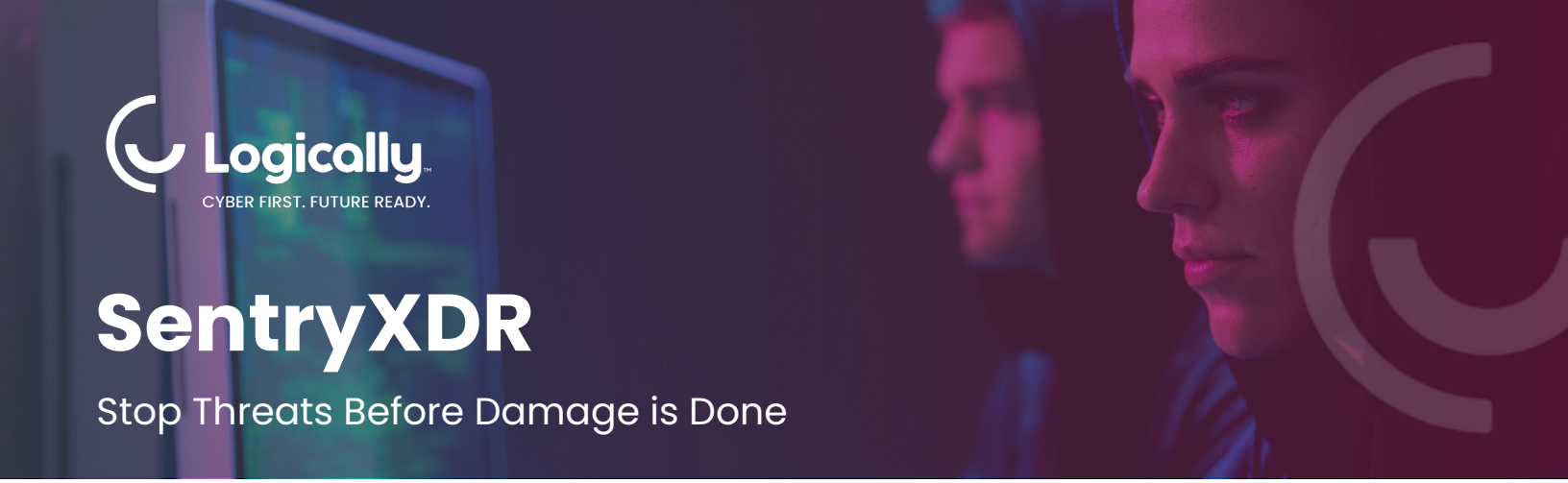


Logically
CYBER FIRST. FUTURE READY.

SentryXDR

Stop Threats Before Damage is Done

Modern cyberthreats move fast, bypassing endpoints and living undetected within your network. For mid-market IT and security teams, the challenge is compounded by alert fatigue, siloed tools, and limited staff capacity.

SentryXDR closes the gap.
With real-time detection, automated remediation, and 24/7 SOC expertise—**backed by AI/ML intelligence and built for hybrid environments**—SentryXDR empowers your team to stop threats before damage is done.

WHAT YOU'LL GAIN

True XDR, Built for the Real World

- **End-to-End Visibility**
  Ingests logs and flows from firewalls, endpoints, Active Directory, cloud, NAC, and more.
- **AI/ML-Driven Threat Detection**
  Correlates user behavior and anomalies to surface unknown threats and lateral movement.
- **Credential Abuse Protection**
  Detects compromised identities and triggers auto-remediation at the Active Directory layer.
- **Advanced Traffic Analysis**
  Stops threats moving east-west or north-south before they escalate.
- **24/7 Human-Led SOC**
  Dedicated analysts monitor, investigate, and respond—day and night.
- **Global Threat Intelligence**
  Informed by 40+ real-time feeds, including NSA sources and international honeypots.
- **Automated Remediation**
  Responds with speed and precision—no manual intervention required.
- **Audit-Ready Reporting**
  Easily meet HIPAA, PCI-DSS, SOX, NIST, and GDPR requirements.

WHAT SETS US APART

77M+
security events analyzed daily

5,000+
applications monitored

1,000+
active threat indicators tracked

Full-stack visibility: edge, endpoint, and cloud

Native MITRE ATT&CK alignment

Deployed in days —not weeks

Powered by the Seceon AI/ML engine

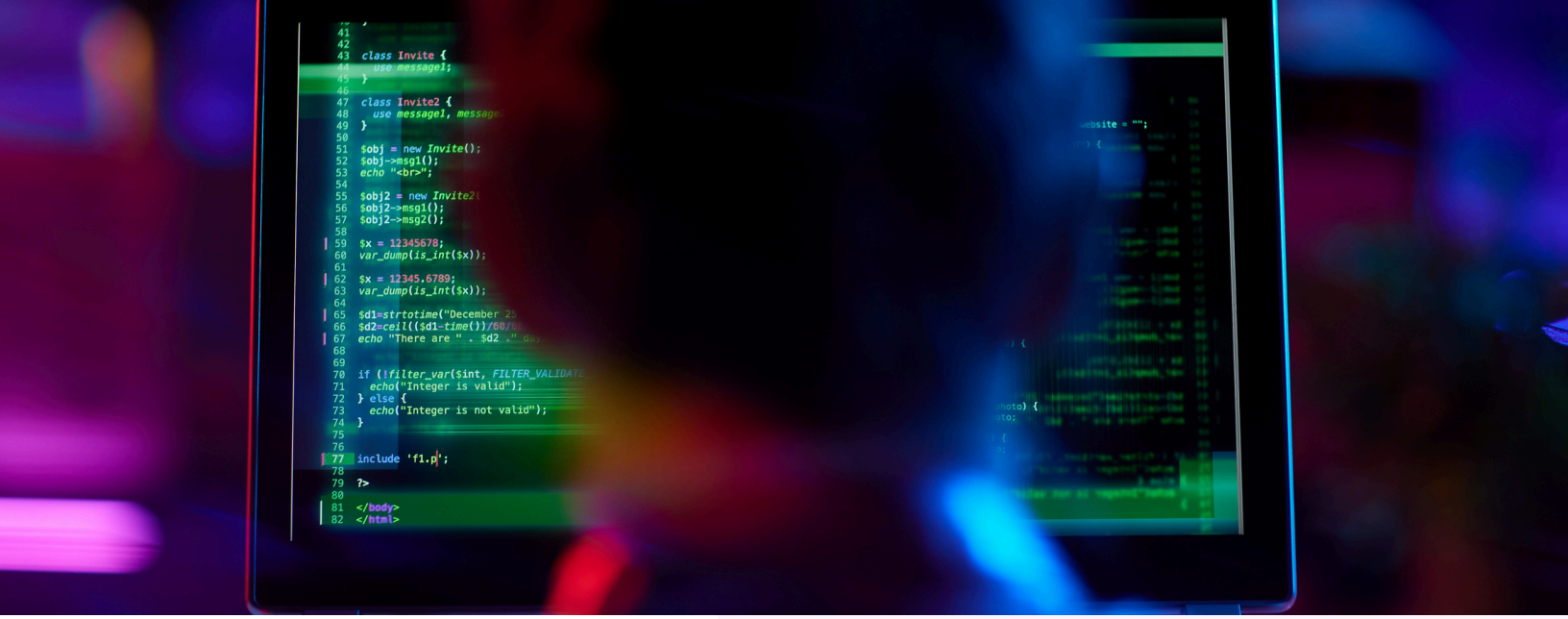
WHO IT'S FOR

Mid-market organizations managing hybrid environments

Regulated industries that need continuous compliance visibility

IT and security leaders seeking to consolidate SIEM, SOAR, MDR, and analytics

SecureBase customers ready to elevate into full-stack XDR coverage



WHAT'S INCLUDED

- Unified log ingestion across firewall, endpoint, AD, O365, NAC, and cloud
- Machine-learning based threat correlation and alerting
- Daily threat intelligence updates from top global sources
- Auto-remediation workflows and hands-on analyst support
- Executive dashboards and compliance-ready reporting
- Privilege monitoring and AD misconfiguration detection

USE CASE SNAPSHOT

Healthcare System Secures Compliance and Slashes Threat Dwell Time

Scenario:
Multi-site healthcare network with 800 endpoints and HIPAA compliance challenges

Change:
Legacy SIEM lacked endpoint visibility, failed to detect lateral movement, and missed the mark in a compliance audit

Solution:
Logically deployed **SentryXDR 360** across cloud, firewall, and AD—all within 5 business days

Outcome:

- 83% reduction in Mean Time to Respond (MTTR)
- 12 critical threats auto-contained before data exfiltration
- Passed OCR audit with remarks: "Exceeds compliance standards"

Logically. Cyber-First. Future Ready

www.logically.com | hello@logically.com