GUARDIAN
MANAGED SECURITY. REIMAGINED.

PrismX™: Redefining Perimeter Defense

Move beyond MDR/XDR with PrismX - proactive cybersecurity built for today's threat landscape.

Organizations need full visibility into their entire environment, real-time intelligence on emerging threats, and the ability to stop attacks before they start. Traditional tools can't deliver that. It takes a solution built for how today's attacks actually happen.

"Only 17% of organizations can clearly identify and inventory a majority (95% or more) of their assets."

— Gartner, 2024

Modern threats evolve faster than reactive defenses can respond. The biggest threats to your organization aren't the ones MDR/XDR sees--they're the ones it doesn't even look for.

What MDR/XDR Misses

- **Limited visibility**
  Protects managed endpoints but ignores thousands of external attack points.
- **Incomplete Vulnerability Assessment**
  Scans only protected endpoints, leaving gaps across the infrastructure.
- **Restricted data collection**
  If it's not installed or integrated, it's invisible.
- **Reactive approach**
  SOC reacts after attackers are inside.

How PrismX Responds

- **Total Asset Coverage**
  Includes cloud, IoT, shadow IT, and unmanaged infrastructure.
- **Continuous Vulnerability Assessment**
  Real-time detection and automation verification of remediations.
- **Comprehensive Data Ingestion**
  Millions of signals collected across your full digital environment.
- **Proactive Threat Hunting**
  Identifies threats before they breach.

What is PrismX™?

PrismX is a full-spectrum cybersecurity platform that combines zero-trust enforcement with proactive threat intelligence. It continuously protects beyond just your managed endpoints to include your entire digital footprint by integrating always-on vulnerability scanning, real-time dark web intelligence, and hunter-led detection across cloud, IoT and shadow assets.

PrismX™ by Guardian--visibility, enforcement, and threat hunting all in one ecosytem that **evolves with your attack surface.**

Why Organizations Choose PrismX

Zero-Trust Enforcement Across All Assets - Eliminate implicit trust and contain threats before they spread.

Complete Visibility - 75% more comprehensive asset inventory than traditional tools.

Proactive, Not Reactive - AttackSOC finds threats in the reconnaissance phase, not after they strike.

Continuous Coverage - Always-on vulnerability monitoring, asset discovery, and threat intel.

Operational Efficiency - Realize a 65% reduction in team workload through automation.

Proven Business Impact - 40% reduction in incident-related costs and faster time to remediation.

How PrismX Works

- **Discover and Analyze -** Map your complete environment and uncover vulnerabilities.
- **Protect and Hunt -** Enforce zero-trust access and proactively detect threats in the recon phase.
- **Respond and Learn -** Automate response and adapt with real-time intelligence.

Results That Matter

94% faster remediation
99.7% access attempts blocked
40% lower incident costs
65% workload reduction

The AttackSOC™

Traditional SOCs, by nature of their functionality, are passive. They wait for alerts. They monitor dashboards. They investigate incidents after damage is done. PrismX's AttackSOC is different. Our analysts think like adversaries.

- **Hunter-first mindset -** Actively searches for attacker behavior. No waiting for alerts.
- **Full-environment analysis -** Analyzes signals from cloud, shadow IT, IoT, and umanaged assets, not just endpoints.
- **Adversary-mindset -** We think like they do, and find what they're targeting before they strike.
- **Early detection -** Identifies attack patterns in reconnaissance phase, weeks before traditional SOCs would detect anything.

It's time to close the loop, from asset discovery to adversary disruption.
Get started with Guardian PrismX today.

To learn more, visit www.guardiancssp.com or contact us:
Steve Heinrich, Regional Sales Director
steve.heinrich@guardiancssp.com | 512-426-7580

GUARDIAN
MANAGED SECURITY. REIMAGINED.

www.guardiancssp.com