WWW.13LAYERS.COM | CONSULTING@13LAYERS.COM

13 LAYERS

MANAGED SECURITY SERVICES
WWW.13LAYERS.COM
@13-LAYERS

TOTAL NETWORK PROTECTION. FROM THE PERIMETER TO THE ENDPOINT

REACTIVE	PROACTIVE
SPEED	
Traditional cybersecurity solutions rely on analyzing traffic that is already doing damage while inside a network. By the time endpoint protection, SIEM, SOC have been alerted and attempt to remediate the damage has already occurred	Malicious traffic is removed in real time before it enters the network.This intelligence is then fed into existing reactive layers making them dynamically stronger
INTELLIGENCE	
Signature and definition based reactive solutions rely on intelligence sources publicly available (paid or free). They often aren't comprehensive enough to provide a full picture of the sophisticated attack chain.	We collect data from 28+ locations around the globe based on known proxies for sophisticated attackers and APT groups. Detected malware are reverse-engineered and ThreatINTELLIGENCE is passed back into your network every 30 minutes disrupting sophisticated attacks 24/7/365
MATURITY	
Static, reactive solutions analyze past attacks instead of preventing the next attack. False positives take time away from more important security tasks such as increasing maturity levels and maintaining uptime.	Providing a proactive solution allows us the time to focus our resources on R&D while still maintaining a strong security stack. We take this intelligence and feed it into your organizations other layers, increasing your security and giving you greater maturity across all of your traditional reactive solutions.
HUMAN INTERACTION	
False positives caused by security alerts are causing companies to lose focus on proactive tasks, requiring more personnel that are very difficult to find.	threatPROTECT leverages threatINTELLIGENCE, our proactive security device, produces no false positives, and requires no human intervention. false positives generated by traditional EDR platforms are cut by 50% or more allowing for your IT and Security teams to focus on proactive projects.
TRAINING AND EDUCATION	
Manual research is required to understand the large volume of false positives and how they affect a company's network. It can take months to learn how to use multiple tools from multiple vendors. Integrating vendor solutions together adds to these difficulties.	Our monthly threat intelligence reviews, phishing simulators and online learning portal make it easy to increase the capabilities of your workforce. With minimal training required for any program you can improve employee understanding in a short amount of time.
DEPLOYMENT AND INTEGRATION	
Artificial Intelligence-based solutions take time to learn environments, and Network monitoring and SIEM solutions can take months to get all sources ingested. Your company's data is being analyzed in the cloud infrastructure of multiple vendors which may cause deployment, integration, and accountability issues.	threatINTELLIGENCE can be deployed at each network segment in under 15 minutes without the need for asset discovery or cloud analysis. Our threatEDR platform can be delivered to any internet-connected device, while leveraging a single cloud for threat analysis.
BUDGET	
SIEM+SOC consumption-based models will charge more as both the amount of data and sources ingested are analyzed. Other solutions may also have additional license fees to get all features, or maintenance and upgrade costs which makes budgeting complicated across multiple vendors terms.	We have an easy to budget endpoint-based model that charges a simple monthly fee for each physical device with Microsoft, Linux or IOS operating systems. We don't charge extra for IoT devices, mobile devices and network devices. You get all the features of our solutions at no additional cost, allowing you flexible scaling options.