

# CDC Reveal360

Continuous clarity for security posture, service performance, and business value

Enterprise security teams do not lack data. They lack a clear, connected way to understand what that data means for risk, performance, and decision-making.

Threat intelligence sits in one tool. Vulnerability data lives in another. Detection rules are managed elsewhere. Asset inventory may be incomplete or outdated. Governance, risk, and compliance (GRC) reporting often happens in separate workflows. When leaders ask, “Are we protected against the threats most relevant to us?” or “What value is our managed security service delivering?” the answer often requires hours of manual correlation across disconnected systems.

CDC Reveal360 changes that.

CDC Reveal360 is CyberProof’s centralized visibility hub for cybersecurity and IT. It unifies security, exposure, defense, operational, and compliance data into customizable, role-based workspaces that help organizations understand not only their security program health, but also the output and value of their managed services. As CyberProof positions it, CDC Reveal360 is not where the work happens. It is where all work becomes visible.



## The challenge: fragmented visibility creates decision friction

Most enterprise environments suffer from product sprawl and dashboard overload. Different stakeholders see different slices of reality, but few see the full picture. That creates operational friction, slows prioritization, and makes it difficult to communicate security posture in business terms.

**For CISOs and security leaders,** that means board reporting becomes a manual exercise built from snapshots rather than continuous reality.

**For security operations managers,** performance metrics and threat exposure are often visible, but not together.

**For service delivery teams,** value is delivered continuously, but visibility into that work is often limited to periodic reviews.

**For compliance leaders,** checkbox reporting does not provide a live connection to the controls, services, and posture data that matter most.

The result is a gap between what is happening and what stakeholders can actually see.

# What CDC Reveal360 delivers

CDC Reveal360 provides a flexible and customizable widget-based experience layer that allows each persona to tailor views to their needs while staying connected to the same underlying operational reality. It serves as a data hub for cybersecurity, IT, GRC, and business insights, bringing together information from threat intelligence, defense telemetry, detections, vulnerabilities, assets, identities, compliance data, and security operations center (SOC) performance.

Key capabilities include:



## Role-configured workspaces

Customizable views tailored to CISOs, threat analysts, security operations managers, service delivery managers, customer security leads, and risk and compliance stakeholders.



## Cross-platform data unification

A connected view across endpoint, SIEM, vulnerability management, identity, GRC, and threat intelligence sources so teams can move from fragmented signals to a coherent narrative.



## Defense coverage analysis

Visibility into active threat groups, campaigns, techniques, detections, controls, and gaps to help organizations understand defense readiness and prioritize what matters most.



## Inside-out transparency

A live view of how cloud, cybersecurity infrastructure, and services are operating, helping managed service clients see incidents handled, SLAs met, posture trends, service metrics, and ongoing outcomes without relying solely on quarterly reviews.



## Risk visualization over time

Customizable views of overall risk, threat exposure, defense posture, and trends that help teams measure improvement, communicate outcomes, and support more confident decisions.

## Why it matters by role

### For CISOs and security leaders

CDC Reveal360 helps turn fragmented technical data into a continuous, defensible security posture narrative with board-ready reporting and clearer investment priorities.

### For security operations managers

CDC Reveal360 connects team performance, service-level agreement status, and workload distribution to actual threat exposure and defense posture, helping teams better align effort to risk.

### For threat management analysts

CDC Reveal360 provides a shared analytical surface for connecting threat intelligence, MITRE ATT&CK coverage, campaigns, and detection gaps without losing context.

### For service delivery managers and client security leads

CDC Reveal360 creates continuous visibility into service health, operational outcomes, and posture improvements, making the managed service relationship more transparent, measurable, and collaborative.

### For compliance and risk leaders

CDC Reveal360 supports centralized compliance monitoring that goes beyond simple documentation by tying posture and reporting to live controls and service data.

# Business outcomes

CDC Reveal360 helps organizations:



**Unify** fragmented security and infrastructure data into role-specific insights



**Understand** security posture, operational performance, and managed service value in one shared experience



**Make** faster strategic and operational decisions with context intact



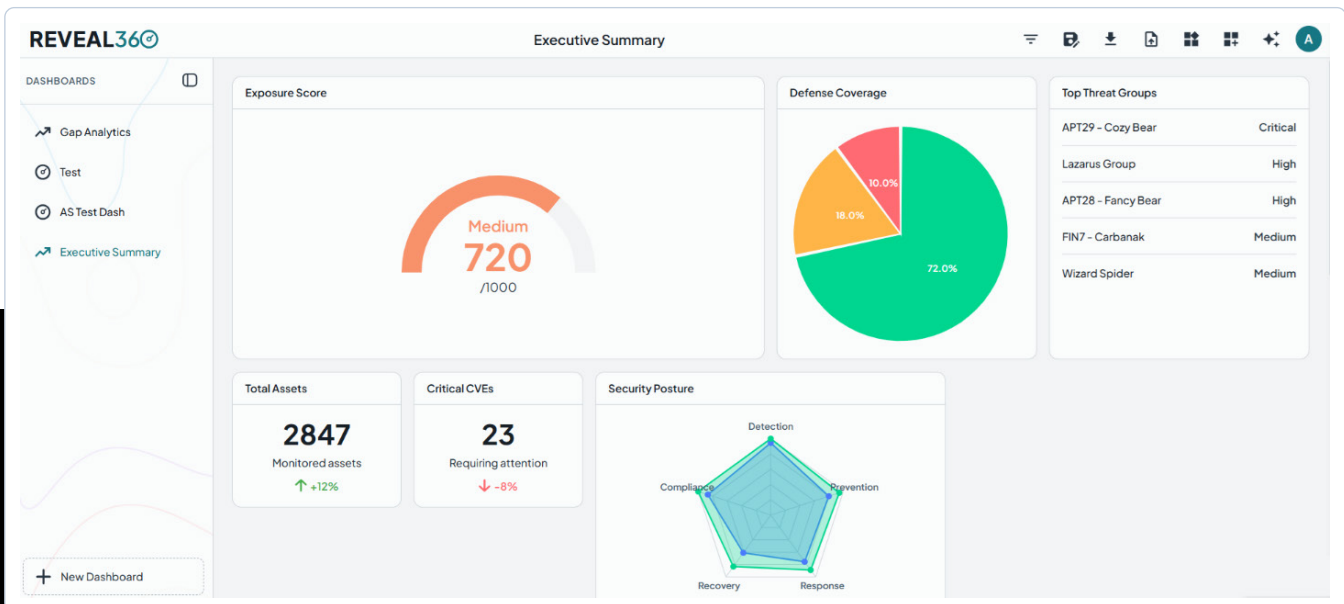
**Improve** communication with executives, boards, regulators, and internal stakeholders



**Increase** transparency across co-managed security operations



**Support** measurable business outcomes, security posture improvement, and stronger risk management.



See CDC Reveal360 in action and discover how your organization can connect posture, performance, and business value in one place:

[Request a demo →](#)

[Take a tour →](#)

Speak with CyberProof about a [threat exposure assessment](#) to identify gaps, prioritize what matters most, and define the right next step for your security program.

CDC Reveal360 is available as a standalone platform and is also included as part of CyberProof managed service offerings.