optec

Fully Automate Threat Detection, Investigation & Response

Broader Protection, Increased Effectiveness with XDR

Extended detection and response (XDR) solutions are increasingly popular as organisations recognize the inefficiencies, and in many cases ineffectiveness, of security infrastructures comprised of many individual "best-of-breed" security products deployed from different vendors over time.

Common challenges arising from this point-product approach include:

- **Gaps in security:** with each product operating in its own silo, opportunities often arise for cyberattacks to enter in between
- **Too much security information:** with each product generating individual alerts and other information, security teams can easily miss indicators of cyberattacks
- **Uncoordinated response:** with each product operating independently, it falls on the human operator to share information and coordinate response actions

By moving to an integrated security infrastructure, organisations are often able to close security gaps, correlate security information, and automate operations. That's where FortiXDR can help, building on the broad, integrated, and automated Fortinet Security Fabric with fully automated threat detection, investigation, and response. This helps organisations improve their security posture and operational efficiency, easing the burden on security teams.

The Only XDR Solution Powered by Artificial Intelligence

FortiXDR is the only XDR solution that leverages artificial intelligence (AI) to easily automate the incident investigation process typically handled by a security analyst. Security teams can often struggle to handle all the security information they receive, increasing the risk of missing sophisticated cyberattacks.

Using telemetry, FortiXDR increases the chance of detecting attacks and creates more points of response to mitigate their impact quickly. This not only offers organisations extended protection, but also frees up security professionals to focus on more strategic roles.

Benefits of FortiXDR:

- Provides a simple multi-product detection framework.
- Dramatically reduces the number of alerts by 77%+ on average.
- Ensures that cyberattacks don't get "lost in the noise".
- Eases the operational burden on security teams.

Gartner reports that 80% of organisations are planning to consolidate security vendors in the next two to three years.

What Makes FortiXDR Different?

Given the increasing volume, sophistication and speed of today's threat landscape, security teams are more challenged than ever. FortiXDR goes beyond data correlation/analytics for detection and centralised response actions across products. It includes an AI decision engine that automatically investigates and handles incidents like an expert SOC analyst, reducing your incident response time and the burden on your security team.

It covers more points of the attack surface, including endpoint, Internet of Things (IoT), identity and access layers, network and cloud, email and web applications, as well as all stages of the Cyber Kill Chain to give the next level of protection.

Broader Coverage

FortiXDR not only covers the foundational network and endpoint components, but also extends the ability to include access, email, web applications and cloud, giving you more information for analysis, enrichment and ultimately classification.

FortiXDR also offers the ability to extend telemetry both earlier and later into a cyberattack, allowing it to cover the entire Cyber Kill Chain and giving you a significant security advantage.

On average, FortiXDR converts 100 high-value individual alerts into 10 high-fidelity incident detections for further investigation and response.

Reliable & Effective

As with all Fortinet solutions, FortiXDR offers you the highest standard of protection and reliability. All Fortinet security products that feed into FortiXDR consistently receive top marks in independent testing conducted by third parties such as AV-Comparatives, ICSA Labs, NSS Labs, Virus Bulletin and more.

Full AI-Powered Automation

FortiXDR harnesses the power of artificial intelligence to enable full automation of not only data normalisation/correlation and detection analytics, but also the incident investigation, classification and remediation process. As a result, it increases your security posture while reducing your team's workload rather than adding to it.

Increased Security Posture & Operational Efficiency

FortiXDR takes an innovative approach in fully automating the process of detection, investigation and response. This increases the likelihood of identifying cyberattacks in progress before they turn into data breaches or ransomware incidents, as well as freeing your security team up for higher-value strategic activities.

Extend your Security Today with Optec & FortiXDR

As Fortinet Engage Advanced Partners, Optec can help make extending your threat detection and response easy and stress-free. Get in touch with us today to discuss your FortiXDR solution.

Contact us at sales@optec.co.uk or 01280 878 597.