers with current and legacy operating systems as well as POS and OT systems — all in a single integrated platform, with flexible deployment options and a predictable operating cost.

www.firstnet.com
Phone (24/7): 086 198 9896
Email: support@firstnet.co.za

EDR as a Service

REAL-TIME ENDPOINT PROTECTION, DETECTION AND AUTOMATED RESPONSE

Our offering enables proactive reduction of the attack surface, including vulnerability assessment and proactive risk mitigation-based policies that enable communication controls of any discovered application with vulnerabilities.

We can provide the first layer of defense via a custom- built, kernel-level Next Generation machine-learning-based Anti-Virus (NGAV) engine that prevents infection from file-based malware.
Backed by best of breed technology, FirstNet's EDR as a Service is the only solution that detects and stops advanced attacks in real-time, even when the endpoint has been compromised. No breaches, no data loss, no problem. FirstNet's EDR as a Service eliminates dwell time and provides a suite of automated Endpoint Detection and Response (EDR) features to detect, defuse, investigate, respond and remediate incidents.

HIGHLIGHTS

FirstNet's EDR as a Service is backed by the only endpoint security solution built from the ground up to detect advanced threats and stop breaches and ransomware damage in real-time even on an already compromised device, allowing you to respond and remediate incidents automatically to protect data, ensure system uptime, and preserve business continuity. FirstNet's EDR as a Service defends everything from workstations and servers with current and legacy operating systems to POS and manufacturing controllers. Build with native cloud infrastructure, FirstNet's EDR as a Service can be deployed in the cloud, on-premise in an air-gapped environment and as a hybrid deployment.

EDR Benefits

PROTECTION:

With FirstNet's EDR as a Service, you get proactive, real-time, automated endpoint protection with the orchestrated incident response across platforms. It stops the breach with real-time post-infection blocking to protect data from exfiltration and ransomware encryption.

SCALABILITY:

With a native cloud infrastructure and a small footprint, FirstNet's EDR as a Service can be deployed quickly and scale up to protect thousands of endpoints.

MANAGEMENT:

FirstNet's EDR as a Service delivers a single unified console with an intuitive interface. The cloud-managed platform closes the loop and automates repetitive endpoint security tasks so your IT or SOC staff do not have to.

MANAGED DETECTION AND RESPONSE

FirstNet have a dedicated SecOps team that can assist customers with the detection, analysis, containment, and remediation of security incidents to reduce the time to resolution, limiting the overall impact to an organization.
The solution will work in sync with the customer's incident response plan with regular touch points to ensure a cohesiveness with the customer staff, enabling a more efficient and effective response.

Chat to your FirstNet representative for more information on our MDR service and how we can help you.

EDR Features

DISCOVER AND PREDICT

- Discover and control rogue devices (e.g., unprotected or unmanaged devices) and IoT devices
- Track applications and ratings
- Discover and mitigate system and application vulnerabilities with virtual patching
- Reduce the attack surface with risk-based proactive policies

PREVENT

- Enable machine learning, kernel-based NGAV
- Enrich findings with real-time threat intelligence feeds from a continuously updated cloud database
- Protect disconnected endpoints with offline protection
- USB device control

DETECT AND DEFUSE

- Leverage OS-centric detection, highly accurate in detecting stealthy infiltrated attacks, including memory-based and "living off the land" attacks
- Stop breaches in real-time and eliminate threat dwell time
- Achieve analysis of entire log history
- Prevent ransomware encryption, and file/registry tempering
- Continuously validate the classification of threats

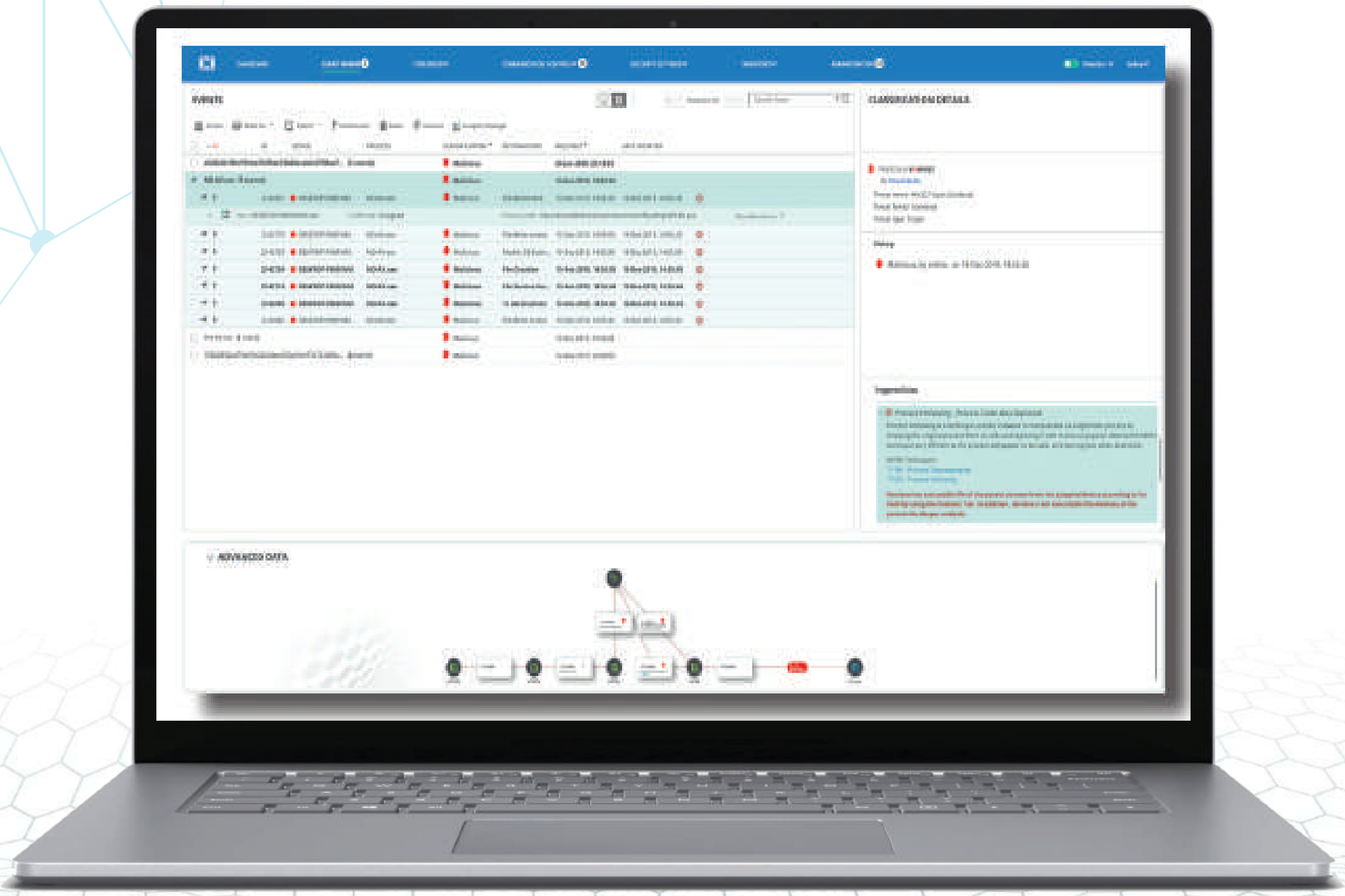
RESPOND AND REMEDIATE

- Automate incident classification and enhance the signal-to-alert ratio
- Standardize incident response procedures with playbook automation
- Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets
- Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups)
- Gain full visibility of the attack chain and malicious changes with patented code tracing
- Automate cleanup and roll back malicious changes while preserving system uptime
- Optional managed detection and response (MDR) service delivered by FirstNet's SecOps team

EDR Features

INVESTIGATE AND HUNT

- Automate incident classification and enhance the signal-to-alert ratio
- Standardize incident response procedures with playbook automation
- Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets
- Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups)
- Gain full visibility of the attack chain and malicious changes with patented code tracing
- Automate cleanup and roll back malicious changes while preserving system uptime
- Optional managed detection and response (MDR) service delivered by FirstNet's SecOps team

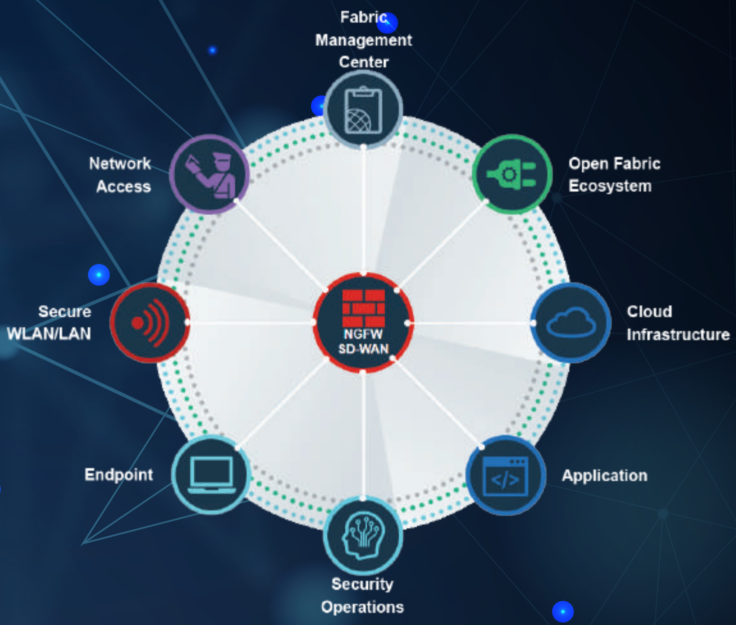


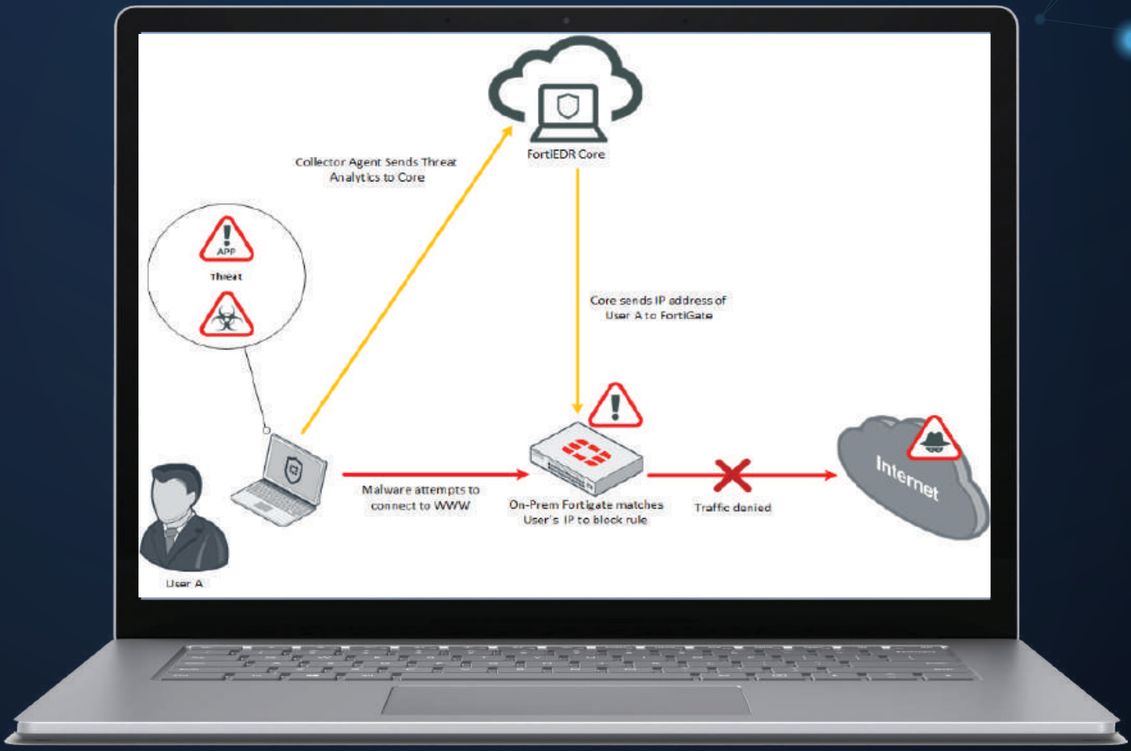
FORTINET
Security Fabric Integration

Customers with existing investments in FortiNet Firewalls, FortiSIEM or FortiSandbox whether it is delivered as a service from FirstNet or owned by the customer can leverage from the integration between FirstNet's EDR as a Service and the FortiNet Security Fabric.

FirstNet's EDR as a Service connector enables the sharing of endpoint threat intelligence and application information with FortiGate. FirstNet's EDR as a Service management can instruct enhanced response actions for FortiGate, such as suspending or blocking an IP address following an infiltration attack. This allows fast response to detected threats helping customers to protect and respond automatically rather than manually.

FirstNet's EDR as a Service can send events and alerts to SIEM's for threat analysis and forensic investigation. This can be FortiSIEM or any other capable 3rd party SIEM.

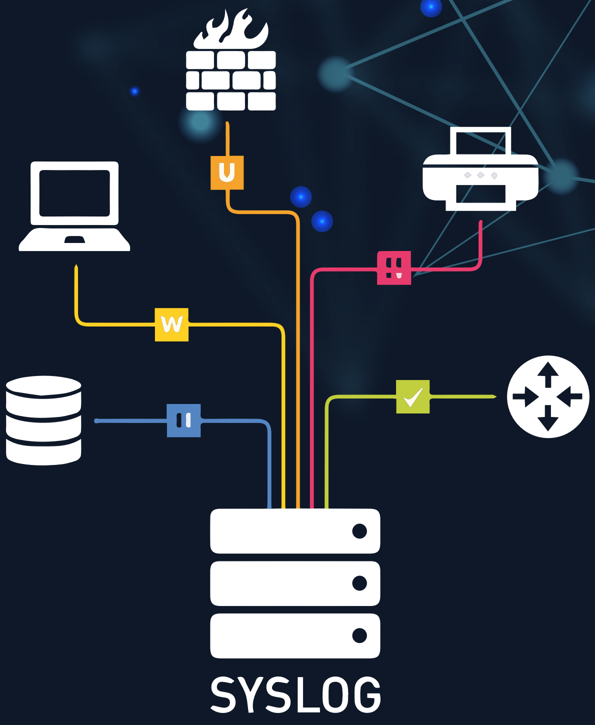



FortiEDR Core
Collector Agent Sends Threat Analytics to Core
APP
Threat
Core sends IP address of User A to FortiGate
Malware attempts to connect to WWW
On-Prem Fortigate matches User's IP to block rule
Traffic denied
Internet
User A

www.firstnet.com
Phone (24/7): 086 198 9896
Email: support@firstnet.co.za

3rd Party
SOC and SIEM Integration

Customers who utilize existing SIEM or SOC solutions can continue to benefit from these services. FirstNet's EDR as a Service easily ships logs to external platforms in standard SYSLOG formats allowing easy integration and continued continuity for these 3rd party platforms



End-to-end
Security

Speak to your FirstNet representative about our Security Fabric as a Service offering and 2FA as a Service offering so we can help secure multiple facets of your business network and users, as well as guide you on your security journey..

www.firstnet.com
Phone (24/7): 086 198 9896
Email: support@firstnet.co.za

FirstNet Technology Services

MDR
As a Service

An add-on service to FirstNet's EDR as a Service, FirstNet's Managed Detection and Response (MDR) Service focuses on monitoring the alerts and suspicious threats detected by EDR as a Service. The goal is to ensure all customer alerts are acknowledged and addressed accordingly. This team of threat experts reviews and analyzes every alert, proactively hunts threats, and takes actions on behalf of customers to ensure they are protected according to their risk profile. Additionally, the FirstNet MDR team provides guidance and next steps to incident responders and IT administrators. The following is a list of activities delivered as part of the MDR service.

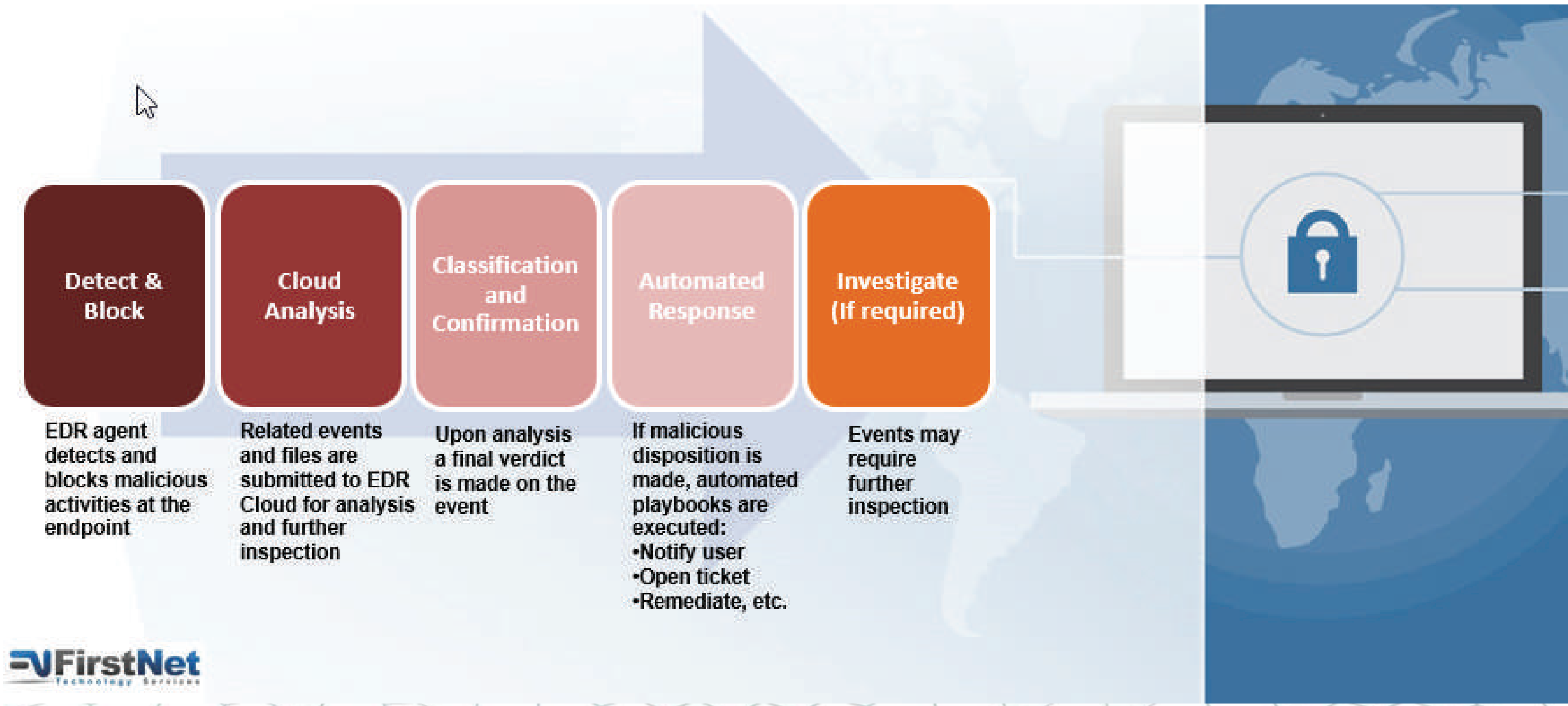
END-TO-END SECURITY

Our team of experts will work around the clock to monitor and hunt for threats and analyze events that may have entered your environment, leveraging alerts from the EDR as a Service Platform. Activities include but are not limited to:

- Analyzing malware both static and dynamic
- Analyzing memory for malicious processes
- Identifying potential vulnerable and unwanted programs
- Environment tuning—setting micro exceptions for clean applications

Once a compromised host(s) has been identified, the FirstNet MDR team will provide the initial tactical containment options with the goal of isolating the threat without impacting business operations. These options leveraging the EDR as a Service technology can include:

- Stopping a process from writing to the disk
- Blocking communications to another device



Detect & Block

EDR agent detects and blocks malicious activities at the endpoint

Cloud Analysis

Related events and files are submitted to EDR Cloud for analysis and further inspection

Classification and Confirmation

Upon analysis a final verdict is made on the event

Automated Response

If malicious disposition is made, automated playbooks are executed:
•Notify user
•Open ticket
•Remediate, etc.

Investigate (If required)

Events may require further inspection

Some of these containment options may already be automated through our technology IR playbooks. If not, the team can assist with additional configurations with playbooks as well as group/security policies..

MDR
As a Service

In addition, based on our threat analysis we will provide guidance for remediation steps, which can include both tactical and strategic steps. Some tactical options that can be both manual and automated are:

- Terminating a process
- Removal of a file
- Removing persistency from the registry

Our team will ensure you have the right information to make educated decisions about security issues we discover. Every security event that is triggered by our EDR as a Service technology is handled within 24 hours. If the issue is critical, we will respond appropriately. Once the event is analyzed, the team will send an incident email notification explaining the threat and recommendations for review and/or remediation steps.

Customers may also escalate a request for more information and/or guidance about an incident or event through email. Our team of experts are available 24/7 to assist with those requests. Depending on the criticality, the communications can be via phone or web conference call. As the engagement progresses, customers may want to know more about their environment regarding the platform health and/or specific threats or trends. Periodically our Security Product Manager and our FirstNet MDR team team provide an environment assessment. This assessment can include:

- Device coverage and EDR as a Service license usage
- EDR as a Service Platform health
- Malware and vulnerable or unwanted program findings
- Overall threat trends and recommendations
- Process questions and issues
- Address remediation issues as needed