ON2IT
ZERO TRUST INNOVATORS

The next leap in EDR
Managed Cortex XDR as a Service

Cortex XDR Prevent and Pro deliver the most advanced endpoint detection and response, also adding integration with the network and the cloud. It's a complete solution that's offered for a fixed monthly fee.

THE CHALLENGE

Managing Endpoint Detection and Response (EDR) solutions is too complex and costly for inhouse teams

Attackers must complete a certain sequence of events, known as the attack lifecycle, to successfully accomplish their objectives, whether stealing information or running ransomware. To succeed, nearly every attack relies on compromising an endpoint, and although most organizations have deployed endpoint protection, infections with malware and exploits are still common.

But attackers don't just target endpoints, they aim at an organization's entire infrastructure. They use lateral movement and stealth techniques to exfiltrate valuable data or compromise operations.

THE SOLUTION

24/7 Managed Next Generation EDR

XDR is the next leap forward for endpoint detection and response (EDR), adding integration with the network, the cloud and other relevant agents and data sets.

It expands the capabilities of advanced endpoint solutions with machine learning and automation that reduces manual efforts, allowing our security analysts to focus on prevention and mitigation of threats that matter most to your organization. Our Security Automation and Orchestration Platform offers complete and 24/7 transparency in how we handle your security and mitigate risks.

Real visibility into real threats:

As endpoint-based attacks have become more automated and complex, IT and security departments face an event overload, a shortage of trained security analysts, lack of time and increasing staff cost. There's constant pressure on CISOs and CSOs to have better visibility across the entire infrastructure, faster response, and the ability to mitigate threats before damage occurs. What they need are outcome- based solutions that reduce the time, cost and complexity of event triage, incident investigation, response, and hunting. Instead of a sea of false positive alerts that increase workloads, they need visibility into the real threats.

Palo Alto Networks and ON2IT:

The managed endpoint solution offered by ON2IT is a single cloud-based product that combines the most advanced endpoint XDR security products from Palo Alto Networks with ON2IT's SOC-as-a- Service for a fixed monthly fee. It's the ideal combination of detection, pre-emptive protection, response and forensics. It is available for Linux, Mac, Android, and Windows endpoints (servers, desktops, on premise and in the public cloud).

The ON2IT solution leverages the award-winning Cortex XDR endpoint protection to block security breaches and ransomware attacks that use malware and exploits, known or unknown, before they can compromise endpoints.

Advanced automation techniques:

Cortex XDR provides the ON2IT SOC analysts and forensic specialists with rich contextualized log and event data and threat intelligence. By using automation techniques such as deep learning, behavioral baselining and Indicators of Good©, the ON2IT Security Automation and Orchestration Platform separates the noise from the relevant alerts, enabling our analysts to focus on identifying and remediating critical security events for ON2IT customers. We can reduce future risk and continually strengthen prevention by applying knowledge gained through detection, investigation and response.

YOUR MONTHLY CORTEX XDR PREVENT OR PRO SUBSCRIPTION FEE INCLUDES:

- Cortex XDR license fees
- ON2IT Security Automation & Orchestration Platform
- Threat Event Enrichment, Analysis & Correlation
- Incident Monitoring, Alerting & RCA
- Remote Breach Support
- Security Dashboard
- Compliance Reporting
- Automated Rules of Engagement
- AI-based Threat Hunting*
- Behavior Baselining*
- Post-Mortem Investigation*

*In combination with Cortex XDR

Clear business outcomes

- No worries about talent and staffing
- Extends benefits of EDR to complete infrastructure
- The right expertise and remediation 24/7
- Cost savings
- Cloud delivery allows fast deployment and scaling

Validated by independent research

Independent research organization The MITRE Corporation recently released the final results of its MITRE ATT&CK™ cybersecurity evaluations. The evaluation, which used the MITRE ATT&CK framework, shows that Cortex XDR Prevent provide the broadest coverage with fewest missed attack techniques among 10 Endpoint Detection-and-Response (EDR) vendors.

Out of 136 attack techniques tested, 121 techniques were detected by Cortex XDR Prevent, with 93% fewer misses than the next product.

ON2IT and Palo Alto Networks: true cybersecurity innovators

ON2IT's full support for Palo Alto Networks technology since 2009 reflects the importance of true cybersecurity innovation in our DNA.

ON2IT is a Palo Alto Networks ASC Elite, ATP, CPSP, MSSP, CSSP, Diamond Partner, winner of Traps global award and Managed Services Partner of the year.

We are driven by the notion that automation, innovation and a never-ending curiosity and search for improvement can actually make the Internet a safer place.

We are on to it, and you?

More information about Managed Cortex XDR? Call (214) 206-8446

7300 Lone Star Drive / Suite C200 Plano, TX 75024
E-mail: sales@on2it.net / Phone: (214) 206-8446

www.on2it.net