BLUETIDE
COMMUNICATIONS

About Extended Detection & Response (XDR)

XDR consolidates and extends detection and response capabilities across various security layers, encompassing endpoint, cloud, identity, network, and mobile. This empowers security teams with centralized, end-to-end enterprise visibility, robust analytics, and automated response capabilities throughout a broad spectrum of the technology stack.

Unified Analytics

XDR streamlines the analysis of correlated incidents, enabling swift and efficient response and remediation. With AI and machine learning capabilities, it can analyze extensive data points in real time, identifying attacks and malicious behavior much faster than security teams manually correlating incidents and addressing threats.

XDR Use Cases

- Detect Endpoint Device Vulnerabilities
- Hunt Threats Across Domains
- Investigate Security Events
- Perform Endpoint Health Checks
- Predict Future Attacks
- Prioritize and Correlate Alerts

Data Collection & Integration

XDR monitors data in an enterprise's technology environment, spanning endpoint devices, firewalls, cloud infrastructure, and select third-party applications. XDR identifies incidents and threats across the environment and collates related occurrences, optimizing security alerts and allowing security teams to understand a cyberattack more clearly.

Incident Management

XDR allows enterprises to respond automatically or manually to threat incidents. XDR can use preset conditions to quarantine devices and remediate threats by blocking IP addresses or mail server domains. Security analysts can also review incident reports and recommended solutions and act accordingly.

Contact BlueTide Sales at **337-205-6720** or **sales@bluetidecomm.com**

BLUETIDE COMMUNICATIONS

XDR PLATFORM VS. TRADITIONAL AV

DETECTION CAPABILITIES	Utilizes AI and machine learning to unveil sophisticated attacks that do not rely on known malware signatures. It not only focuses on prevention but also detection, helping organizations become resilient against zero-day threats and Advanced Persistent Threats (APT).	Detects known malware based on virus signatures
RESPONSE & REMEDIATION	Automates the response after an incident, enabling quicker remediation and reducing the dwell time of threats.	Primary focus on remediation following threat detection. Infected files are isolated or deleted to prevent further spread.
INTEGRATION	Provides an integrated approach by integrating various security technologies into a single platform. It combines endpoint protection, network security, and security information to present a cohesive view of the security status.	Antivirus solutions safeguard specific systems
AUTOMATION	Provides automated security operations to reduce the IT security team's workload. It also offers proficient threat-hunting capabilities, utilizing artificial intelligence to detect threat patterns and anomalies effectively.	Requires manual intervention for effective threat response
SCALABILITY	By utilizing cloud-native infrastructure, it can easily expand to cover growing numbers of endpoints, adapting to the business’s expansion	As the number of devices rises, conventional antivirus software may prove insufficient.

Contact BlueTide Sales at **337-205-6720** or **sales@bluetidecomm.com**

BLUETIDE
COMMUNICATIONS

XDR PLATFORM VS CROWDSTRIKE

	XDR Platform	CrowdStrike
Protection	☑ **Powered by patented behavioral AI, operational at all times, no internet connection required.**	☒ Human-powered cybersecurity can cause delays and misses, and cloud-dependent protection may not be enough.
Detection	☑ **The most comprehensive, easiest to visualize MITRE coverage.**	☒ Requires extensive tuning with diminishing results, as seen during MITRE Enterprise Evaluations.
Remediation	☑ **Automated remediation with one-click remediation and rollback.**	☒ Manual and script-based mitigation for most alerts types. No rollback support.
Operating Systems Feature Parity	☑ **Rich feature parity across all supported operating systems, including Windows, macOS, and Linux.**	☒ No feature parity, and the Falcon agent's Reduced Functionality Mode can put devices temporarily out of support.
Enterprise Grade Configuration Choices	☑ **Out of the box multi-tenancy, RBAC, enables you to scale and to manage geographically dispersed sites**	☒ CrowdStrike support only offers manual, partial multi-tenant configuration, which can take days.
Automated Deployment	☑ **Singularity Ranger covers your blind spots and automatically deploys new agents in real time, as needed.**	☒ Visibility only for managed devices, creates ongoing risk of exposure.
Remote Management and Forensics	☑ **Manage large deployment with remote script across multiple assets. Full remote native OS tools coverage.**	☒ Manage individual assets using remote commands, no bulk operations.

Contact BlueTide Sales at **337-205-6720** or **sales@bluetidecomm.com**

BLUETIDE
COMMUNICATIONS

XDR PLATFORM VS MICROSOFT

	XDR Platform	Microsoft
Protection	☑ **Powered by patented behavioral AI, operational at all times, no internet connection required.**	☒ Requires extensive tuning, and continuously fails to deliver meaningful results in MITRE ATT&CK evaluations.
Detection	☑ **The most comprehensive, easiest to visualize coverage.**	☒ Requires extensive tuning with diminishing results, as recognized by underwhelming industry evaluations.
Remediation	☑ **Automated remediation. Revert malicious activities with one-click remediation and rollback.**	☒ Offers automatic remediation for a small subset of alerts. No automatic remediation on macOS or Linux.
Ease of Use	☑ **One management console that provides full context to SOC analysts every single day.**	☒ Microsoft's capabilities are separated between different product consoles.
Protection Parity Across OSes	☑ **Award winning protection across Windows, Linux and macOS.**	☒ Good protection on latest versions of Windows, but weak on legacy Windows, Linux and macOS.
Automated Deployment	☑ **Singularity Ranger covers your blind spots and automatically deploys new agents in real time, as needed.**	☒ Requires manual deployments. Users will only receive a list of assets not running the solution.
Licensing	☑ **SentinelOne's licensing model is simple and modular, with no complexity.**	☒ No standardized licensing rates per user or by usage across different products and services. Required add-ons and services for certain offerings

Contact BlueTide Sales at **337-205-6720** or **sales@bluetidecomm.com**

BLUETIDE
COMMUNICATIONS

XDR PLATFORM VS PALO ALTO

	XDR Platform	Palo Alto
Protection	☑ **Powered by advanced behavioral AI, operational at all times, and provides robust security for endpoints, cloud, and identity attack surfaces.**	☒ Cortex XDR platform offers disjointed capabilities, added through acquisitions and requiring individual deployments, creating unnecessary complexity, and performance issues.
Detection	☑ **Comprehensive analytics detection, and coverage easily visualized. Turn queries into automated hunting rules for faster mitigation.**	☒ Generates too many false positives, according to multiple peer review websites.
Remediation	☑ **Automated remediation. Revert malicious activities with one-click remediation and rollback.**	☒ Many remediation capabilities require additional licensing and deployment of Cortex xSOAR.
Automated Deployment	☑ **Singularity Ranger covers your blindspots and automatically deploys new agents in real time, as needed.**	☒ Requires manual deployments based off a long list of assets not running the solution.
Transparent Licensing Model	☑ **Prioritizes offering a simple and modular licensing model with no complexity.**	☒ Offers a licensing model so complex that requires a pricing calculator to understand. Confusing licensing for products.
Disconnected Solutions	☑ **Singularity XDR provides coverage across Endpoint, Identity, and Cloud.**	☒ Disconnected solutions between endpoint and cloud and no identity coverage.

Contact BlueTide Sales at **337-205-6720** or **sales@bluetidecomm.com**

BLUETIDE
COMMUNICATIONS

XDR PLATFORM VS TREND MICRO

	XDR Platform	Trend Micro
Protection	☑ **Enables teams to automatically mitigate cyber threats across Windows, macOS, and Linux.**	☒ Only allows you to quarantine malicious binaries for cyber threat mitigation.
Detection	☑ **Works out-of-the-box, comprehensive coverage with greater visibility in industry evaluations.**	☒ Only offers manual and maintenance-heavy detection and requires several configuration changes, as proven in industry evaluations.
Remediation	☑ **Patented automatic and 1-click remediation & rollback.**	☒ Does not offer rollback support. Customers can only use wipe and load recoveries.
Ease of Use	☑ **Teams can easily manage policies and updates across endpoints and cloud workloads.**	☒ Only allows security teams to run static configuration scans to tune which rules to turn on/off for modules.
Automated Deployment	☑ **Singularity Ranger covers your blindspots and automatically deploys new agents in real time, as needed.**	☒ Requires manual deployments based off a long list of assets not running the solution.

Unified Visibility Control	SecOps, Simplified	DevOps Friendly
SentinelOne's enterprise-grade protection preserves workload immutability, auto-scales protection with demand, and automates remediation with no complex tuning required.	Our agent supports 12 major Linux distributions and operates entirely in user space, ensuring no tainted kernels or kernel panics. Devs can update their OS image at their convenience.	SentinelOne integrates protection, detection, and response across hybrid cloud workloads and user endpoints, utilizing cloud metadata and beyond.

Contact BlueTide Sales at **337-205-6720** or **sales@bluetidecomm.com**