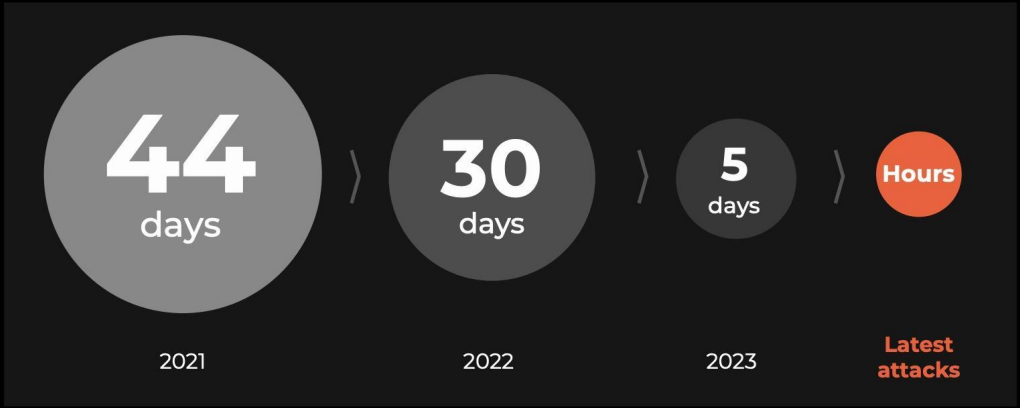
The Modern SOC, Reimaged

Luis Trincheiras
Systems Engineer
ltrincheiras@paloaltonetworks.com

Attacks are happening faster than organizations can respond

Average Days from "Compromise" to "Exfil" [1]

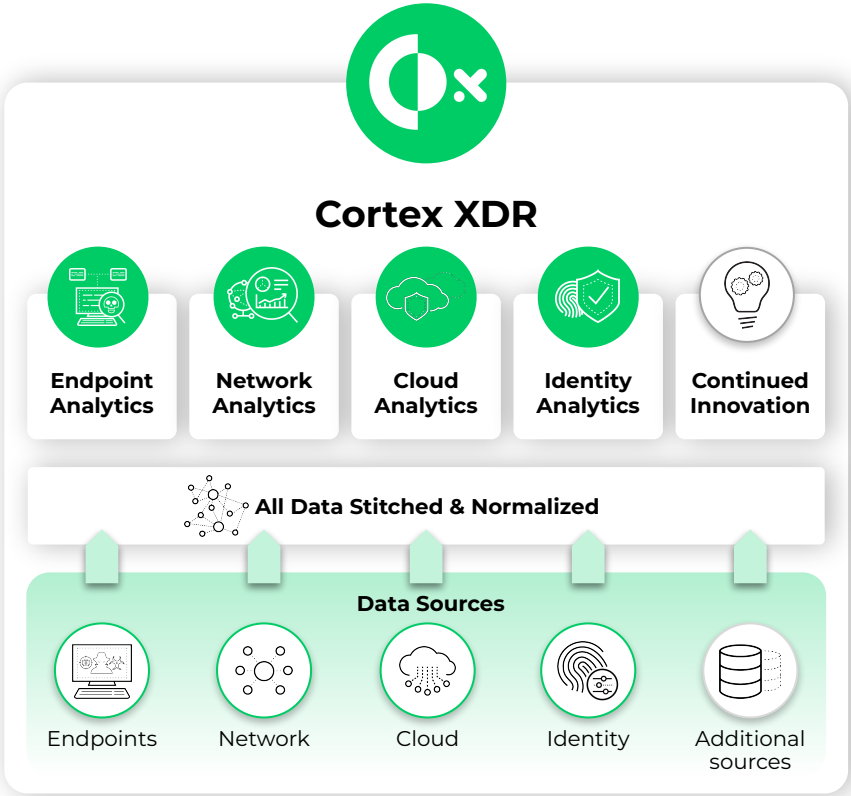


Industry average
6 DAYS
to remediate

SEC adopted rule
4 DAYS
to disclose material cybersecurity incident[2]

Sources:
[1] Unit 42 Cloud Threat Report - Volume 7, 2023, Unit 42 Engagement Experience;
[2] Under the new SEC Rules, the occurrence of a cybersecurity incident must be reported within four business days of when the incident is determined to be material by the reporting company.

Cortex XDR: The central product for a next-gen SOC; it integrates & normalizes all data, drives AI/ML analytics



Cortex XDR: Collect, Detect, Protect

1.
Block attacks

MITRE-leading endpoint security

- Next-generation antivirus
- Device control, disk encryption, host firewall

2.
Accurately Detect

- Behavioral analytics with machine learning
- Customizable detection
- Vulnerability assessment

3.
Swiftly Investigate

- Root cause & timeline analysis
- Threat hunting
- Integrated threat intel

4.
Respond & Adapt

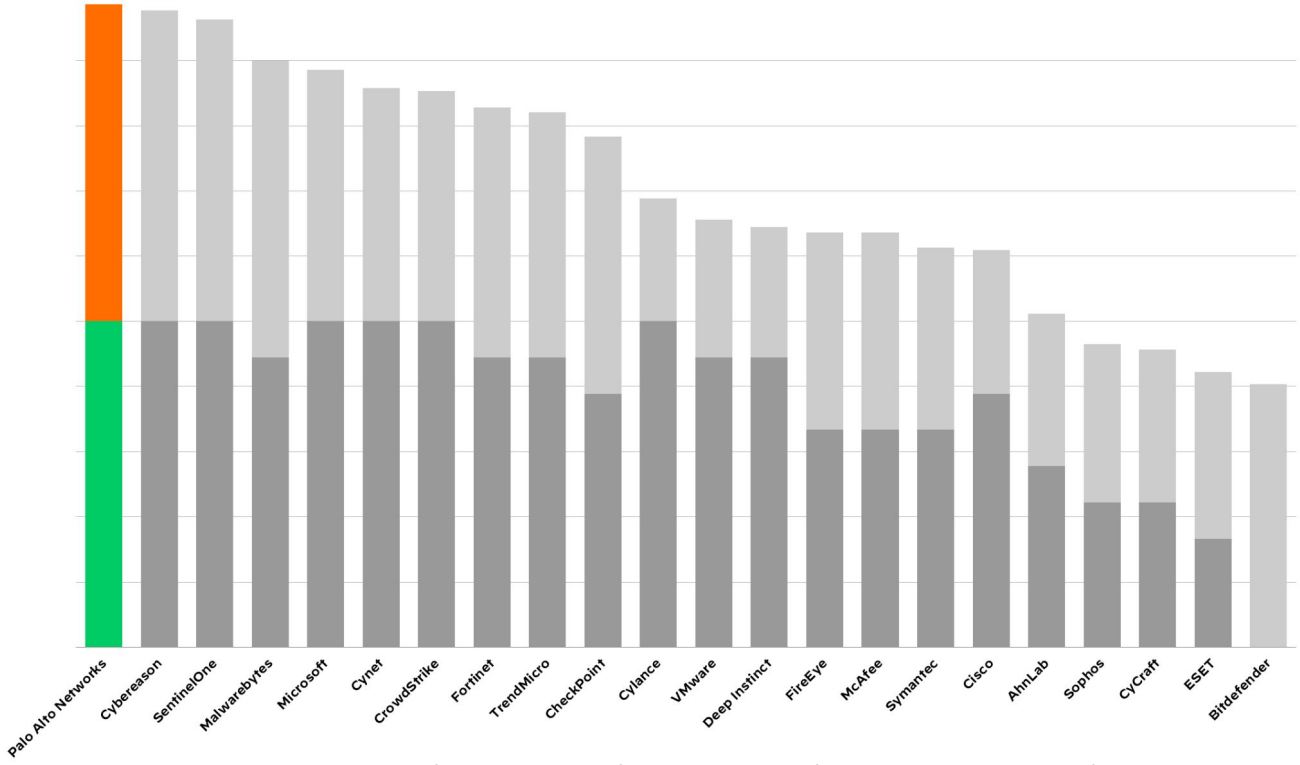
- Integrated enforcement
- Live Terminal
- Search and Destroy
- Automated incident response

CORTEX XDR | paloalto NETWORKS

Unbiased Testing Unbeatable Results

Compare results directly from [MITRE Engenuity's site]

Cortex XDR Triumphed in the 2022 MITRE ATT&CK Evaluations



2022 ATT&CK: Combined Technique Detections and Protections

Technique Detections Protections

- **100% protection,** including Linux and Windows
- **100% detection** of all 19 attack steps
- **107 of 109 technique detections**, highest of any vendor
- **Only 1 config change**

Note that Technique Detections exclude configuration changes. Not all vendors participated in the Protections or the Detections for Linux evaluations.

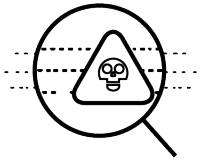
What is Unit 42 MDR?

Built on Cortex XDR

Confidence from technology that has proven 100% Prevention and Detection in MITRE ATT&CK evaluation

Managed by Unit 42

Unit 42 security analysts will continuously monitor your environment and hunt for threats.



Enriched with Context

Unit 42 analysts benefit from an industry-leading repository of threat intelligence to find emerging attacks quickly.

Unit 42 MDR: At-a-Glance

Setup & Onboarding

- Product deployment
- Personalized onboarding and configuration
- XDR administration & management

Continuous Monitoring

- 24x7x365 monitoring of XDR estate
- Comprehensive visibility
  - Endpoint
  - Network (NTA)
  - Cloud
  - Identity
- Alert management
- Continuous tuning
- Event notification

Proactive Hunting & Protection

- Proactive hunting for advanced threats
- Integrated high fidelity threat intelligence
- Actionable threat and impact reports
- Direct access to team
- Managed Threat Hunting

Investigation & Response

- Threat containment
- Incident investigation
- Communication and collaboration
- Remediation & recovery with Cortex XDR

Major Incident Response

- Access to Unit 42 Incident Response for major events

Security Posture Optimization

- Automated health checks
- Vulnerability assessment
- Host inventory