

Security & Managed Services

End-to-End Cybersecurity & Managed Support

End-to-End Cybersecurity and 24/7 Managed Support to Protect
and Sustain Your Business Operations



Threat Protection

Identity & Access

Managed Operations

Incident Response

Compliance

Smarter Solutions. Stronger Communities.

The Security Imperative

The threat landscape has never been more complex — organizations need an integrated, always-on security posture, not point solutions.



Shield Breach

Rapidly evolving attacks
across cloud, on-prem, and
hybrid



24/7 Coverage Gap

Internal teams outpaced
by speed and
sophistication of threats



Compliance Risk

Single breach triggers
disruption, regulatory exposure,
and lost trust

- Modern enterprises face a rapidly evolving threat landscape spanning cloud, on-premises, and hybrid environments
- Internal IT teams are often under-resourced and outpaced by the speed and sophistication of modern attacks
- A single unmitigated breach can result in operational disruption, regulatory exposure, and loss of stakeholder trust
- The answer is a governed, Microsoft-native security program backed by expert managed operations

What We Deliver



Neurocraft's Security & Managed Services practice provides comprehensive, Microsoft-aligned protection across every layer of your digital environment.



End-to-End Cybersecurity

Threat protection, risk management, and incident response built on Microsoft Defender, Sentinel, and Azure Security Center



Identity & Access Management

Governing who can access what, with least-privilege enforcement across all identities and systems



Data Protection

Safeguarding sensitive data at rest, in transit, and in use — with classification, encryption, and DLP controls



Threat Intelligence

Continuous monitoring and actionable insights from real-time signals across Microsoft's global threat network



24/7 Managed Support

Always-on operations so your business never operates unprotected — analyst-backed monitoring around the clock

Microsoft Security Stack



Every Neurocraft security engagement is built on Microsoft's integrated security platform — proven tools, unified visibility, and enterprise-grade controls.

POSTURE MANAGEMENT

Azure Security Center

Unified security posture management and threat protection for hybrid workloads

THREAT PROTECTION

Microsoft Defender

Advanced threat protection across endpoints, identities, cloud apps, and data

SIEM / SOAR

Microsoft Sentinel

Cloud-native intelligent threat detection, investigation, and automated response

IDENTITY & ACCESS

Microsoft Entra ID

Identity governance, MFA, conditional access, RBAC, and privileged identity management

COMPLIANCE AUTOMATION

Azure Policy & Blueprints

Automated compliance enforcement and standards governance at scale

DATA GOVERNANCE

Microsoft Purview

Data governance, classification, and compliance management across your estate

Identity & Access Management



Identity is the new perimeter — securing who accesses your systems is the single most impactful control an organization can deploy.

- Microsoft Entra ID configuration — users, administrators, applications, and service identities
- Multi-factor authentication (MFA) enforcement across all access points
- Role-based access control (RBAC) and least-privilege policy design
- Conditional access policies based on user risk, device compliance, and location
- Privileged access discipline — separation of duties and admin account protection
- User lifecycle management — provisioning, de-provisioning, and access reviews



Verify

Authenticate every identity — MFA, risk-based sign-in, and device compliance checks



Authorize

Grant least-privilege access — RBAC roles, conditional policies, and Entra ID governance



Monitor

Continuously track sign-in activity, anomalies, and privileged identity usage in real time



Review

Periodic access reviews, lifecycle audits, and right-sizing of entitlements over time

Threat Protection & Security Operations

Neurocraft delivers continuous threat visibility and rapid response capability — so threats are detected and contained before they become incidents.



Detect

- Security posture management

Continuous assessment of your security baseline against best practices

- Vulnerability detection

Identifying gaps in cloud and on-premises environments before attackers do

- Microsoft Sentinel SIEM

Centralized log collection, correlation, and intelligent alerting

- Threat intelligence integration

Enriched signals from Microsoft's global threat network



Respond

- Incident response

Defined playbooks, escalation paths, and remediation workflows

- Security Operations Center (SOC) support

Analyst-backed monitoring for critical environments

- Escalation & containment

Rapid triage and isolation to limit the blast radius of any incident

- Post-incident review

Root cause analysis and remediation tracking to prevent recurrence

Data Protection & Compliance



Protecting sensitive data and meeting compliance requirements are not afterthoughts — they are built into every layer of Neurocraft's security framework.

- **Data classification**
Identify and label sensitive data using Microsoft Purview
- **Encryption at rest and in transit**
Enforced across cloud storage, databases, and communication channels
- **Data loss prevention (DLP)**
Policies that prevent unauthorized sharing or exfiltration
- **Compliance management**
Support for NIST, ISO 27001, HIPAA, and FedRAMP-aligned frameworks
- **Audit logging and evidence capture**
Administrative activity tracking and retention for compliance reporting
- **Change tracking and policy enforcement**
Automated guardrails so standards are maintained continuously



NIST
Cybersecurity
Framework



ISO 27001
Information Security



HIPAA
Health Data Privacy



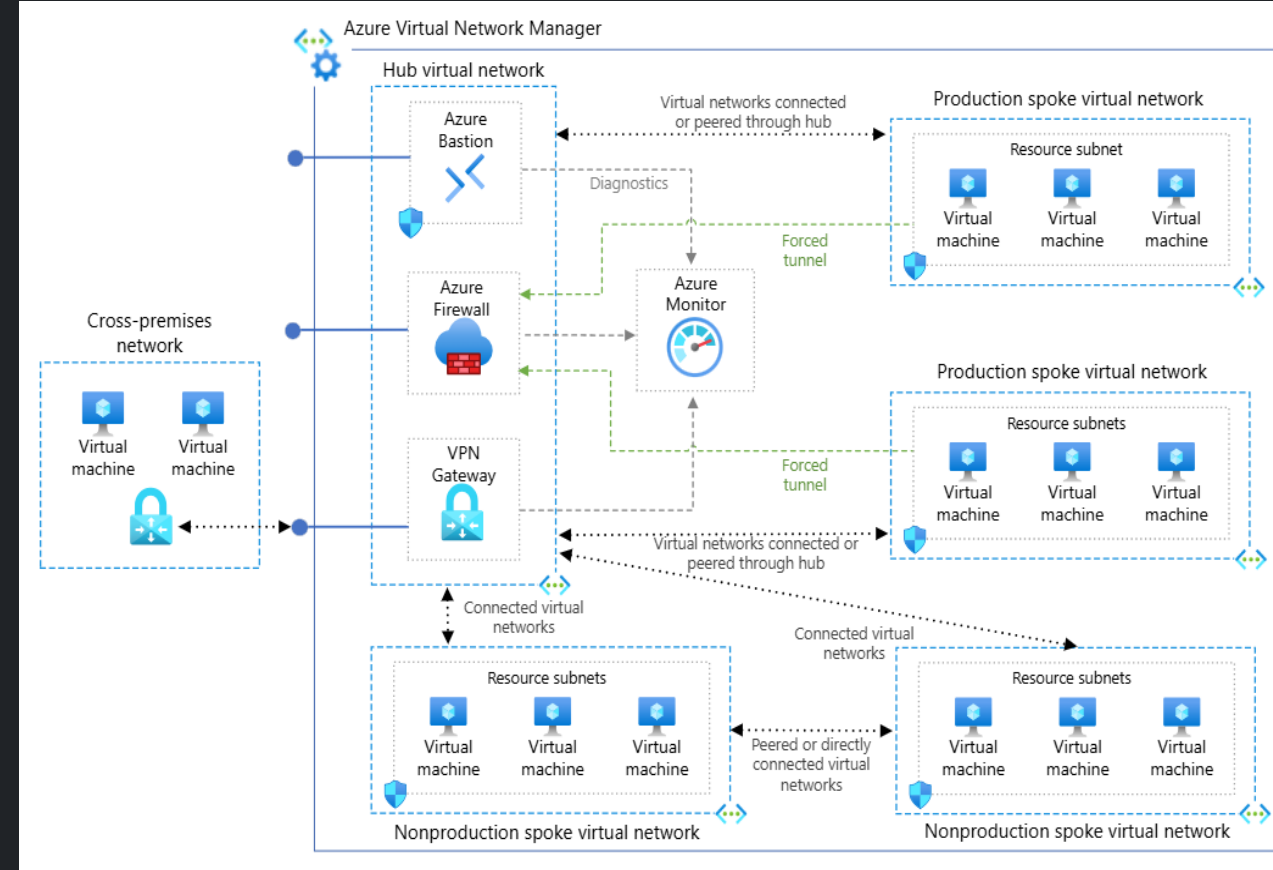
FedRAMP
Federal Cloud Security

Network Security & Cloud Governance



A secure perimeter starts with disciplined network architecture and governance standards that control what enters, what exits, and what can communicate internally.

-  Network segmentation — hub-spoke architecture, private endpoints, and restricted exposure zones
-  Firewall and routing controls — Azure Firewall, DNS filtering, and secure routing policies
-  Private access patterns — VPN, ExpressRoute, and private link configurations for cloud services
-  Azure Policy governance — allowed services, naming standards, tagging, region strategy, and deployment guardrails
-  Subscription and resource management — structured environments that scale without losing control
-  Cost governance integration — spend visibility and right-sizing as part of a sustainable operating model



Managed Operations — Always On



Security is not a project — it is an ongoing commitment. Neurocraft's managed operations model keeps your environment monitored, maintained, and continuously improved.



Observability

- Unified dashboards and real-time alerting
- Log analytics and performance baselines
- Continuous visibility across cloud and hybrid workloads



Backup & Recovery

- Backup policies and retention schedules
- Restore validation and DR runbooks
- Tested on schedule — not just documented



Incident Management

- Defined process with escalation model
- Change control and on-call routing
- Rapid containment and structured remediation



Service Management

- Runbooks and standard operating procedures
- Knowledge transfer and operational reporting
- Self-documenting environments — no tribal knowledge dependency

Business Continuity & Disaster Recovery

When disruption occurs, organizations that have invested in tested recovery plans recover faster and with far less business impact.

01



Prioritize

- Rank systems by criticality
- Define RTO and RPO targets per workload tier
- Map workload dependencies



02



Protect

- Automate scheduled backups with geo-redundant replication
- Enforce least-privilege access controls
- Encrypt backups end-to-end



03



Validate

- Run tabletop and live restore exercises
- Verify RTO/RPO targets are achievable
- Close identified coverage gaps



04



Operate

- Monitor backup health in real time
- Review recovery readiness quarterly
- Update runbooks after infrastructure changes

✓ Outcome: Clients gain a clearer recovery posture and a cloud environment that is easier to trust during disruptions.

Why Neurocraft



Neurocraft combines Microsoft certification, deep industry experience, and a commitment to governed, sustainable operations — making security a strategic differentiator, not a cost center. ^[2]



Microsoft Solutions Partner

Certified and accredited across the Microsoft security and cloud portfolio



Microsoft-Native Delivery

Every control, tool, and practice aligns to Microsoft's Well-Architected and security frameworks



Seamless Integration

Security controls that fit your existing Azure, M365, and hybrid environment



Expert Team

Architects and engineers with real-world experience across energy, healthcare, public sector, and manufacturing



Continuous Improvement

Not just implementation — sustained operations and optimization delivered as an ongoing commitment

Powered by:

Microsoft Partner

Azure

Defender

Sentinel

Entra ID

Smarter Solutions. Stronger Communities.

NEUROCRAFT.AI | Houston, Texas | Info@neurocraft.ai

Get Started

Protecting your organization starts with a conversation — let Neurocraft help you assess your current posture and build a path forward.



Schedule an Executive Security Briefing

Review your current security posture and identify priority gaps with a Neurocraft expert. Tailored for IT leadership and executives — strategic, focused, and actionable.

Contact us to schedule →



Request a Security Assessment

Structured evaluation of your cloud, identity, network, and compliance environment. Receive a clear picture of where you stand and a prioritized roadmap for improvement.

Request your assessment →

Your Organization, AI-Ready

Whether you are just beginning your data journey or ready to scale AI across the enterprise, Neurocraft meets you where you are and takes you where you need to go — on Microsoft's most trusted platforms, guided by a team that has done it before.



Schedule an Executive Briefing

Talk to a Neurocraft expert about your specific challenges and goals.



neurocraft.ai

Explore all service areas and industry solutions online.



Info@neurocraft.ai | Houston, Texas

Smarter Solutions. Stronger Communities.