Endpoint Detection and Response Architecture

Joe Martins, CISSP
Solutions Architect

Global Products & Solutions
January, 2020

Fortinet Endpoint Detection & Response Architecture

FortiEDR

Detecting sophisticated malware attacks.

FortiEDR is cloud native and enterprise ready, with the ability to easily scale to tens of thousands of endpoints. FortiEDR differentiates itself from other products in the market with features that include:

- Pre-execution prevention via kernel-level Next Generation AntiVirus (NGAV) engine with machine learning features that prevents infection from known and unknown threats.
- Forensics with process & memory capture as well as process tree analysis and control.
- Threat Hunting by searching across the recorded environment for processes or hash values.
- Contextual playbooks can be created to automate response by subject host and incident classification. The playbooks enable different notification, isolation and remediation options.
- Attack surface reduction and Virtual Patching achieved via mapping known vulnerability CVEs to discovered applications on the endpoint. A pre-canned policy can be implemented to isolate vulnerable applications until they can be patched. This is critical in an OT environment.
- Post-infection defusing mechanism that allows to surgically isolate processes from communicating or modifying files as a data exfiltration and tampering prevention so that the server or workstation continues to be productive
- IOT and rogue devices discover and control. This intelligence can be used in the Security Fabric to prevent a vulnerable or unpermitted devices from communicating and if compromised attacking.

Standalone: FortiEDR is an essential edition to the Security Operations organization with built in playbooks for automated response.

Fortinet Security Fabric: FortiEDR is also integrated into the Fortinet Security Fabric, and can interact with the FortiOS Automation Framework using automation stiches to respond to indications of attack or compromise at the network layer. Through the Fabric integration, FortiEDR can also respond to 3rd party security devices through integration with FortiSIEM enabling control of over 400 other manufacturers' products. This same integration can make use of FortiNAC to control device access to over 2500 device types.

FORTINET

Fortinet Endpoint Detection & Response Architecture

FortiInsight
Detecting Insider Threats

Where FortiEDR focuses on sophisticated malware attacks, **FortiInsight** focuses on the end user via User & Entity Behavior Analytics (UEBA).

FortiInsight uses machine learning analytics to monitor endpoints, data movement, and other user activities. Using a lightweight collector on the endpoint, FortiInsight detects unusual behavior that may be malicious or in violation of policy. When integrated with FortiSIEM, FortiInsight provides organizations with complete visibility into their data activity, enabling them to reduce the risks of insider threats that can lead to breaches or compliance events.

FortiInsight provides:

- An endpoint collector for visibility into files being moved to or from cloud storage applications, instant messaging, and other applications moving data. In addition, it tracks file names being moved via encrypted means.
- UEBA, powered by rule sets and augmented with AI, detects known and unknown threats ranging from malicious insider activity to compromised accounts.
- Recordings of user, machine, application, file, behavior, and network destinations/source activities for a complete forensic level of detail to support investigation and compliance purposes.
- A big data storage architecture for endpoint meta-data allows for retroactive rules and the ability to see past events in the current context.
- The endpoint collector has a store-and-forward capability that reports on potentially suspicious activity when offline, eliminating network blind spots.
- FortiInsight uses big data technology to collect billions of events that are collated, analyzed, and presented to your security team, providing near instant access to the information collected. For example, teams can see: who downloaded a payroll database, why someone uploaded a customer list to certain IP addresses, and how many people used unapproved cloud storage applications.

These components of FortiInsight enhance visibility, delivering the information that security teams need to respond quickly and efficiently before risky or malicious behavior turn into a data breach.

FORTINET

Fortinet Endpoint Detection & Response Architecture