

Reference architecture and flow diagram for

CyberProof's Defense Management Solution



The Importance of Defense Management in Cybersecurity

In today's dynamic threat landscape, defense management is essential for maintaining cyber resilience. CyberProof's Defense Management services offer a proactive, threat-led approach that aligns security operations with real-time exposure insights. By integrating MXDR, tailored threat intelligence, advanced threat hunting, and detection engineering (also called Use Case Management) driven by Continuous Threat Exposure Management (CTEM), organizations can reduce alert fatigue and focus on what truly matters.

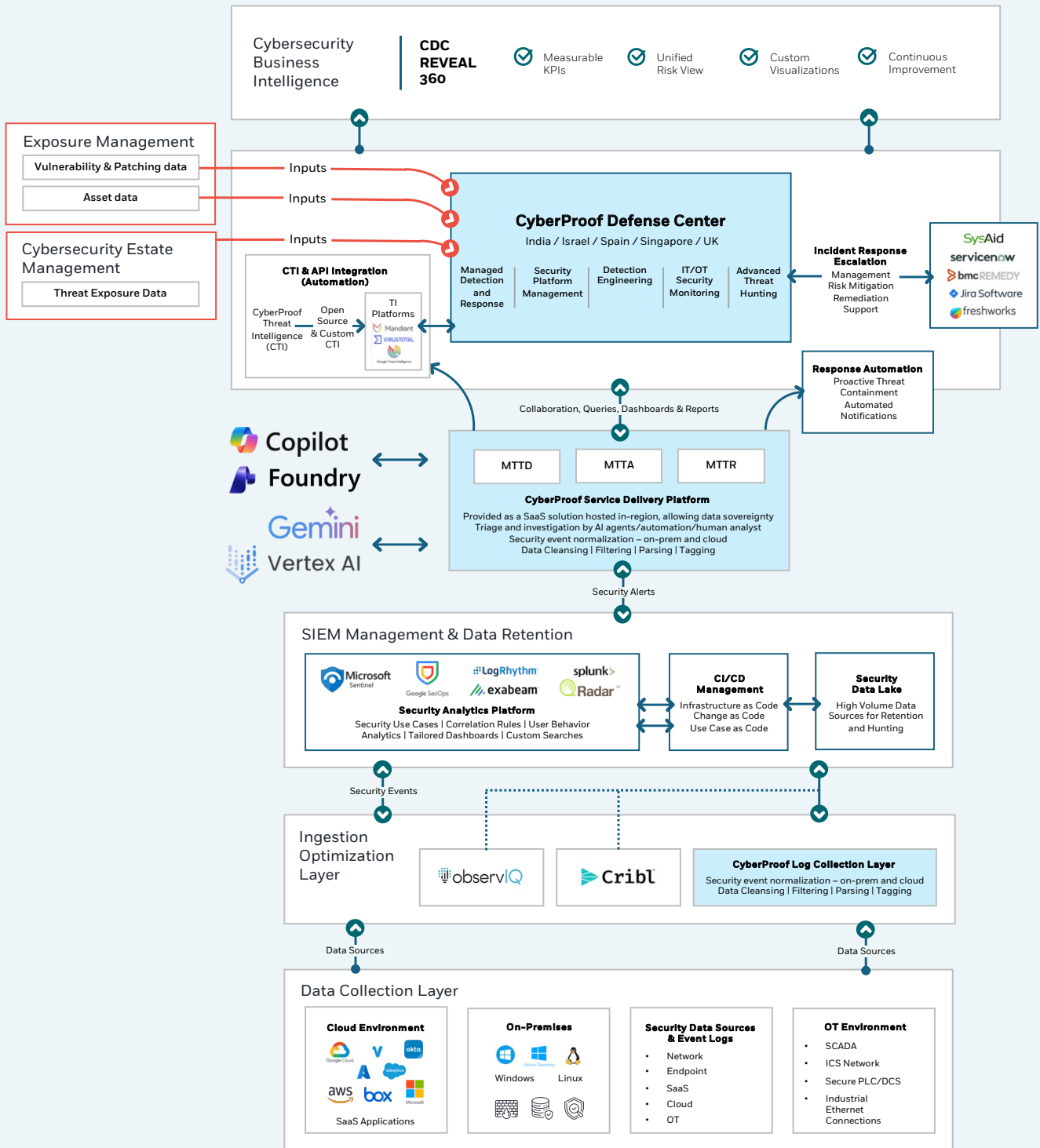
This co-managed model empowers security teams to adapt quickly to evolving threats, leveraging automation expert-driven use case management, and agentic AI to enhance detection capabilities and reduce time to detect and remediate threats. The platform's integration with CTEM ensures that defenses are not only reactive but strategically aligned with business risk.

Ultimately, defense management transforms cybersecurity from a reactive necessity into a strategic advantage –

enabling smarter decisions, faster response times, and measurable improvements in operational efficiency. It's not just about stopping attacks; it's about staying ahead of them.



Reference Architecture for CyberProof's Defense Management



Reference architecture for CyberProof's Cybersecurity Defense Management services

The Defense Management reference architecture diagram presents a comprehensive view of CyberProof's integrated defense management ecosystem. At the top, the CDC Reveal360 dashboard serves as the central visibility layer, SOC activity such as incidents, alerts, threat levels, SLA trends, and detection and response metrics. The dashboard also includes data such as current threat levels and other insights as required, ensuring a holistic view of the operational health and responsiveness of the security environment.

The core of the architecture is CyberProof's Defense Management services, which include MDR/MXDR, detection engineering, incident response, security platform management, advanced threat hunting, and IT/OT security monitoring (where relevant). These services are interconnected, enabling a dynamic and threat-led approach to cybersecurity. They work in concert to detect, prioritize, and respond to threats based on business risk and exposure.

The diagram also shows how Defense Management is strengthened by Cybersecurity Estate Management and Exposure Management, which provide asset visibility, contextual risk insights, and telemetry to improve prioritization, detection, and response.

On the left are integrations to AI infrastructure, including Microsoft Copilot, Google Gemini, Microsoft Foundry, Google Vertex, and other AI models, to enhance decision-making and operational efficiency. On the right, CyberProof Incident Response Management connects to platforms like ServiceNow for ticketing, while CTI/IT feeds from sources such as Anomali, VirusTotal, and IBM X-Force Exchange provide external threat intelligence inputs.

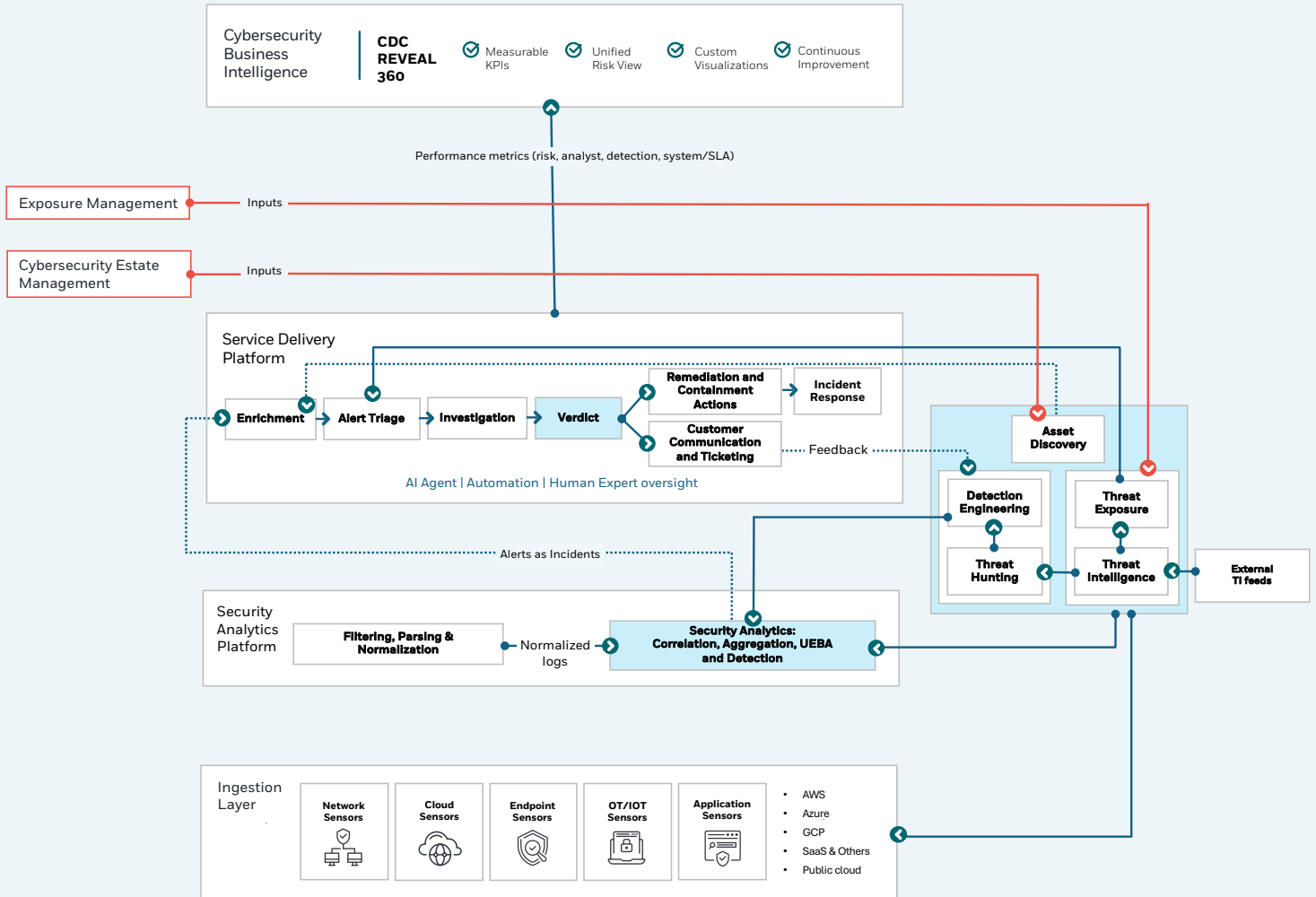
A key part of the architecture is the Ingestion Optimization Layer, which reduces data volume and cost by cleansing, filtering, parsing, and tagging events before they enter the analytics pipeline. All data is stored in a central location, but by forwarding only what's needed, this layer keeps operations lean while still ensuring strong visibility and compliance.

At the base is the Data Collection Layer, which aggregates logs and telemetry from diverse on-prem, cloud, OT/IoT, and application sources.

Overall, the architecture illustrates a highly orchestrated and intelligence-driven defense strategy that enables proactive threat management and operational transparency.



Flow Diagram for CyberProof's Defense Management



Flow diagram of CyberProof's Cybersecurity Defense Management solution



The diagram presents a layered architecture that begins with the Ingestion Layer: logs, alerts, and configuration data collected from network, cloud, endpoint, OT/IoT, and application environments – on-premises and in the cloud.

The flow also shows how Defense Management consumes and enriches inputs from Cybersecurity Estate Management and Exposure Management, using asset context and prioritized risk to improve detection, response, and continuous security improvement.

From there, data moves toward the security analytics platform (typically a SIEM). In practice, a data engineering step (for example, Cribl) often sits between ingestion and analytics to handle filtering and volume reduction, while parsing and normalization may occur in the SIEM and/or the data engineering layer.

Threat intelligence enriches and correlates events, and it can also inform upstream/downstream security controls where automation supports that integration. The resulting alerts flow into the service delivery platform for case management, automated enrichment, triage, investigation, and analyst verdicts, followed by playbook-driven containment and remediation actions.

When remediation requires customer ownership or approvals, the workflow transitions to customer communication and ticketing. Finally, outcomes close the loop: tickets and investigations generate feedback into SOC, detection engineering and threat hunting, while threat hunting is further guided by threat intelligence to continuously strengthen coverage and response.

At the top of the diagram, CDC Reveal360 provides holistic risk view and visibility into metrics and key SOC functions such as security event monitoring, threat detection, threat hunting, and incident response.

The diagram illustrates a tightly integrated, threat-led defense model where remediation outcomes feed back into Reveal360 for continuous improvement of detections, playbooks, and response workflows.



Why Defense Management Matters for Your Organization

In an era of increasingly sophisticated cyber threats, defense management is no longer optional, it's foundational to business resilience.

Proactive threat response:

Defense management enables your organization to detect and respond to threats before they escalate, reducing risk exposure.

Operational efficiency

By integrating automation, threat intelligence, and incident response workflows, it streamlines security operations and minimizes manual effort.

Business-aligned security

It prioritizes threats based on business impact, ensuring that resources are focused where they matter most.

Visibility and control

Centralized dashboards and analytics provide real-time insights into incidents, alerts, and performance metrics.

Scalable and adaptive

Defense management evolves with your organization, adapting to new technologies, environments, and threat vectors.

With defense management in place, your security team can shift from reactive firefighting to strategic risk reduction, empowering smarter decisions and stronger protection.

Taking the Next Step in Defense Management

Defense management is more than a security operations upgrade—it's a strategic capability that aligns threat detection, response, and exposure management with business risk. For organizations ready to strengthen their cybersecurity posture, the next step is translating these concepts into action. We recommend:



Read more about it –

The [Defense Management webpage](#) offers valuable insights into CyberProof's co-managed, platform-driven approach.



Additional reference architecture diagrams –

- [Reference architecture for Cybersecurity Estate Management](#)
- [Reference architecture for Exposure Management](#)



Request a tailored threat exposure assessment –

Begin with a focused evaluation of your current threat landscape. Identify where visibility gaps exist and how threat prioritization can be improved.

[Get an assessment of your defense readiness.](#)



Engage CyberProof experts –

Schedule a session with our team to walk through your environment, review this flow architecture in detail, and identify where Defense Management can provide immediate value. Start with a focused pilot or use case, such as cloud detection, endpoint response, or threat hunting, and expand gradually as your defense maturity grows. [Book a session with CyberProof.](#)



Connect to the bigger picture –

Link Defense Management outcomes to your broader exposure management and threat-led defense strategy. Visibility and detection are just the beginning, the ultimate goal is proactive, risk-aligned defense. [Schedule a strategic discussion.](#)

CyberProof's Defense Management services help you move from reactive security to proactive resilience.

[Contact CyberProof to explore how to get started.](#)

CyberProof[®] | Better Security,
A UST Company | Together.