BLOCKED!
Seven Pillars of Ironclad Endpoint Security

paloalto NETWORKS | CORTEX

Table of Contents

Introduction

From mobile devices to laptops and cloud containers, endpoints remain a target of increasingly complicated attacks. Many attacks rely on compromising an endpoint to succeed despite the fact that organizations have deployed some form of endpoint protection.

Attackers can easily bypass antivirus with inexpensive, automated tools, rendering traditional approaches to endpoint security ineffective at protecting against breaches. To effectively combat security threats, organizations need to arm themselves with the best endpoint protection available.

While focusing on prevention is critical, the ability to detect and respond swiftly to stealthy attacks has become a driving force in securing today's complex environments. What can security teams do to stop attackers from penetrating endpoints and deploying ransomware or stealing information? Sifting through the various vendor messages and sales pitches isn't easy.

Let's look at the current state of endpoint security technology to begin navigating this space.

Not All Endpoint Security Is Created Equal

Endpoint protection first got its start when antivirus software was developed to scan endpoint files for malware to detect and remove these files from computers. To keep up with evolving threats, next-generation antivirus (NGAV) was introduced to combat new forms of malware by using machine learning capabilities that no longer relied on signatures or consistent system scanning to identify already-infected devices.

While NGAV is a step in the right direction, it still leaves gaps in endpoint security that result in some organizations layering more tools on top of dated solutions. This only further complicates the problem, with multilayered solutions resulting in siloed SecOps, noisy alerts, increased false positives, and frustrated security teams trying to stay ahead of the security curve.

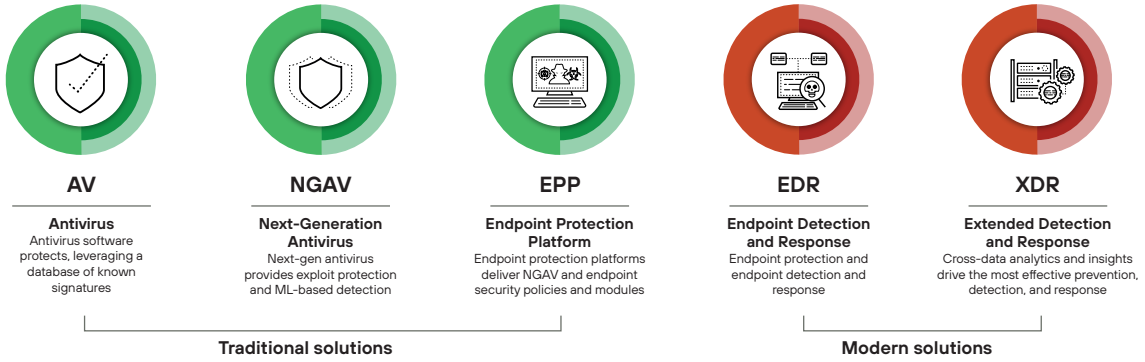

Figure 1: Endpoint security solutions available today

The rise of endpoint protection platforms (EPP) looked to address these gaps by combining NGAV together with solutions like host firewall, encryption, and USB device control for more elevated threat prevention. However, the nature of modern threats quickly identified a critical need that EPPs didn't address: the ability to detect and respond to the small percentage of threats, likely the most damaging, that can slyly bypass defenses.

Furthermore, the threat landscape has dramatically shifted with the advent of AI-generated attacks. Adversaries now leverage AI techniques to craft evasive malware, launch highly targeted campaigns, and rapidly adapt to defensive measures. These advanced threats easily bypass traditional endpoint protection, demanding a more intelligent and proactive approach. To counter this, organizations must adopt endpoint security solutions that use AI to their own advantage, countering adversarial AI. These technologies employ machine learning and advanced analytics to automatically prevent, detect, and respond to threats in real time, outmaneuvering adversaries and safeguarding critical assets.

To counter these advanced threats, cybersecurity solutions are evolving to incorporate more sophisticated AI and machine learning algorithms. These new solutions offer:

- Behavioral analysis to identify anomalous activities.
- Predictive analytics to anticipate and prevent potential threats.
- Real-time threat detection.
- Automated incident response and remediation.
- Continuous learning and adaptation to new threat patterns.

For cybersecurity practitioners, this evolution means:

- A shift from reactive to proactive security strategies.
- Increased focus on behavioral analysis and anomaly detection.
- Greater emphasis on threat intelligence and data analytics.
- The importance of integrating AI-driven solutions into existing security stacks.

The Need for Endpoint Detection and Response

Today's most popular and effective endpoint security strategy is to adopt endpoint detection and response (EDR) technology. EDR acknowledges that endpoint protection will never be perfect—it's impossible to block everything automatically. You may block 99% of breach attempts, but that still leaves 1% running wild. These attacks need to be discovered and mitigated using advanced detection and response capabilities.

As the endpoint security market has matured, EDR solutions have combined the best protection and detection capabilities to provide an extremely effective tool for protecting against threats that live on the endpoint. EDR

is instrumental in shortening response times for incident response teams and, ideally, eliminating threats before damage is done.

EDR brings a number of benefits to security analysts, including real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities. Faster investigations can be achieved through better visibility into incidents. Organizations that have already implemented an EDR solution report a reduced mean time to detect (MTTD) threats, a decrease in the number of alerts that go uninvestigated, and a reduction in average time to contain threats.

While EDR has proven to be a crucial component in modern endpoint security, the evolving threat landscape and the increasing complexity of IT environments have led to the development of extended detection and response (XDR). XDR builds upon the capabilities of EDR by integrating and correlating data from multiple security layers, including endpoints, networks, cloud workloads, identities, and applications.

The evolution of EDR to XDR provides several key advantages:

- **Holistic visibility**: XDR extends visibility beyond just endpoints, offering a comprehensive view of the entire IT ecosystem. This allows security teams to detect and respond to threats that may traverse multiple attack vectors.
- **Advanced threat correlation**: By analyzing data from various sources, XDR can identify complex, multistage attacks that might not be apparent when looking at endpoint data alone.
- **Streamlined operations**: XDR platforms often incorporate automation and orchestration capabilities, enabling more efficient threat investigation and response across the entire environment.
- **Improved threat hunting**: The broader dataset and advanced analytics provided by XDR enhance proactive threat hunting capabilities, allowing security teams to uncover hidden or emerging threats more effectively.
- **Reduced alert fatigue**: By correlating alerts from multiple sources, XDR can provide context-rich, high-fidelity incidents, reducing the number of false positives and helping security analysts focus on the most critical threats.

The 7 Pillars of Ironclad Endpoint Security

Today's endpoint security market is flooded with various options that may appear to potential buyers to all offer the same thing. But the fact is, as the endpoint security market has evolved, not all products have followed suit and not all companies are focused on continued innovation to stay ahead of attackers. To cut through the noise and pinpoint the most relevant security attributes you should demand when seeking an endpoint security solution, let's take a more detailed look at seven pillars of modern and effective endpoint security.

1. Cloud-Native Solutions

Cloud-native security solutions offer several key advantages over traditional on-premises solutions. These advantages include scalability, real-time updates and threat intelligence sharing across the entire protected organization, and reduced operational overhead, as maintenance and updates are managed by the security vendor.

Cloud-native solutions also facilitate better integration with other cloud-based security tools and services, enabling a more cohesive and comprehensive security strategy. Furthermore, they provide enhanced visibility and control across distributed workforces and remote endpoints, which is crucial in today's hybrid work environments. By leveraging the power and flexibility of cloud computing, these solutions can offer more robust threat detection and response capabilities, often utilizing advanced AI and machine learning algorithms that benefit from the vast computational resources available in the cloud. For cybersecurity professionals, adopting cloud-native endpoint security solutions is becoming increasingly essential to effectively protect modern organizations against evolving cyberthreats.

2. Advanced Threat Prevention

There are an estimated 450,000 new instances of malware registered every day.[1] Traditional antivirus solutions that rely on signature databases and updates just can't keep up with the sheer number of new threats. To stay ahead of today's pervasive threat environment, you should require best-in-class threat prevention that eliminates zero-day malware, ransomware, and fileless attacks. Look for a robust solution that includes NGAV and uses artificial intelligence (AI), machine learning, and behavior-based protection. These features should be delivered through a combination of cloud and local endpoint analysis.

Also, look for features like integrated host firewall and disk encryption to help lower endpoint security risk, meet regulatory requirements, and centrally manage endpoint security policies. Inclusion of Device Control allows management of USB access to ensure potential USB threats

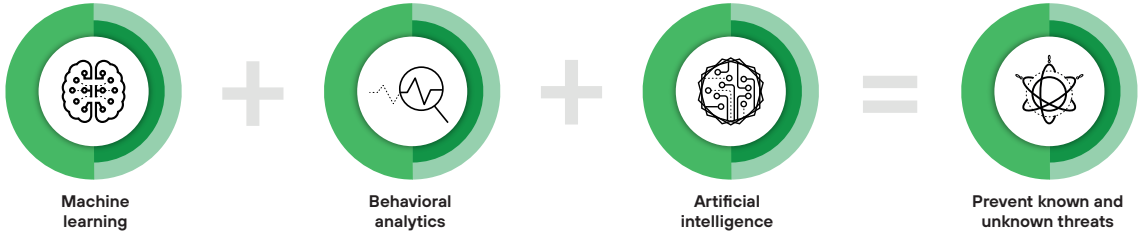

Figure 2: Analytics and machine learning help identify malware and block stealthy threats

1 "Malware," AV-Test, last accessed on August 8, 2024.

are mitigated, preventing malware and data loss. Additionally, vulnerability assessments can help to provide you with real-time visibility into vulnerability exposure and current patch levels across your endpoints.

The best endpoint protection solutions should block exploits by technique, block malware files using machine learning, and look across multiple behaviors to stop malicious behavior.

3. Superior Detection Capabilities

The most intricate and potentially damaging attacks can elude even the best defenses, requiring keen detection capabilities to quickly identify and stop unwanted activity before a breach occurs. The best way to identify these attacks is with rich data collection and detailed endpoint telemetry that is analyzed with machine learning.

Ideal endpoint security solutions will offer a comprehensive set of machine learning and analytics techniques. Using behavioral analysis to analyze user activity in real time can immediately detect intrusions and active attacks without interfering with endpoints. Detection systems must also be highly customizable based on the specific needs of your environment. This involves supporting both custom and predefined detections.

And finally, visibility is key. Telemetry data from multiple sources analyzed with machine learning can provide a clear view into an attack chain during the investigation of an incident.

Understanding the quality of detections is crucial when seeking an endpoint security solution. It's important to evaluate the types of threats the solution detects as well as the technology used for detection. Many solutions take a limited approach to detection and don't provide broad enough coverage of threats. Refer to independent tests such as the MITRE ATT&CK Evaluations to assess the breadth and accuracy of detection coverage. The ability of a solution to tag the MITRE ATT&CK tactics and techniques in alerts, incidents, and detection rules helps SOC teams gain insight into contextual technical details and adversary behavior to take swift, appropriate action.

Pro Tip

Need to quickly cut through the noise to understand if a vendor's detection claims are legitimate? Here's a list of innovative Threat Detection features to look for:

- Intelligent grouping of alerts into incidents
- ML-powered incident scoring
- Endpoint forensics, including memory data
- Cross-data analytics
- Cross-customer analytics
- Indexed, real-time search across endpoints
- Long-term data storage

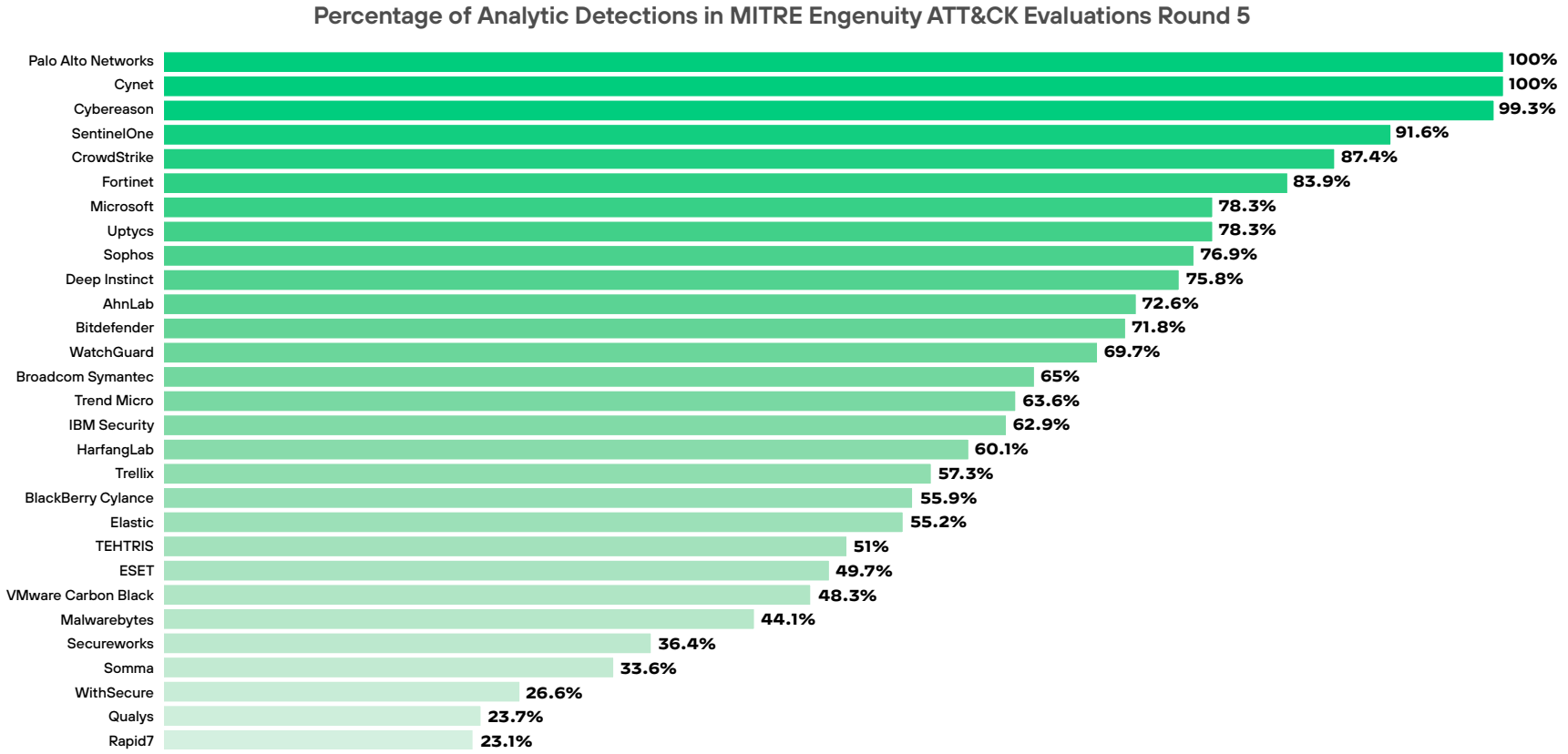

Figure 3: Cortex XDR delivered high-quality detections for every malicious action in the detection phase, notching a 100% Analytic Detection rate

4. Simplified Investigation and Response

To reduce response times, choose an endpoint security solution that can provide a complete picture of incidents with rich investigative details. Investigations should be simplified by using automation rather than requiring manual effort to reveal the root cause, sequence of events, and threat intelligence details of alerts. Security analysts shouldn't have to pivot between screens during investigations. This takes time away from other actions and adds complexity by requiring analysts to manually correlate different sources of data.

Advanced attacks, such as insider threats, low-and-slow attacks, and advanced persistent threats may require manual verification from a security analyst. With proper incident management, alerts can automatically be correlated and consolidated into incidents to reduce the number of individual alerts, streamline investigations, and speed incident response.

Automated response capabilities in EDR and XDR solutions have seen significant improvements in recent years, addressing many of the challenges previously faced by security teams:

- **Advanced AI-driven triage**: Modern solutions now employ more complex AI algorithms that can automatically prioritize and categorize alerts based on their potential impact and the organization's specific risk profile. This has dramatically reduced the number of alerts requiring manual investigation.
- **Contextual analysis**: Automated systems have become much better at understanding the context of potential threats. They can now correlate data from a wider range of sources, including user behavior analytics, threat intelligence feeds, and historical incident data, to provide a more accurate assessment of each alert.
- **Automated root cause analysis**: The ability to automatically trace the root cause of an incident has improved significantly. Modern systems can now quickly reconstruct the attack chain, identifying initial entry points and subsequent lateral movements without manual intervention.
- **Adaptive response playbooks**: Automated response capabilities now include adaptive playbooks that can adjust their actions based on the specifics of each incident. These playbooks can initiate a series of automated actions, from isolating affected endpoints to initiating system rollbacks or patch deployments.
- **Integration with SOAR**: Tighter integration with security orchestration, automation, and response (SOAR) technologies has enabled more comprehensive automated responses across the entire security infrastructure, not just at the endpoint.
- **Machine learning-enhanced false positive reduction**: Significant strides have been made in reducing false positives through advanced machine learning techniques. These systems can now learn from past incidents and analyst feedback to continually improve their accuracy.

- **Automated threat hunting**: Proactive threat hunting has become more automated, with systems able to continuously scan for indicators of compromise or unusual patterns that might signal a nascent attack.
- **Real-time collaboration features**: Automated systems now include features that facilitate real-time collaboration among security team members, automatically assigning tasks and sharing relevant information to speed up manual investigations when needed.

These advancements have significantly improved the efficiency of security operations, reducing the time required for threat detection and response, and allowing security analysts to focus on more complex, strategic tasks. The integration of these automated capabilities with human expertise has created a more robust and responsive security posture for organizations adopting these advanced EDR and XDR solutions.

5. Ease of Deployment and Management

Endpoint security should help to maximize productivity through a platform that includes endpoint policy management, detection, investigation, and response in a single management console. Disjointed tools force analysts to pivot from console to console to investigate incidents, resulting in slow investigations and missed attacks.

Cloud-native platforms offer streamlined deployment, eliminating the need to deploy new on-premises log storage or network sensors. Agents should be easy to install, with no need to reboot endpoints to begin protection. Modern endpoint security options simplify operations by eliminating the need for on-premises logging and management servers. End users will experience better performance and less disruption compared to burdensome and resource-hogging antivirus.

6. Identity-Based Security

Identity-based security has emerged as a critical component of modern endpoint security strategies, reflecting the evolving nature of cybersecurity threats and the changing risk environment of enterprise IT. As organizations increasingly adopt cloud services, support remote work, and manage a diverse array of devices, compromised identities are increasingly used within the attack chain. Identity has become the new perimeter, serving as the primary control point for accessing corporate resources and data.

More advanced XDR solutions have the ability to incorporate data from identity providers and correlate that data with all other sources to understand the role of identities in an attack. Security analysts can be notified automatically if a compromised identity is detected and take automated or precise action to remediate the issue and halt the attack.

7. Industry Validation and Independent Testing

When evaluating endpoint security solutions, you should always seek out those that are mature, with proven performance through third-party testing, analyst validation, and customer testimonials. Seek analyst research, validate performance, and request a demo or production environment to test for interoperability, integration, and organizational fit.

The MITRE Engenuity Evaluations are intended to help vendors and end users better understand a product's capabilities in relation to MITRE's publicly accessible ATT&CK framework. MITRE developed and maintains the ATT&CK knowledge base, which is based on real-world reporting of adversary tactics and techniques. Review the results in detail, noting the importance of attack prevention and quality of detections provided without delays or configuration changes required.

AV-Comparatives provides an Endpoint Prevention and Response (EPR) Test to help validate the effectiveness of antimalware solutions. This evaluation takes into account endpoint threat prevention, ease of use, and thoroughness of investigation and response capabilities, examining both security efficacy and total cost of ownership.

And finally, each organization's environment is unique. Testing a solution during a proof of concept (PoC) and in production in the form of a pilot is critical for assessing its integration, usability, and interoperability.

Figure 4: EPR CyberRisk Quadrant™ by AV Comparatives

An Industry Leader

Cortex XDR was awarded Strategic Leader in the 2023 Endpoint Prevention and Response Test for the ability to block every attack scenario tested at the lowest total cost of any vendor in the evaluation. This result, coupled with our recent performance in the 2023 MITRE Engenuity ATT&CK® Evaluations demonstrates our deep commitment to security efficacy and the operational efficiency of SOC teams that place their trust in our technology.

Future-Proof Security: Extending Protection Beyond the Endpoint with XDR

While EDR provides a strong endpoint security solution, it only solves one piece of the puzzle and SOC teams only have limited time and resources to put everything together. With EDR capabilities as a cornerstone, XDR expands and unifies threat detection and response, improving security and reducing the need for siloed specialty tools. Organizations seeking to implement EDR can improve their defenses by advancing to XDR, which correlates data collected from endpoint, network, cloud, and identity sources to detect threats with machine learning analytics, giving security operations a comprehensive view of the attacks they face and the ability to eliminate them faster. Consolidation of siloed security tools arms SOC teams with a single platform to use for protection, detection, investigation, and response.

The integration of XDR with SOAR platforms can further improve security outcomes. This integration aims to create a more unified and efficient security operations ecosystem, capable of replacing security information and event management (SIEM) solutions:

XDR–SOAR Integration

- **Automated response orchestration**: XDR triggers can now seamlessly initiate SOAR playbooks, allowing for more rapid and coordinated incident response across the entire IT infrastructure.
- **Enriched incident data**: SOAR platforms can pull detailed contextual data from XDR to enhance incident investigation and response processes.
- **Feedback loop**: Actions taken by SOAR playbooks can be fed back into XDR systems, helping to refine detection rules and improve future threat identification.

Unified Security Operations

The integration of XDR and SOAR has led to the concept of unified security operations platforms, replacing SIEM. These solutions aim to provide a single pane of glass for security teams, combining the strengths of each technology:

- Comprehensive visibility across the entire attack surface.
- Streamlined workflow from detection to response.
- Reduced alert fatigue through better prioritization and automation.
- Improved mean time to detect (MTTD) and mean time to respond (MTTR).

Cortex XDR

Regardless of where you are in your endpoint strategy, Cortex XDR® can help by providing a single platform to meet your current needs and prepare you for the future.

Security teams frequently express frustration with the overwhelming number of tools they must manage, often needing to switch between multiple consoles to investigate alerts. Despite these tools, threats still manage to bypass defenses. Cortex XDR addresses these issues by being the first extended detection and response platform that consolidates data from any source. With advanced behavioral analytics and machine learning, Cortex XDR accurately detects threats and simplifies investigations by uncovering the root cause of alerts. Its tight integration with enforcement points speeds up containment, allowing you to halt attacks before they can cause significant damage.

Cortex XDR provides:

- **Best-in-class endpoint threat prevention**: Named a Strategic Leader in the 2023 AV-Comparatives Endpoint Prevention and Response (EPR) Test, Cortex XDR provides ironclad endpoint security to stop attacks.
- **Industry-leading detection accuracy**: In the 2023 MITRE Engenuity ATT&CK Evaluations, Cortex XDR stood alone in providing 100% Protection while delivering 100% Visibility and 100% Analytic Coverage (detections) with zero configuration changes or delayed detections.
- **Accelerated investigation and response**: Cortex XDR cuts investigations by 88% with root cause analysis and intelligent alert grouping.
- **Award-winning, analyst-recognized endpoint security**: Cortex XDR has been recognized as a Leader in the 2023 *Gartner® Magic Quadrant™ for Endpoint Protection Platforms (EPP)*, and a Leader in *The Forrester Wave™: Extended Detection and Response (XDR) Platforms, Q2 2024*, with several acknowledgments:
  - › **Commitment to disruption**—evident from our monetary investment in R&D and continuous delivery of quality features
  - › **Empowering analysts**—to detect and respond effectively
  - › **Enhancements**—centered on enabling more platform features and analytics for identity and cloud
- **Flexible response**: With the broadest set of response options in the industry, including Live Terminal, Search and Destroy, script execution, and host restore, Cortex XDR lets security teams instantly stop fast-moving threats.
- **Enterprise-wide attack protection**: Cortex XDR can collect cloud, network, identity, and many other data sources to extend detection and response across your entire enterprise.

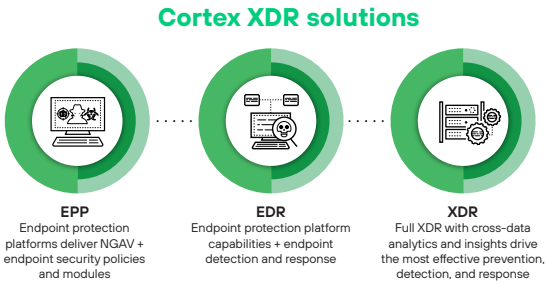

Figure 5: Cortex XDR provides a single, unified platform for endpoint protection, endpoint detection and response, and extended detection and response

The Imperative of Advanced Endpoint Security

In today's environment of sophisticated cyberthreats, robust and adaptive endpoint protection is essential. Endpoints are prime targets for cybercriminals, acting as gateways to an organization's network and sensitive data. The shift to cloud-native solutions, the integration of AI and machine learning, and the evolution from traditional antivirus to advanced EDR and XDR platforms highlight the dynamic nature of endpoint security. These advancements enhance threat prevention, detection, and incident response, easing the burden on security teams and minimizing breach impacts.

As endpoint security converges with identity-based protection, cloud security, and broader IT infrastructure defense, organizations must adopt integrated strategies that adapt to evolving threats. Investing in cutting-edge solutions and continuously evolving security postures are critical for protecting assets, maintaining continuity, and building resilience. In an era where a single compromised endpoint can have devastating consequences, endpoint security isn't just a technical necessity but a fundamental business imperative.

Protect Your Endpoints. Learn More Today.

- XDR For Dummies
- The Essential Guide to the 2023 MITRE Engenuity Evaluations
- Endpoint Prevention and Response (EPR) Product Validation Report Palo Alto Networks Cortex XDR Pro
- Cortex XDR Datasheet

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

cortex_eb_blocked!-seven-pillars-of-ironclad-endpoint-security_082924