HORIZON IoT

SECURING CONNECTED OPERATIONS THROUGH CYBER RESILIENCE

Cybersecurity & Operational Resilience Framework

IDENTITY | AI ASSISTED DETECTION | ZERO TRUST | DATA PROTECTION | CLOUD | IoT & OT | RESILIENCE



Solution Overview and Implementation Framework | November 2026

Protect identities, data, connected systems, and essential operations

Cybersecurity becomes practical when safeguards align with the customer environment, operational priorities, existing architecture, responsible data use, and measurable outcomes. Horizon IoT helps public sector and enterprise organizations evaluate, source, integrate, deploy, and support validated cybersecurity capabilities through a partner enabled delivery model.

Capabilities and Secure Architecture

Capabilities can be configured individually or combined into a phased cybersecurity program. A layered architecture connects identities, endpoints, applications, networks, cloud or hosted environments, connected devices, operational systems, monitoring, analytics, and lifecycle support.

Identity and access security

Authentication, authorization, access governance, least privilege, privileged access, and Zero Trust controls.

AI assisted anomaly detection

Abnormal user, device, network, application, and system behavior across supported environments.

Monitoring and resilience

Visibility, alerting, escalation, continuity, backup, recovery, and coordinated response workflows.

Network, endpoint, and application protection

Secure access, segmentation, application control, traffic protection, and continuous monitoring.

Cloud and hosted environment security

Identity, connectivity, application protection, data safeguards, monitoring, backup, and resilience.

Data protection and technical privacy safeguards

Encryption, access controls, secure handling, governance, monitoring, and recovery capabilities.

IoT and operational environment security

Device visibility, secure connectivity, segmentation, access control, and abnormal behavior monitoring.

Technical security assessments

Posture reviews, control gap identification, architecture review, vulnerability findings, and remediation recommendations.

Secure and Interoperable Architecture

Architecture layer	Illustrative components
Customer and operational experience	Approved workflows, dashboards, alerts, investigations, reporting, continuity, and support.
Applications and security analytics	Identity, endpoint, network, application, cloud, device, anomaly, and operational security capabilities.
Data and integration	Telemetry, APIs, logs, asset context, approved data exchange, retention, backup, and reporting.
Connectivity and protection	Wired, wireless, cellular, edge, segmentation, encryption, secure access, and monitored pathways.
Devices and infrastructure	Endpoints, gateways, servers, cloud services, IoT devices, operational assets, and security technologies.
Operations and support	Monitoring, escalation, maintenance, remediation, recovery, documentation, and lifecycle coordination.

AI Assisted Cybersecurity Intelligence

AI assisted analytics can help identify unusual patterns, surface anomalies, and prioritize conditions that require investigation. Human oversight, approved procedures, and accountable decision making remain central to the security process.



Identity behavior insights

Identify unusual access patterns, privilege use, authentication activity, or account behavior for review.

IoT and operational anomalies

Identify unusual device, gateway, sensor, network, or operational activity where supported telemetry is available.

Endpoint and application anomalies

Surface unexpected process, application, configuration, or workload behavior across supported systems.

Cloud and hosted environment signals

Analyze supported identity, access, application, connectivity, data, backup, and workload events.

Network and communication patterns

Review unexpected connections, traffic flows, segmentation events, or communication changes.

Operational prioritization

Organize trusted observations, exceptions, vulnerabilities, trends, and risks for accountable investigation.

Responsible AI use

Each use case should define purpose, approved data, data quality, human review, acceptable use, privacy, documentation, monitoring, escalation, and the accountable decision supported by the insight.

Cybersecurity and Operational Resilience

Connected organizations depend on trusted identities, secure connectivity, resilient operations, and accountable technology governance. Controls should extend across users, devices, networks, applications, APIs, cloud or hosted services, data platforms, administrators, vendors, and supported operational systems.



Identity and access

Strong authentication, role based access, least privilege, privileged administration, and separation of duties.

Data and application security

Encryption, governed interfaces, approved exchange, logging, retention, backup, and recovery requirements.

Device and endpoint security

Secure configuration, inventory, software lifecycle, approved management access, and health visibility.

Monitoring and escalation

Security logging, alert ownership, investigation, vulnerability coordination, and defined communications.

Network protection

Segmentation, encrypted communications, secure remote access, private connectivity options, and monitored pathways.

Continuity and recovery

Fallback workflows, recovery priorities, remote diagnostics, lifecycle planning, and tested support handoffs.

Flexible Engagement Choices

Assessment and advisory

Technical posture reviews, architecture review, control gaps, vulnerability findings, and remediation priorities.

Professional resources

Qualified consultants and contractors aligned with customer requirements and resource availability.

Technology integration

Validated security platforms connected with customer systems, identity, networks, applications, data, and operations.

Phased or ongoing support

Pilot, project, managed, hosted, on premises, or hybrid approaches selected according to validated scope.

Featured Cybersecurity Use Cases

Horizon IoT coordinates architecture, technology sourcing, integration, deployment, and support around each approved use case without centering individual technology providers.

Identity, access, and Zero Trust

User, administrator, device, service, and supported machine identity controls with least privilege and continuous verification.

Cloud and hosted environment security

Identity, connectivity, application protection, data safeguards, backup, monitoring, and resilience.

AI assisted anomaly detection

Behavioral monitoring across supported identity, endpoint, application, network, cloud, device, and operational data.

IoT and operational security support

Connected device visibility, secure connectivity, segmentation, access control, and abnormal behavior monitoring.

Network and endpoint protection

Segmentation, secure access, application control, traffic protection, endpoint safeguards, and continuous monitoring.

Vulnerability assessment and testing

Qualified partner delivered vulnerability assessment and penetration testing based on authorized scope.

Customer Environments

Government and civic services

Secure access, applications, data, hosted environments, monitoring, continuity, and service delivery.

Healthcare and research

Identity, endpoint, connected device, application, data, and operational safeguards aligned with customer requirements.

Transportation, ports, and logistics

Connected fleet, asset, facility, network, and operational security with anomaly awareness and segmentation.

Education and campuses

Identity, endpoint, network, cloud, application, building, and connected campus security.

Utilities and infrastructure

Device visibility, secure integration, access controls, monitoring, segmentation, and continuity support.

Commercial and industrial operations

Distributed facilities, devices, applications, networks, data, and supported industrial environments.

Governance, Scope, and Customer Trust

Cybersecurity solutions require clear purpose, approved scope, privacy, responsible AI use, technology governance, procurement transparency, lifecycle ownership, performance measures, documentation, and accountable procedures. Capabilities are validated and scoped for each engagement.

Implementation and Horizon IoT Delivery Model

Phase	Core activities	Outputs
1. Discover	Environment, priorities, stakeholders, constraints, dependencies, and desired outcomes.	Discovery summary and target scope.
2. Assess	Architecture, controls, identities, assets, risks, telemetry, and capability fit.	Findings and prioritized recommendations.
3. Design	Solution architecture, technologies, roles, safeguards, deliverables, and acceptance criteria.	Solution design and responsibility matrix.
4. Pilot	Configuration, integration, monitoring, workflows, testing, documentation, and validation.	Pilot findings and go forward decision.
5. Deploy	Phased implementation, change management, testing, training, and operational handoff.	Operational deployment and support package.
6. Improve	Measurement, remediation, lifecycle review, control tuning, and expansion planning.	Performance actions and security roadmap.

Horizon IoT as the Accountable Solution Lead

Horizon IoT leads customer discovery, architecture, authorized technology sourcing, systems integration, pilots, deployment, adoption, support, lifecycle coordination, and ecosystem management. Horizon IoT serves as the prime contractor and central point of accountability.

Partner Enabled Delivery with Clear Boundaries

Delivery can draw on team based experience and qualified consultants, contractors, technology providers, distributors, connectivity resources, cybersecurity specialists, and field service organizations according to each engagement. Partner names and proprietary delivery details are not required in public facing materials, while customer proposals and statements of work should clearly identify the approved scope, roles, methods, platforms, and deliverables.

Define a Practical Cybersecurity Pilot

Begin with a specific environment, service, application, device group, identity population, network segment, or operational workflow. The pilot should validate visibility, control effectiveness, workflow fit, anomaly detection, integration, usability, security, continuity, support responsibilities, and measurable value.

SCOPE	INTEGRATION	SAFEGUARDS	MEASURES
Environment, assets, identities, users	Systems, data, telemetry, workflows	Access, privacy, segmentation, recovery	Visibility, risk reduction, response, value

Practical pilots create evidence for responsible cybersecurity expansion.

Validated Public Capability Scope

Included in this framework

Identity and access security; AI assisted anomaly detection; monitoring and resilience; network, endpoint, and application protection; supported cloud and hosted environment security; data protection and technical privacy safeguards; IoT and operational environment security support; technical assessments; partner delivered vulnerability assessment and penetration testing; and cybersecurity professional resources.

Not represented as broad standalone coverage

Comprehensive policy development, digital forensics, incident consulting, broad compliance auditing, and enterprise cybersecurity governance are not presented as general capabilities unless separately validated and explicitly scoped for a customer engagement.

Customer specific confirmation

Specific technologies, platforms, certifications, staffing, service levels, methods, regulatory mappings, and deliverables are confirmed during discovery, proposal development, and contracting.