Hillstone NETWORKS

WHITE PAPER

Hillstone Networks

AI-Driven XDR Solution

Introduction

Enterprise networks have changed rapidly in recent years, driven by the increased adoption of cloud and big data services, the remote working phenomenon wrought by the COVID-19 pandemic, and other trends. The resultant diversified network access channels, coupled with an increasingly large and complicated network ecosystem, has led to a soaring workload for IT and security teams across the board, from provisioning, to operations and maintenance.

In tandem with these changes, the number and severity of network attacks is increasing exponentially. Advanced persistent threats (APTs), ransomware and other attacks continuously probe for network weaknesses to exploit. Once access is inevitably gained, these threats will sit quietly and silently propagate across network assets to maximize the damage when it decides to carry out its malicious intentions. Furthermore, with the expansion of the network edge due to the trends toward work-from-home/work-from-anywhere and cloud services, it is next to impossible to completely block all vectors of attack. Network traffic, the number of endpoints, and points of entry have all increased exponentially, complicating and even thwarting pre-breach detection.

Traditional security technologies that rely upon blacklists/whitelists and signature databases are unable to defend against new cyberattacks like zero-day threats, unknown malicious code attacks, low-frequency behavioral attacks and similar threats. In fact, studies have shown that even the most advanced AI/ML enhanced pre-breach tools are only as much as 50% effective at blocking all threats.

Compounding the problem is the disparate deployment of various security devices across the network for the purpose of single-point detection and defense. Often comprised of products from different vendors, these devices create isolated islands (or silos) of network security and bring high operations and maintenance costs. This type of construct can also lead to security fragmentation – the lack of ability to share information and coordinate operations – as well as an inability to accurately visualize changes in security conditions and effectively respond to threats, attacks, and abnormal behaviors.

It is clear, then, that a new security strategy is required to provide situational awareness across all network and security assets, as well as the ability to help security administrators intuitively and rapidly coordinate defenses when a threat, attack or anomaly arises, and free them to carry out incident investigation and handling where needed. A relatively new class of security technologies, called extended detection and response (XDR), offers these capabilities and more.

Contents

Current Pre-Breach Mitigation Strategy

Taking a deeper look at current security strategies, pre-breach mitigation largely focuses on signature matching. Put simply, if a user has a certain type of signature that is deemed to be malicious, that user will be blacklisted and will be unable to breach the network. However, hackers have developed very complex methods of disguising or altering their signature so that they can bypass even AI/ML-enhanced perimeter security solutions.

Strict whitelist/blacklist policies might seem to be a viable alternative or augmentation to signature matching, but they operate much like an IPS, i.e., an IPS blocks traffic automatically, but it may accidentally block legitimate traffic. Similarly, if too strict of a whitelist policy is enacted in a pre-breach strategy, it will block valid business operations, effectively restraining a business in much the same way a malicious hacker would. The point is, attackers are without a doubt proficient at disguising their signatures, but the solution can't be to block everything.

Even for endpoint security products that feature advanced AI- and ML-based detection technologies, their position in the network limits their ability to effectively 'see' and respond holistically across the entire network. For example, a next-gen firewall, which is critically important for security defenses, has a view of only the traffic that traverses it; similarly, a web application firewall can examine only traffic to and from the web resources that it defends.

The Problems in Post-Breach Mitigation Strategy

Regardless of the tactics used to disguise signatures, the attackers' malicious intentions and malevolent behavior always fall under certain categories of malware families. This is what current post-breach mitigation strategy is based upon: Flagging abnormal behaviors. However, studies have shown that a hacker is able to roam undetected on a network for an average of 56 days – or nearly two months – before current post-mitigation solutions are able to detect and remove them.

Enter XDR, which can bolster both pre-breach and post-breach mitigation strategies by combining and correlating logs and other information from multiple devices, breaking down security information silos. At its core, XDR provides deep visibility, highly accurate threat identification and swift containment and mitigation, while simplifying security operations and management and eliminating alarm fatigue for the already overburdened security teams.

The Rise of XDR

We cannot discuss XDR in detail without first discussing its predecessor – EDR, or endpoint detection and response. EDR focuses on protecting endpoints such as laptops, tablets, and IoT devices through malware detection and antivirus. EDR typically works in conjunction with a firewall. To visualize this, imagine a firewall to be the gate to a house. An EDR would be like a guard dog that is attached to each person that passes through the gate.

One of EDR's biggest limitations is that it offers visibility only into managed devices and endpoints. However, endpoints can come from a plethora of origins, such as users visiting your websites or interfacing with databases and servers. Without visibility into those endpoints (because they are unmanaged endpoints), studies have shown that EDR is actually only able to detect around 28% of attack vectors.

XDR expands upon the concept of EDR by creating a centralized management center that compiles data from EDR, firewalls, web application firewalls, and other security (and non-security) services/devices in the network into one cohesive report that can be utilized to formulate a plan of action. Going back to the analogy, you might think of XDR as a watchtower that can see everything going on below it, analyze and understand it, and then take action to defend against threats.

In essence, an XDR takes low-confidence risk assessments from various security services within the infrastructure, then combines them into a single, high-confidence report. Thus, as threats continue to evolve and outsmart current pre-breach and post-breach solutions, so does the need and interest for XDR solutions to evolve and outsmart said threats.

Defining an XDR Solution

From a high-level view, the key capabilities of an XDR solution include integration, analysis, and response. Integration refers to the ability to integrate metadata from multiple products and services, which can be almost any source including third-party vendors or even external providers and cloud services. This data is then standardized and integrated to provide comprehensive visibility while breaking down security information silos and greatly reducing blind spots. The importance of this integrated approach cannot be overstated; it is the key to improving threat detection accuracy and providing effective and efficient defense against threats.

Analysis is the second linchpin of an XDR solution's capabilities. Upon successful integration, XDR products are capable of implementing holographic analysis on the standardized data to provide the context behind other security products' metadata and log reports. Holographic analysis is a style of analyzing data that is based on the principles of holographic storage, which records information using multiple angles of light. Through holographic analysis, an XDR solution is able to instantaneously scrutinize an instance or an occurrence from countless perspectives, and thus provide highly accurate identification and detection of threats.

This is ultimately the purpose of an XDR product – to collect countless snapshots of an occurrence instantaneously and then correlate and analyze them. With context, the logs from individual security products and services become much more coherent. In addition, depending on the strength of the artificial intelligence (AI) and machine learning (ML) utilized by the XDR solution, the logs that are created post-analysis can poten-

tially be free of false positives and duplicates.

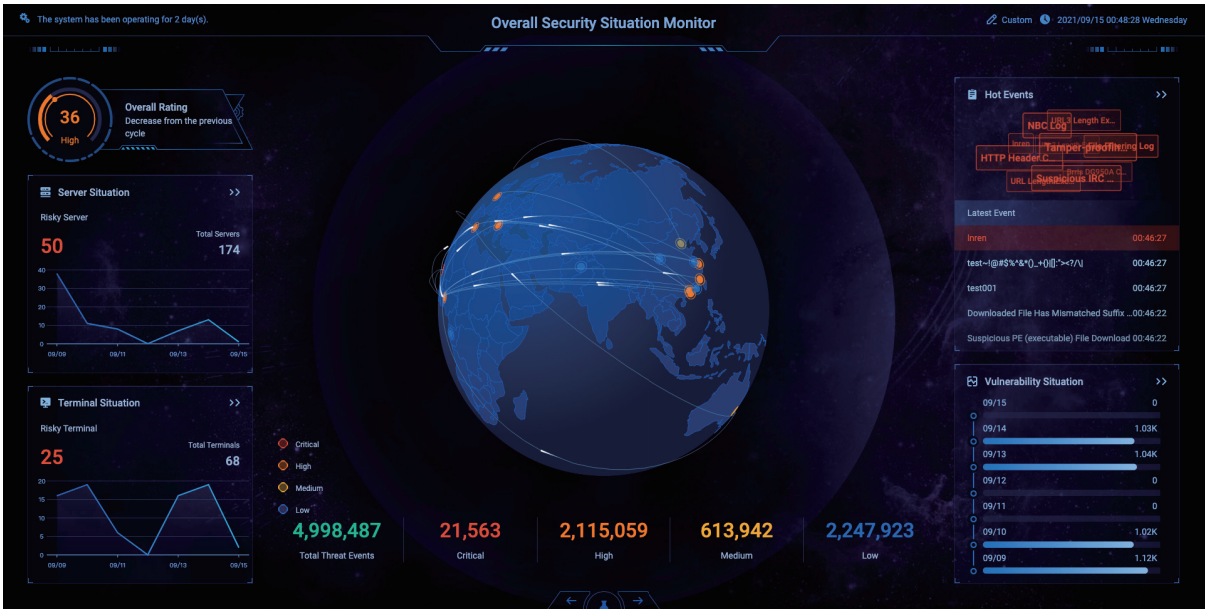
This stage is one of the key reasons for the adoption of an XDR solution: to relieve alarm fatigue. When CISOs and security teams review the logs of their security products, they are often bombarded by thousands of reports, with wildly varying threat criticality levels. Even if these logs can present results based on the level of criticality, it is difficult to understand the severity of the threats without gaining more context from different perspectives, or in this case, different security products' threat logs.

By collecting, standardizing, correlating and analyzing logs and other data across a wide variety of security products, XDR can present a unified view of threats and attacks as well as their respective levels of criticality. This greatly reduces alarm fatigue and frees security personnel for case management and investigation.

The ability to see and understand also affords an XDR the ability to act – to respond to threats and attacks in a comprehensive and holistic manner for highly effective defenses. Depending on the level of integration with point security products like NGFWs, WAFs and others, XDR can orchestrate responses automatically across them to cohesively respond to even zero-day and emerging threats. Along with integration and analysis, response is the third key capability of XDR. Together, they provide complete visibility, highly accurate identification of threats and attacks, and swift containment and mitigation.

Hillstone Networks' XDR Solution: iSource

Hillstone's iSource XDR solution represents a radical new approach to cybersecurity. iSource is a data-driven, AI-powered threat intelligence platform that integrates massive security data, investigates correlations of incidents, identifies potential threats, automates security orchestration, and responds cohesively across multiple security products and platforms for unrivaled security operation efficiency.



Integration Spanning the Ecosystem

Massive amounts of data are integrated into iSource across the entire network environment, including Hillstone security products and services as well as third-party products like servers, endpoints, vulnerability scanners and other sources. For example, Insight, from Hillstone's CloudHive micro-segmentation solution, generates logs and reports on intra-VM traffic, as well as east-west and north-south traffic within the private cloud. Hillstone's WAF provides insight on application-layer traffic, and Hillstone NGFWs offer data on traffic at the network edge.

Individually, Hillstone CloudHive, WAF and NGFW can provide valuable logs on potential threats. However, these are only breadcrumbs or pieces of a larger puzzle.

Like a police team operating in a crime scene, these breadcrumbs provide valuable clues that can help solve the crime – or in this case, help identify nascent threats and attacks.

iSource can integrate a wide variety of data across the full spectrum of the network, from endpoints to cloud. This data might include NetFlow, Sysmon, Syslogs, metadata, threat information and third-party logs, all of which are then standardized, correlated and analyzed to provide complete visibility and break down security information silos. It not only brings full security visibility with far fewer blind spots, but also improves detection accuracy and minimizes false positives.

AI- and ML-Powered Big Data Analysis

Once all sets of data have been standardized and integrated, the iSource threat intelligence engine digests and analyzes it to create a cohesive and comprehensive report. This big-data analysis platform utilizes a distributed real-time computing framework coupled with search engine capabilities, and AI and ML algorithms to perform an in-depth analysis in real-time. For example, by correlating and analyzing data from a wide variety of sources, iSource might detect a botnet command-and-control (C&C) path, an attack chain, ransomware, cryptomining, or any number of other threats.

iSource leverages information from third-party intelligence partners worldwide to provide additional input for the analysis engine to leverage and enable comprehensive vulnerability and risk management. Additionally, by integrating with third-party partners, iSource gains a very comprehensive signature database. Pairing this with machine-learning technology that Hillstone has been developing since the early 2010's yields a very thorough correlation analysis engine that is capable of generating in-depth, high-confidence logs. During this process, false positives and duplicates are additionally eliminated to mitigate alarm fatigue for security teams.

Automated Security Orchestration and Cohesive Response

If a remediation strategy has been configured, once a threat is identified, iSource will automatically execute the appropriate mitigation actions according to a predefined playbook. These playbooks can either be created according to default templates provided by Hillstone Networks, or they can be user-defined and built from scratch, customized for the user's business needs. iSource includes the option of eliminating automatic implementation of mitigation strategies and leaving that step purely up to the discretion of the user. If playbooks are implemented, iSource will communicate recommended action steps back to the point security solutions and services that are fully integrated with iSource.

This process continues in an infinite loop, from standardization, correlation and analysis, to comprehensive automatic or manual threat response. Through its continuous intake of data, deep analysis and coordinated response, iSource enables swift incident triage and attack containment before damage can be done.

Unified Management and Reporting

Hillstone's iSource offers a customizable dashboard that allows simple and rapid access to the organization's security posture with comprehensive statistical information such as rankings and counters, as well as incident summarization and security trends with graphical charts and lists. iSource also supports template-based or customizable reports that can be generated on schedule or on demand. Public APIs enable integration with third-party tools or security products to inject security data generated across the entire security fabric and perform interactions to contain threats.

Conclusion

Assets are the core for security and risk management; conversely, the end-purpose of threats and attacks is to gain access to those same data assets. Hillstone iSource provides comprehensive visibility and risk management to assets like servers, endpoints, and even applications and services, from multiple dimensions including risks, vulnerabilities, and threat events.

Through integration across a wide variety of point security products and other devices, it continuously assembles, standardizes, and correlates occurrences, anomalies, and nuances for deep visibility. Its big-data analysis engine then accurately identifies potential threats and attacks, allowing automated security orchestration and cohesive response across the network ecosystem. It presents statistical data, such as the distribution, trends and criticality of threats and vulnerabilities, along with detailed information on individual assets. The holistic XDR approach offered by iSource protects assets by rapidly identifying and mitigating potential exposures to threats throughout the network, from the endpoint to the cloud.

Hillstone
NETWORKS

Visit **www.hillstonenet.com** to learn more
or contact Hillstone at **inquiry@hillstonenet.com**