paloalto NETWORKS | CORTEX

The Essential Endpoint Security Buyer's Guide

Learn the Most Important Capabilities That Enterprise Endpoint Security Must Deliver

TABLE OF CONTENTS

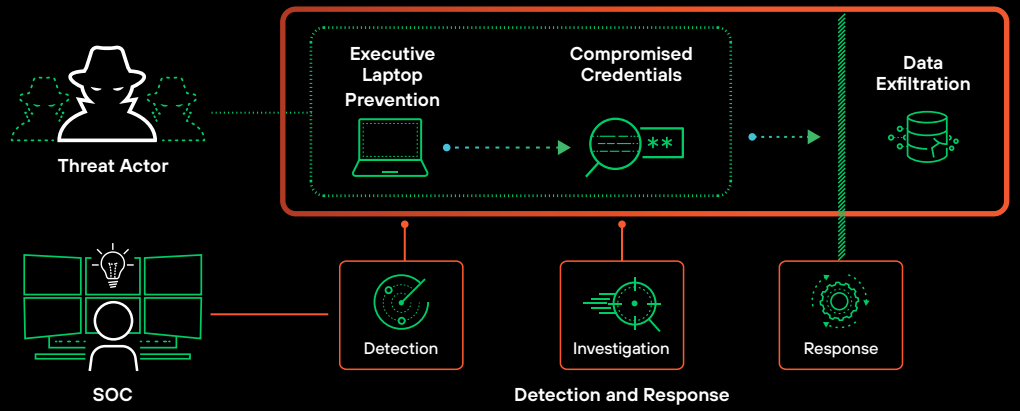
OVERVIEW

Advanced persistent threats, ransomware as a service, and AI-powered attacks are redefining the security game and challenging organizations to stay ahead of the security curve. Unfortunately, today's siloed security solutions struggle to keep pace with these evolving threats, leaving organizations vulnerable to attacks. This means attackers gaining access to your organization isn't a matter of "if" but of "when."

Security teams are overwhelmed by an abundance of alerts, complex investigations, and the constant risk of missed attacks. Drowning in data is hardly an understatement as organizations increase their digital footprint in the cloud and everywhere else, exponentially increasing the volume and variety of security telemetry to be analyzed.

Endpoint security is the foundation of cyberdefense. It's where attackers get stopped or succeed in their initial compromise, and it's where the most useful data comes from to hunt them down. It's critical to security posture overall and to security operations (SecOps), who need to see and stop cyberattacks before a breach.

To that end, a robust **endpoint security strategy** is vital to stay ahead of the security curve. It should provide comprehensive visibility and analytics across traditional endpoints, networks, cloud workloads, mobile devices, identities, and beyond, enabling rapid detection and response with a unified approach that supports the growing importance of security operations.



> By 2028, 30% of enterprises will adopt preventative endpoint security, endpoint detection and response, and identity threat detection and response from the same vendor, up from approximately 5% in 2024.
>
> - Gartner[1]

[1] Evgeny Mirolyubov et al., Magic Quadrant for Endpoint Protection Platforms, Gartner, September 2024.

NAVIGATING ENDPOINT SECURITY: KEY CHALLENGES FOR SECURITY ROLES

Key Challenges for Security Roles

CISOs

Chief information security officers (CISOs) grapple with justifying security investments to the board while demonstrating tangible improvements in the organization's security posture. They face the challenge of translating technical metrics into business value, managing risk in an ever-evolving threat landscape, and ensuring compliance with various regulations. CISOs must also balance the need for robust security measures with business agility and user productivity, all while operating within budget constraints and addressing the cybersecurity skills gap.

SecOps Leads

SecOps, or security operations center (SOC) leads are tasked with ensuring their team has the right knowledge, processes, and tools to respond effectively to any threat. They face challenges in understanding adversary tactics and techniques, coordinating responses across multiple tools and platforms, and managing alert fatigue and burnout within their team. SecOps leads must also continually adapt their strategies to address new types of threats, optimize resource allocation, and improve mean time to detect (MTTD) and mean time to respond (MTTR).

Security Architects

Security architects face the challenge of designing and implementing a comprehensive endpoint security strategy that addresses evolving threats while integrating seamlessly with existing infrastructure and security operations. They struggle with identifying and closing potential blind spots in security controls, managing the proliferation of security tools, and ensuring interoperability between various solutions. Their primary concern is continuously improving the organization's security posture while balancing effectiveness, cost, and user experience.

Security Analysts

Security analysts are on the front lines of threat detection and response, dealing with a constant stream of alerts and potential security incidents. They struggle with alert fatigue, often chasing false positives that consume valuable time. Their primary challenges include prioritizing alerts effectively, reducing investigation time, and balancing routine tasks with proactive threat hunting and in-depth analysis of critical incidents.

THE TOP 10 QUESTIONS TO ASSESS ENDPOINT SECURITY PROVIDER CAPABILITIES

1. How Does the Solution Handle the Detection of Sophisticated Attacks?

Endpoint Detection and Response (EDR) Capabilities

Look for a solution that offers state-of-the-art endpoint detection and response capabilities that continuously monitor endpoints for signs of malicious activity, allowing for rapid detection and response to sophisticated threats.

Rich Endpoint Data Collection

An effective solution should collect extensive telemetry from endpoints to uncover potential threats. By gathering process information, file activity, network connections, registry changes, user activity, and more, the solution can detect threats that might be missed by more narrowly focused tools.

Machine Learning (ML) and Behavioral Analysis Techniques

Look for solutions employing numerous, continuously updated machine learning models for automated threat prevention and detection. These should leverage real-world insights from cybersecurity experts, automatically incorporating the latest threat intelligence. This approach significantly reduces manual analysis time, accelerates threat detection and response, and frees analysts to focus on critical incidents.

Customizable Detection Rules and Predefined Detections

While a solution should come with a wealth of out-of-the-box analytics and detection rules, it should also offer flexibility for customization. Security teams should be able to create and fine-tune detection rules to address their organization's specific needs and threat landscape. This combination of predefined and customizable detections ensures comprehensive coverage against a wide range of advanced attacks.

2. What Advanced Threat Prevention Capabilities Does the Solution Offer?

Multilayered Approach

Implement a defense-in-depth strategy that integrates exploit prevention, AI-powered malware analysis, cloud-based file inspection, behavioral threat detection, and ransomware safeguards—ensuring that if an attack evades one layer, it's caught by another—creating a comprehensive security mesh that protects against sophisticated threats from malware to fileless attacks.

Behavior-Based Protection and Exploit Prevention

Ensure the solution leverages advanced Behavioral Threat Protection to analyze interrelated process behaviors and reveal active attacks. This comprehensive monitoring enables detection of multistage threats that may be missed when processes are examined individually, while robust Exploit Protection Modules provide critical safeguards against OS and application vulnerabilities.

AI- and Machine Learning-Based Protection

Implement an AI-driven security engine that scrutinizes all incoming files while continuously learning to counter emerging attack patterns, enabling the detection and blocking of sophisticated threats that traditional signature-based defenses might miss.

3. What is the Solution's Approach to Investigation and Response?

Automated Alert Correlation into Incidents

Seek a solution that leverages machine learning to automatically group related alerts into unified incidents, substantially reducing alert fatigue and enabling analysts to focus their attention on high-priority security issues.

Incidents Prioritized by Risk and Scored

Deploy a machine learning-based system that analyzes and scores incidents based on risk factors, enabling rapid assessment of attack scope and impact to ensure optimal allocation of security resources.

Root Cause Analysis and Attack Chain Visualization

Look for capabilities that automatically uncover root causes while providing reputation data and visual attack chain mapping for each incident, enabling analysts to rapidly understand threat context and scope.

Automated and Manual Response Options

Implement a flexible response framework that combines automated actions for routine threats with manual intervention options for complex scenarios, enabling security teams to execute both rapid, automated remediation and carefully tailored responses based on threat context.

Integration with SOAR Platforms

Choose a solution that seamlessly integrates with SOAR platforms to enhance automated workflows and streamline incident response processes across the security stack.

4. How Does the Solution Address the Challenges of Alert Fatigue and False positives?

Seek a Solution that Employs Intelligent Alert Grouping and Incident Scoring Capabilities Using AI-driven Alert Triage and Prioritization

Look for an AI-powered solution that intelligently groups and scores alerts, automatically correlating related events while assessing risk based on impact and threat likelihood. The system should leverage contextual analysis of asset criticality, user behavior, and threat intelligence, while continuously learning from analyst feedback to improve prioritization accuracy and reduce false positives through advanced behavioral analytics.

Reduction of False Positives Through Advanced Analytics

The ideal system should leverage AI-powered analytics and cross-data correlation from endpoints, networks, and cloud environments to accurately differentiate between genuine threats and benign anomalies, minimizing false positives through contextual analysis.

5. How Does the Solution Extend Beyond Traditional EDR to XDR Capabilities?

Effective on Its Own with Just Endpoint Data, but It Can Broaden Context for More Detections and Workflow Consolidation

Find a solution that delivers robust protection using endpoint data alone, while seamlessly incorporating network, identity, and cloud data sources when available to enhance threat detection context and streamline security workflows.

Integration of Data from Extended Sources

Look for the ability to seamlessly integrate data from various sources such as networks, cloud environments, and identity systems because attackers move across multiple environments and single-source visibility leaves dangerous blind spots.

Cross-Data Analytics and Threat Correlation

The solution should offer advanced analytics that can correlate threats across different data sources, providing a more comprehensive view of active security incidents.

Complete Context of an Attack

The ideal solution should provide complete visibility into the entire attack chain, from initial entry to lateral movement and data exfiltration attempts, using a common framework like MITRE ATT&CK.

Transformation to a Unified SOC Platform

Seek a platform that consolidates multiple security tools into a single interface and data source while ensuring extensibility across major SOC technologies, including SOAR, next-generation SIEM, and attack surface management.

6. How Does the Solution Deliver Cloud Detection and Response?

Runtime Security Tuned for Cloud-Specific Architectures (e.g., Containers, Kubernetes, VMs)

The solution should be optimized for the cloud architectures, including containers, Kubernetes, and should offer runtime security that's specifically tuned for these cloud-native architectures, ensuring comprehensive protection across diverse cloud workloads.

Combines Runtime Telemetry with Agentless Scanning and Cloud Service Provider (CSP) Log Data for Comprehensive Understanding of Cloud Activity

Look for a comprehensive cloud monitoring solution that merges runtime telemetry, agentless scanning, and CSP log data with CNAPP security insights to provide complete visibility into cloud activity and workload behavior.

ML-Based Detection/Response and Incident Management Workflows

Choose a solution that runs on an ML-driven security platform that delivers unified detection and response capabilities across cloud and on-premises environments, supporting hybrid and multicloud architectures while maintaining consistent workflows for security teams.

7. How Does the Solution Incorporate Identity-Based Security?

Integration with Identity Providers

Ensure the solution integrates seamlessly with key identity providers like Active Directory and Okta to ingest comprehensive user activity data, providing essential context for enterprise-wide threat detection and response.

Correlation of Identity Data with Other Security Telemetry

Find a solution that correlates identity data with broader security telemetry to deliver comprehensive user activity visibility, incorporating risk scoring and UEBA capabilities to rapidly identify suspicious behavior patterns.

ML-Based, Automated Detection and Response to Compromised Identities

Deploy an ML-powered identity threat detection and response (ITDR) system that automatically identifies abnormal user and entity behaviors to uncover compromised credentials and insider threats, while enabling rapid automated responses to mitigate identity-based attacks.

8. How Does the Solution Simplify Deployment and Management?

Single-Agent Installation and No Reboot Needed After Deployment

This minimizes disruption to end users and allows for rapid deployment and updates across large environments.

Best Practice Security Policies on by Default

This ensures a strong security posture from day one, while still allowing for customization to meet specific needs.

Granular and Phased Control Over the Rollout of Security Content Updates

This allows for testing and rolling out new security content in a phased manner, ensuring stability and minimizing potential disruptions.

Unified Management Console

Seek a solution that provides comprehensive security management through a single, intuitive console—from endpoint policy management to threat detection, investigation, and response—streamlining administration while delivering a cohesive view of the organization's security posture.

Performance Impact on Endpoints

The agent should operate with minimal impact on endpoint performance through low CPU utilization and I/O, ensuring robust security without compromising user productivity or system performance.

Scalability for Large Enterprises

It should easily accommodate growing numbers of endpoints and increasing data volumes without requiring significant infrastructure investments.

9. What Industry Validations and Independent Test Results Support the Solution's Efficacy?

Performance in MITRE Engenuity ATT&CK Evaluations

Check the solution's performance in recent MITRE Engenuity ATT&CK Evaluations. Look for high combined protection and detection scores, ideally with strong out-of-the-box effectiveness without requiring configuration changes. Pay attention to metrics such as analytic coverage and the presence of delayed detections.

Results from AV-Comparatives and Other Independent Tests

Look for high scores in endpoint prevention and response tests, which validate the solution's effectiveness in real-world scenarios.

Customer Testimonials and Analyst Recognition

Consider both peer feedback through industry-specific testimonials that demonstrate real-world performance and the solution's standing in analyst reports like The Forrester Wave™ and Gartner® Magic Quadrant™, as these validate market position and technological capabilities.

10. Does the Solution Support the Progression from EDR to XDR and Ultimately to Full SOC Transformation with AI and Automation?

Foundation for Progressive Growth

Seek a solution that combines core EDR capabilities—including advanced threat prevention, detection, and response—with essential endpoint protection features such as host firewall, disk encryption support, and Device Control for comprehensive security at the endpoint level.

Evolution to XDR Capabilities

Evaluate how the solution expands to XDR by integrating network, cloud, identity, and third-party data for unified visibility and automated correlation across all security telemetry.

Path to Complete SOC Transformation

Ensure the platform can scale for complete automation with SOAR and next-generation SIEM capabilities that reduce attack response from days to minutes.

Future-Proof Architecture

The solution should provide a unified backend that supports your progression through all three stages—from EDR to XDR to a true SOC platform—while maintaining consistent workflows and leveraging AI-driven automation throughout.

CONSIDER CORTEX FOR A FUTURE-PROOFED ENDPOINT SECURITY STRATEGY

After considering the 10 crucial questions for transforming your endpoint security strategy, it becomes clear that a comprehensive, intelligent approach is essential in today's rapidly evolving threat landscape.

Cortex XDR® emerges as a solution that addresses these key considerations, offering advanced threat prevention, detection, and response capabilities that extend well beyond traditional endpoint security.

Cortex XDR's AI-driven approach tackles the challenges highlighted in this paper. It delivers industry-best performance in threat defense, with 100% detection in the 2024 MITRE Engenuity ATT&CK Evaluations. Cortex XDR significantly reduces alert fatigue and false positives, stitches data from multiple sources for a holistic view, and offers both automated and manual response options. These features, combined with its cloud-ready architecture and identity security integration, position Cortex XDR as a powerful tool for modern security teams.

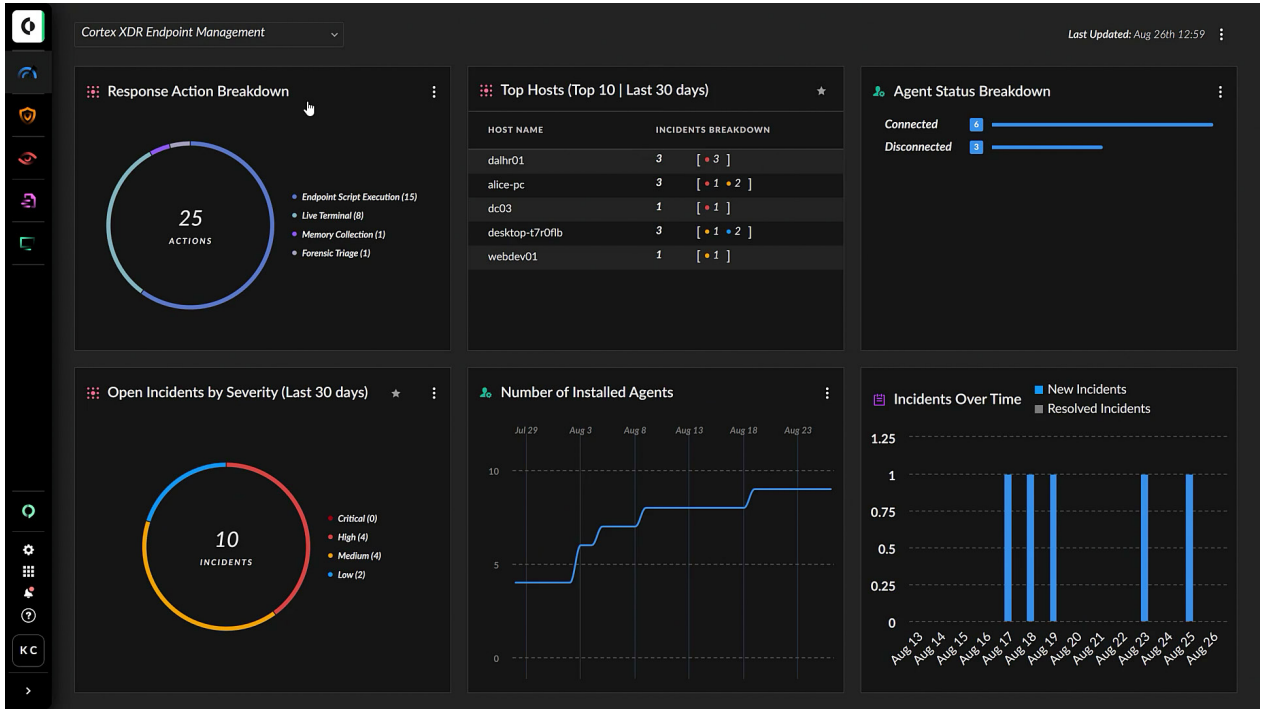


Figure 1: Cortex XDR Endpoint Management

For organizations looking to transform their SOC, Cortex XDR provides a scalable foundation. Its architecture allows security teams to start with core EDR functionalities and gradually expand to full XDR capabilities, aligning with the evolving needs of the organization.

As the next step in this security journey, Cortex XSIAM® builds upon Cortex XDR's capabilities by expanding response automation with SOAR and data ingestion with a revolutionary AI-driven approach to next-generation SIEM. The XSIAM platform transforms security operations with AI and automation to stop attacks in minutes, instead of days or weeks.

By choosing Palo Alto Networks Cortex® solutions, organizations invest in a security strategy that not only addresses current needs but is also poised to tackle future challenges. With its commitment to ongoing R&D, adaptation to emerging threats, and a clear roadmap for addressing future security needs, Cortex XDR and XSIAM offer a path to a more resilient, efficient, and effective security posture in an increasingly complex digital world.

Experience these capabilities firsthand by taking the Cortex XDR product tour, where you can explore the platform's advanced features and see how it transforms endpoint security operations.

COMPREHENSIVE MDR
EXPERT SECURITY OPERATIONS AROUND THE CLOCK

Our Managed Detection and Response (MDR) service, powered by Cortex XDR technology, provides comprehensive 24/7 security coverage by combining human expertise with advanced threat detection and response capabilities. We help organizations of all sizes strengthen their security posture through alert management, incident response, and proactive threat hunting.

Our flexible, outcome-based approach includes customized rules and playbooks tailored to your organization's unique requirements, supported by time-based SLAs for detection and response. By partnering with us, you can instantly mature your security operations, freeing your team to focus on strategic initiatives while we handle the complexities of modern security threats.

Secure your future with Unit 42 MDR for Cortex XDR.

Learn More →

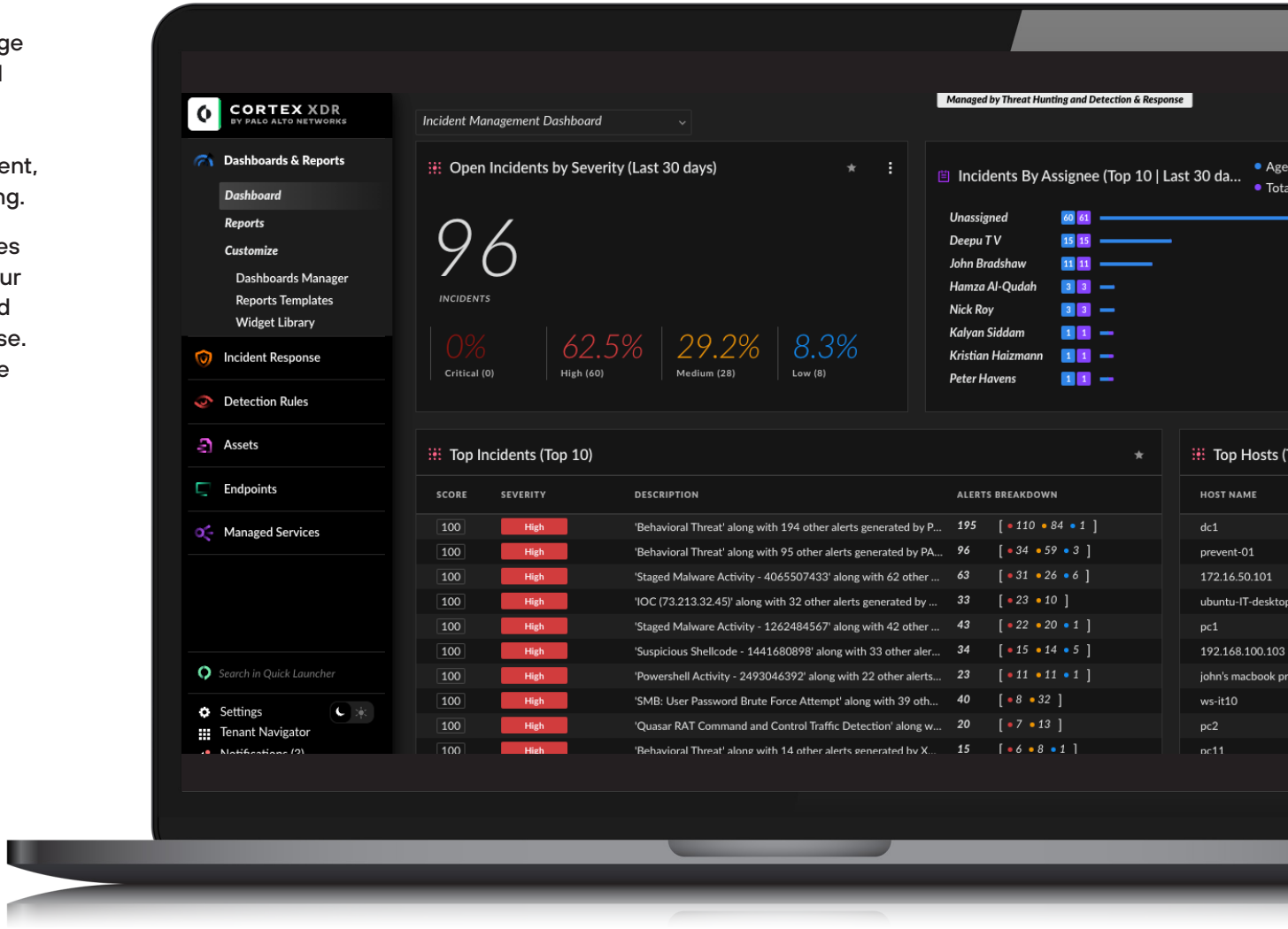
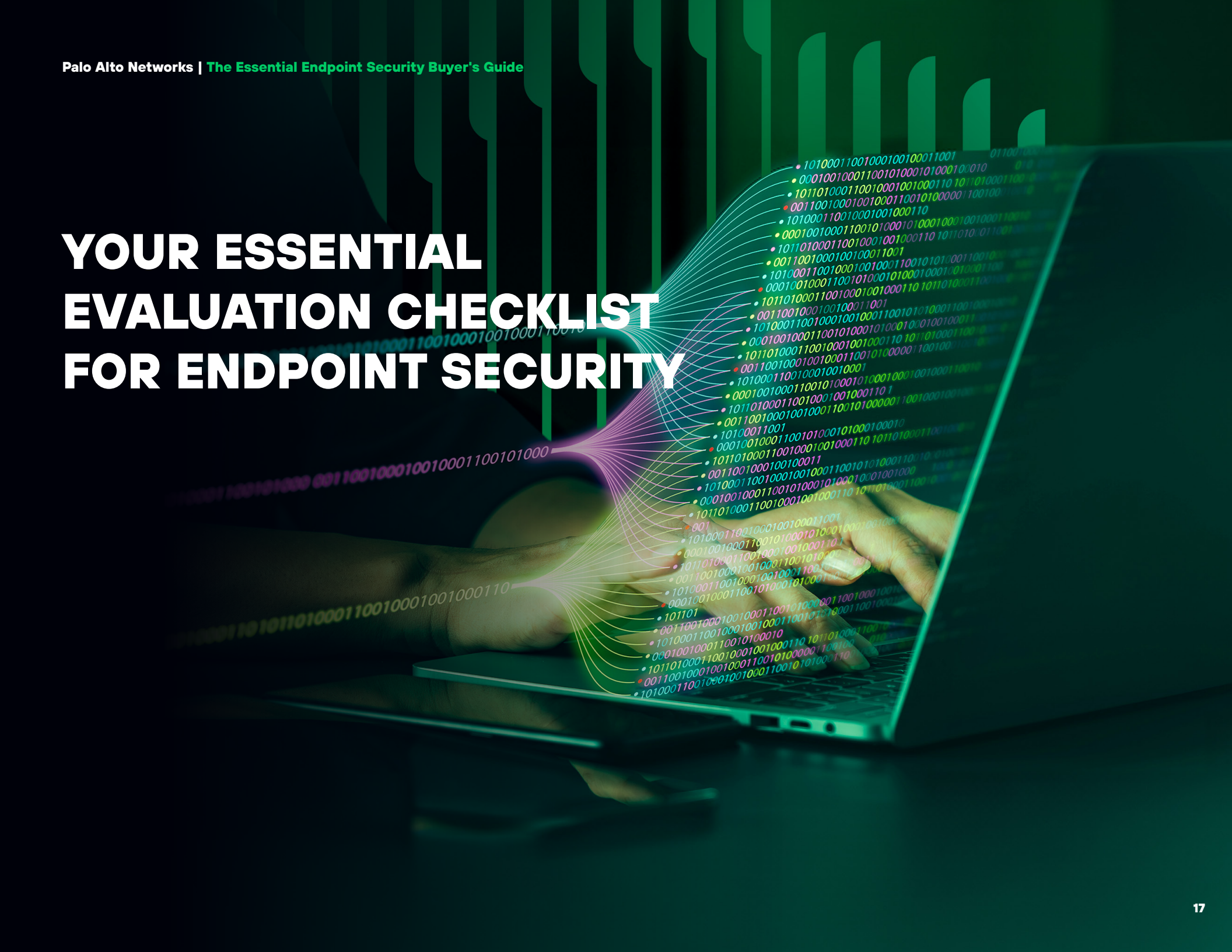


Figure 2: Cortex XDR with Unit 42 Managed Detection & Response (MDR) dashboard

YOUR ESSENTIAL EVALUATION CHECKLIST FOR ENDPOINT SECURITY



Advanced Threat Prevention

Multilayered Protection Capabilities

- ☐ Next-generation antivirus features
- ☐ Ransomware protection
- ☐ Fileless attack prevention
- ☐ Exploit prevention modules
- ☐ Behavior-based protection

AI-/ML-Based Protection Engine

- ☐ Local sandbox capabilities
- ☐ Continuously updated models

Additional Security Features

- ☐ Host firewall functionality
- ☐ Disk encryption support
- ☐ Device control capabilities

Detection Capabilities

EDR Fundamentals

- ☐ Real-time monitoring
- ☐ Comprehensive endpoint telemetry collection
- ☐ Cross-source event correlation

Machine Learning and Analytics

- ☐ Behavioral analysis capabilities
- ☐ Multiple ML models for different threat types
- ☐ Regular model updates

Detection Flexibility

- ☐ Prebuilt detection rules
- ☐ Custom detection creation options
- ☐ MITRE ATT&CK framework alignment

Investigation and Response

Alert Management

- ☐ Automated alert correlation
- ☐ Risk-based prioritization
- ☐ False positive reduction capabilities

Investigation Tools

- ☐ Root cause analysis features
- ☐ Attack chain visualization
- ☐ Detailed incident context

Response Options

- ☐ Automated response capabilities
- ☐ Manual response tools
- ☐ SOAR platform integration

Extended Detection and Response

Data Integration

- ☐ Network data ingestion
- ☐ Cloud security integration
- ☐ Identity provider integration

Cross-Data Analytics

- ☐ Multisource correlation
- ☐ Unified incident view
- ☐ Extended context for investigations

Cloud Security

Cloud Workload Protection

- ☐ Container security
- ☐ Kubernetes protection
- ☐ VM security

Cloud Integration

- ☐ Cloud provider log integration
- ☐ CNAPP integration
- ☐ Multicloud support

Deployment and Management

Implementation

- ☐ Single agent architecture
- ☐ No-reboot deployment
- ☐ Default security policies

Administration

- ☐ Unified management console
- ☐ Role-based access control
- ☐ Policy management tools

Performance

- ☐ Low system impact
- ☐ Scalability for enterprise
- ☐ Bandwidth optimization

Validation and Testing

Industry Recognition

- ☐ MITRE ATT&CK evaluation results
- ☐ Independent test scores (AV-Comparatives, etc.)
- ☐ Analyst recognition (Gartner, Forrester)

Customer Validation

- ☐ Customer references in your industry
- ☐ Case studies
- ☐ Production environment testing results

Future-Proofing

Vendor Assessment

- ☐ R&D investment
- ☐ Feature release cadence
- ☐ Threat research capabilities

Roadmap Evaluation

- ☐ Planned feature additions
- ☐ Technology partnerships
- ☐ Integration capabilities

Platform Evolution

- ☐ Extensible to a complete SOC platform
- ☐ AI/ML development plans
- ☐ Automation capabilities

Cost and Support

Pricing Structure

- ☐ Licensing model
- ☐ Additional module costs
- ☐ Volume discounts

Support Services

- ☐ 24/7 technical support
- ☐ Implementation assistance
- ☐ Training resources

Compliance and Reporting

Regulatory Compliance

- ☐ Built-in compliance reporting
- ☐ Support for major regulations (GDPR, HIPAA, PCI DSS, etc.)
- ☐ Custom compliance report creation

Audit Support

- ☐ Audit trail capabilities
- ☐ Historical data retention options
- ☐ Evidence collection tools

Integration Capabilities

Security Tool Integration

- ☐ SIEM integration
- ☐ Threat intelligence platform integration
- ☐ Ticketing system integration

API Availability

- ☐ REST API documentation
- ☐ Custom integration support
- ☐ API rate limits and quotas

Data Export

- ☐ Custom report generation
- ☐ Raw data export capabilities
- ☐ Data format options

Use this checklist as your guide to selecting a comprehensive endpoint security solution that not only meets your current needs but provides a foundation for your security operations transformation. The right choice will protect your organization today while scaling to address tomorrow's emerging threats.

Vendor Assessment

Company Stability

- ☐ Financial health
- ☐ Market presence
- ☐ Customer retention rate

Support Infrastructure

- ☐ Global support coverage
- ☐ Support response SLAs
- ☐ Knowledge base quality

Community Resources

- ☐ User community size
- ☐ Community forums
- ☐ Third-party integrations marketplace

Operational Requirements

Offline Capabilities

- ☐ Offline protection features
- ☐ Local detection capabilities
- ☐ Data caching mechanisms

Backup and Recovery

- ☐ Agent backup options
- ☐ Configuration backup
- ☐ Disaster recovery support

Resource Optimization

- ☐ CPU usage controls
- ☐ Memory optimization
- ☐ Network bandwidth management

Get Started Today

Schedule your demo to discover how Cortex XDR can help you and your organization simplify operations, stop threats at scale, and accelerate incident remediation today and in the future.

3000 Tannery Way
Santa Clara, CA 95054

Main	+1.408.753.4000
Sales	+1.866.320.4788
Support	+1.866.898.9087