elastic

Search. Observe. Protect.

Unifying data visibility for better threat detection & response.

Making Sense of the Market

Introduction

As the threat landscape evolves, vendors are meeting the challenge by incorporating XDR products as part of their traditional SIEM solutions, in order to create a coordinated, holistic approach. Extended Detection and Response is an emerging integrated solution of protection, detection and response products for endpoints, networks and the cloud.

What XDR promises to do is encapsulate much of the fragmented workflow security teams are experiencing into a single, unified solution. This substantially helps teams to automate and accelerate their analysts' workflow of triage, investigation, escalation, and response — ultimately bringing these capabilities to more users, faster, in order to better protect organizations from cyber attack.

Core components of XDR include:

Visibility

The exponential growth of data has increased the difficulty of the security practitioner's job. A central repository to conduct analysis, root cause identification, and remediation planning is required. XDR solutions that have evolved from endpoint security products are generally unable to ingest and retain the volume and diversity of data sources used by the enterprise.

Elastic's free and open architecture, which ingests any data source, has put the technology years ahead of legacy solutions.

Analysis

A flexible framework is required to compose, enable, and monitor new analytics use cases at scale. There should also be a seamless integration with analyst workflows with the ability to prioritize and build the attack narrative.

Using cross-cluster search, Elastic can bring the search experience to any dataset, reducing costly backhauling of data from different geographic areas. Cross-cluster search empowers analysis of all data in an organization's multi-cloud environment, allowing it to operate without the need to transfer data across regions or providers.

Response

Analysts need a simple, intuitive way to collaborate on an investigation, build a remediation plan, execute on that plan, and report on its success. A centralized XDR solution lets users collaborate to quickly remediate and ideally prevents attacks before they are executed. Native endpoint security solutions built into a broader XDR framework can help reduce the mean time to remediate (MTTR) to zero.

Elastic Limitless XDR

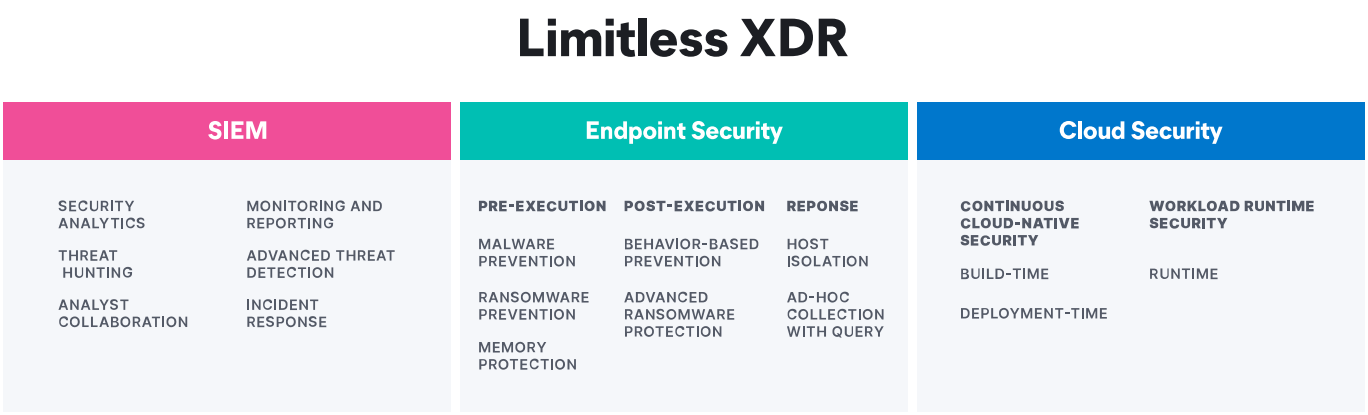
Since SIEM, endpoint security, and cloud security solutions round out each other's capabilities, a security leader's arsenal can be considerably more efficient when deployed as a coordinated, synchronized whole than it would otherwise be if these tools were deployed separately. Organizations with a holistic view of the operational environment, vulnerabilities, and threats are better able to prioritize the risk to critical digital assets.

What makes Elastic's approach to XDR limitless? Limitless data ingestion…limitless analysis…limitless protection…all provided with a scalable pricing structure based on resources used.

Unifying data types to improve detection

Perhaps the best thing about Elastic Limitless XDR is security teams' ability to ingest data from across the organization and view it in one pane of glass. The unification of tools provides the ability to store and ingest data in a single repository, which results in risk reduction through improved visibility, automated detection, and automation of routine tasks that otherwise consumes a significant portion of analysts' valuable time.

The core components of Elastic Limitless XDR include:



SIEM

Security teams are reporting alert fatigue and burnout caused by their being diluted or buried with threat research and tasks of tuning, managing, and maintaining their legacy SIEM and ticketing platforms.

Legacy SIEMs traditionally collect data from multiple sources, but have limited ability to identify meaningful trends or provide automated detection or response abilities. When they do, these capabilities are painfully slow and don't scale well to large amounts of data. Rather, to be useful, SIEMs require a scalable infrastructure with lightning fast results to analysts' many investigation queries.

Because Elastic's SIEM app is built upon the renowned speed of Elasticsearch, with the robust visualization tools of Kibana, it is the backbone of Elastic Security's Limitless XDR solution.

It begins with the ability to ingest any data type — including high-volume data sources — as well as an intuitive and lightning-fast analytics UI that accelerates security operations across the enterprise's attack surface. The ability to ingest data at high volume, as incredibly useful as it is, is uncommon in many other SIEM solutions. Many security teams are restricted in data volume they can ingest, as they are charged on this basis. Elastic charges only by the resources teams use; ingest as much as is needed, then act upon that data at a later time as needed.

Powering security analytics — at scale, on any data set — is core to what differentiates Elastic Security. Working to rapidly extend the capabilities of the Elastic SIEM app are features like machine learning to power analyst insights, host-based behavior analytics, and automated detection aligned with MITRE ATT&CK®-aligned rules.

Through Elastic Common Schema (ECS), the organization is able to gain a holistic view, making it easy to analyze information across and beyond the entity's digital domain – no matter the data sources.

ECS facilitates the analysis of data from diverse sources by providing a consistent and customizable way to structure all types of data. With ECS, analytics content, such as dashboards and machine learning jobs, can be applied more broadly, while searches can be crafted more narrowly and field names are easier to remember.

Mitigating long dwell times

The current retention period for actionable data in most SIEM and XDR systems is far exceeded by attacker dwell times.

Elastic, however, can take action on such large data volumes using an object storage approach, allowing organizations to significantly expand what they can observe in the operational environment and any security threats therein — better orienting their security controls and defending against those threats (See Testing the new Elastic cold tier of searchable snapshots at scale blog for more insights on the object storage approach).

Elastic has a unique vision of what SIEM should be: Fast, powerful, and open to security analysts everywhere. Building on the future of Limitless XDR, Elastic Security is pushing beyond the success of our SIEM app to further integrate the capabilities of endpoint and cloud security. With Elastic Security's approach to SIEM, analysts can quickly address a much broader overview of alerts, prioritize them, and make informed decisions regarding actions to take.

> "Migrating from multiple security tools to Elastic Security has helped us reduce risk. Full visibility across our environment, and fast redemption,which is of significant value to our business."
>
> **Sam Ainscow**
> CISO, Barrett Steel

Endpoint security

As organizations continue to embrace a hybrid, dispersed workforce, where the use of personal devices to perform daily work tasks is becoming the norm, the connection to critical assets is often through unprotected hosts. Endpoint Detection & Response (EDR) was designed to focus on the protection of users' endpoint devices. EDR typically has minimal integration capabilities and results in partial security monitoring, leaving other areas of the network open to attack if not addressed. This issue can be resolved with a more holistic XDR approach.

Limitless XDR further extends endpoint security with prevention and detection in depth. This includes universal data collection for cross-environment analysis, remote host inspection, and distributed response.

While EDR may be more readily implemented into a security team's existing toolset, XDR is far more effective at boosting the team's ability to detect and respond across the organization's full attack surface to better protect crucial assets. With XDR's ability to monitor a diverse set of assets across endpoints, cloud, user, network, and other vectors — and integrate this diverse data into a unified view of the organization's security situation — security risk from siloed data streams is greatly reduced.

EDR uses machine learning to detect and prevent more common but damaging attacks, such as malware and ransomware attacks. XDR complements these capabilities, using powerful analytics to correlate activity and identify threats that may otherwise go undetected. XDR goes beyond blocking malware and ransomware, exposing more sophisticated threats such as supply chain attacks and advanced persistent threats by unifying prevention, detection, and response across the entire ecosystem.

EDR is a key component in Elastic Security's Limitless XDR, alongside SIEM and Cloud security. Users can detect and block unknown and polymorphic malware and ransomware before execution with machine learning, and prevent more advanced threats with behavioral analytics.

Free and open case management

Free and open case management enables users to communicate and collaborate with their team, seamlessly integrating with key remediation vendors and participating in existing workflows of varying scale. The API-first development and webhooks capabilities offer easy integration to any other productivity tool to speed analysis and reporting, as well as other useful customizations that are important to an organization's operations.

Elastic provides a centralized way to coordinate data collection and policy enforcement such as automatically quarantining malware files. During remediation, osquery management allows users to gather any additional information required in the incident process, along with gathering deeper context, performing ad-hoc correlations and invoking remote response actions.

Cloud security and critical linux controls

Elastic's Limitless XDR Solution for cloud security is critical, given the amazingly ubiquitous, but largely unaddressed prevalence of Linux in cloud computing.

As of 2017, Linux was running 90% of the public cloud workload. 62% of the embedded systems market share is Linux, 99% of the supercomputer market is Linux, and 82% of all the smartphones in the world operate on Linux, as do 9 of the top 10 public clouds.[1]

The general consensus is that Linux is the most available and reliable solution for critical workloads in data centers and cloud computing environments. Its dominant presence in cloud solution architecture will no doubt continue.

Strategies to secure information stored on Linux servers often fall dramatically short of ideal, due to tooling gaps required to achieve risk management goals. Linux endpoint security has largely remained an afterthought, despite being a key backbone of cloud computing. To date, addressing the known vulnerabilities of Linux-based servers was primarily done through controls developed for Windows, which lack reliable protection, are too cumbersome to deploy efficiently, or are too expensive to implement and maintain.

Because Endpoint Detection and Response (EDR) technologies have been developed for Windows and Mac-based systems, they miss seeing activity on predominantly cloud-based Linux production servers. Threat hunting using these deficient controls, on Linux production servers, leaves critical gaps that create a challenge for security professionals.

Given cloud's projected growth, addressing Linux security deficiencies within the Windows controls environment must become a major priority if cloud security is to be properly addressed.

Elastic Security's Infrastructure Detection and Response (IDR) platform was purpose-built for the Linux infrastructure. It delivers native solutions for security problems that every Linux administrator faces.

For example, behavioral or organization controls adhering to compliance requirements, or that ensure system safety, can be set up to deliver automated protection for Linux assets.

The IDR platform helps organizations execute real-time proactive offensive and defensive responses to security events in the cloud protect surface. Proactive controls and responses can be set up to create boundaries and controls around sensitive actions to complement traditional access management.

Enabling a Zero Trust cloud strategy

In the Protect Surface approach to Zero Trust, an organization's most critical assets are identified and prioritized, with protections implemented to each in priority order. Using the DAAS method (Data, Applications, Assets, Systems) to identify critical assets will reveal that most critical cloud computing elements are based on or use Linux. Organizations need Linux controls such as those in Elastic's Cloud Security foundation, making it the best platform on which to build a Zero Trust cloud strategy.

[1] CBTnuggets August 10, 2018

Controlling access on a need-to-know basis

To secure each identified Protect Surface, the organization must understand how multiple traffic flows interact with that surface, and place controls as close as possible to the surface they are trying to protect.

Elastic's cloud workload protects hosts from unauthorized, non-compliant, or malicious use when authorized users (i.e., human, programmatic) gain access to them. It also includes a suite of protection capabilities including proactive controls to block activities the organization specifies and is complemented by its capability of threat detection and remediation.

The capability to block the execution of specific commands, based on custom policies, and blocking file systems to disallow access or modification to these sensitive files while providing user and role attribution for such actions, achieves the goal of placing the controls as close as possible to the Protect Surface.

This real time authorization for sensitive commands or file modifications enforces the Zero Trust principle of least privilege, where trust is never granted implicitly but must be continually evaluated.

Additional Elastic Cloud Security capabilities are invaluable in addressing the following aspects of Zero Trust:

Visibility

In a cloud environment, the lack of visibility can lead to cloud computing security issues that put organizations at risk. It is imperative that organizations have comprehensive visibility into their cloud environment on a continuous basis.

With Zero Trust, all access requests are continuously vetted prior to allowing connection to any of the enterprise or cloud assets. Consequently, Zero Trust policies rely on real-time visibility into user credentials and attributes.

Elastic's cloud workload protection increases visibility across the Linux fleet of assets. It covers all entry points that enable direct access to a host via humans and automated scripts. Every user action is tied to the actual user who executed it. User attribution for shared and root accounts, something often difficult to determine, is guaranteed for every action.

Elastic controls privileged user access and is able to stop shared account abuse with in-line MFA made available through integration with a variety of 2FA solution providers. By default, Linux does not have MFA built into its SSH daemon, but by using Elastic's MFA capabilities an organization can ensure that whoever is logging in to take action is the correct person.

Elastic provides security teams visibility into the set of processes in containers through its support of Daemonset deployment methods for self-hosted containers, as well as on-base container-based platforms such as Kubernetes.

The Elastic single dashboard provides an easy-to-read terminal view enabling visibility across all users and shared account action. This includes full command-line and server context. The administrator is able to easily search terminal data and identify issues to resolve.

Policy creation

The development of concise and effective security control policies is a key aspect in preventing cloud security failures. Policies require a clear understanding of the threat models specific to cloud native applications and infrastructure.

Elastic enables command-level guardrails to establish controls, in accordance with policies, for individual commands that users can and cannot execute, including root users and privileged accounts, to protect sensitive data and critical actions.

Custom policies can be created using rich trigger specifications to provide risk alerts and notifications. Human driven and automated responses to anomalous events can be added. Approvals can be policy-based (e.g., user, group, time of day), or manual, through Slack or Teams. Sensitive data is protected by approving dangerous commands executed though Slack and Teams even if initiated by a root user

Inspect and log all traffic in real time

Built on top of Elastic's IDR platform, the Observe function enables tracking and monitoring of what users do and when they gain access to an organization's Linux hosts, covering all entry points that allow direct access to a host via humans and automated scripts.

Administrators are able to track the identity for every action everywhere, even when the user is logged in with default or shared credentials. Every action can and will be attributed to the actual user. This way, organizations can monitor all user activity, in real time, from commands being run to the files and databases being accessed.

Elastic captures all offline activity as well. If a server goes offline, the organization's security team will have a recording of all activity, saving time and ensuring that even when servers are offline, all policies and rules remain operable

Monitor and maintain

Another key tenet of Zero Trust is monitoring and maintaining data for the purpose of collecting and analyzing all the telemetry the organization can accumulate. By putting this telemetry into a large data lake, the organization gains a greater understanding of what is occurring in this protect surface and can use that knowledge to develop a learning system.

The logging capability of Elastic greatly reduces security incident investigation time by allowing clients to search and filter through real-time and archived activity to successfully investigate security events Linux native threats can be identified and fed into the organization's SIEM based on MITRE ATT&CK® alerts and critical events – a critical component lacking in most cloud security tools today.

Controlling access on a need-to-know basis

Elastic simplifies auditing and reporting by storing all activity in an intuitive, searchable engine that enables the organization to take advantage of the great inherent value found in Linux logs. Create, archive, and export an audit trail of user activity using superior Linux auditing capabilities while building customized reports to meet requirements of auditors, regulators, and internal security policies.

Cloud security and critical linux controls

The escalation of cyberattacks and the continuous expansion of attack vectors are providing adversaries with overwhelming flexibility from both a strategic and tactical perspective.

That level of flexibility must be countered with a similar, if not greater, level of flexibility by the security teams of organizations if their effort to defend their critical assets is to succeed. Elastic provides our clients the ability to design and implement a cybersecurity architecture that best addresses their own unique operating environment.

The key to increased flexibility is greater visibility into data flow, data use, and stored data itself. Through the unification of tools, Elastic Limitless XDR lets organizations ingest data from across their environment, store it in a single repository with a single schema, and perform and/or combine many types of searches to improve visibility and appropriate response.

Through this improved visibility, automated detection, and automation of routine tasks, the efficacy and performance of skilled analysts is fully realized. Perhaps equally important is the focus and efficiency of those valuable analysts being enhanced due to the reduction of time spent performing the mundane daily work that most often sees complacency and loss of focus.

Efficient, resource-based pricing

Elastic recognizes the importance of scalability both in scope of the attack surface to be protected and in the depth of the available data to analyze in that effort. The Elastic Stack enables threat hunters to investigate the historical context of data stored. This capability is often limited in other solutions due to their pricing model.

Elastic's resource-based pricing model is based on the resources used and aligns cost with the value received. This resource-based pricing eliminates the requirement of other solutions to count the number of documents ingested, seats needed, agents deployed, or hosts needed. Such rigid, inhibitive pricing models can get in the way of delivering the best search experience and can impede the effort to execute best security practices.

Elastic's resource-based pricing model enables the business to control costs by striking the perfect balance between performance and prioritization to the business function.

Elastic's pricing model scales well and allows the organization to limit the friction associated with growth through the flexibility it affords.

Summary

The mission at Elastic Security is to protect the world's data from attack. We are constantly innovating to ensure our users across the world are protected from tomorrow's attacks, today. The Elastic Limitless XDR solution delivers free and open capabilities of SIEM, endpoint security, and cloud security on a single platform built for limitless analysis — enabling organizations to prevent, detect, and respond before damage is done.

Elastic Security is more than the sum of its parts. The power and expertise of our community helps propel our solution and makes it more readily available to a wider range of users. Ultimately, the more accessible our solution is to security practitioners the world over, the more all parties involved benefit from a better-secured global ecosystem. That's why the Elastic Security XDR solution is designed free and open, so that it's readily available to analysts everywhere.

Limitless XDR is Elastic Security's answer to the data problem that is the crux of today's effective cybersecurity practice. It modernizes security operations, enabling analytics across all data and automating key processes to bring prevention and remediation capabilities to every host of an organization's continually expanding operational environment with the goal of increasing analyst efficacy by minimizing false positives via deep host data and environment-wide visibility.

Try Elastic Security free with a 14 day trial (no credit card required) to begin your organization's journey to a limitless approach to security.