Jasper Woods

Cloud Engineer

(312) 555-0186 | jasper.woods@example.com | linkedin.com/example/jasperwoods | Chicago, IL 60614

STRENGTHS

Security judgment
During PHI control reviews, converted technical findings into practical safeguards; privacy and infrastructure partners came back for clear next steps.

Cloud delivery
Migration cutovers used dependency maps, rollback plans, and owner testing. That steady rhythm helped application teams trust each release.

Executive reporting
Quarterly roadmaps and cost dashboards gave leaders useful choices, not just technical detail; finance partners gained a clearer view of tradeoffs.

Incident response
Runbooks turned tense cloud alerts into shared action. Teams knew who owned each step, and post-incident reviews produced practical follow-through.

Team partnership
Development and operations peers often brought difficult Azure issues early, knowing troubleshooting would stay focused on service impact and customer needs.

SKILLS

Microsoft Azure | Microsoft 365

Cloud Security

Azure Administration

Infrastructure as Code

Cost Optimization

IAM Governance

Incident Response

Risk Management | Vendor Risk

Security Awareness

SUMMARY

Cloud Engineer with 8 years of IT experience building, administering, securing, and improving **Microsoft Azure** and **Microsoft 365** environments across healthcare, professional services, education, and distributed operations. Brings practical experience with IaaS, PaaS, SaaS, **Infrastructure as Code**, **identity and access management**, monitoring, backup, disaster recovery, cloud migrations, and cost optimization. Converts business, privacy, and security needs into controls that protect PHI and sensitive data under HIPAA/HITECH, PCI, and GDPR requirements. Trusted by leadership for quarterly cloud strategy roadmaps, budget dashboards, risk reporting, vendor assessments, incident response, awareness training, and vulnerability remediation. Ready to bring calm technical judgment, clear communication, and hands-on delivery to Northstar Medical Society's cloud and cybersecurity priorities.

EXPERIENCE

Senior Cloud Security Engineer

Lakefront Health Network | July 2025 - Present | Chicago, IL

Owns Azure and Microsoft 365 improvements for clinical, administrative, and member-facing applications. Leads architecture planning, security governance, Infrastructure as Code delivery, cost analysis, audit support, and incident readiness across hybrid environments. Connects engineering decisions with patient privacy, service reliability, and leadership investment priorities.

- Established quarterly cloud strategy roadmaps with current-state diagrams, **future-state architecture**, migration dependencies, risk decisions, and investment recommendations for leadership planning.
- Reorganized Azure landing-zone policies, **Microsoft Entra ID** governance, privileged access reviews, and Defender alert workflows, strengthening protection for PHI and regulated data.
- Directed Terraform and Azure DevOps delivery for network, storage, compute, and monitoring configurations, giving development and operations teams repeatable deployment patterns.
- Built **cloud budget dashboards** from utilization and billing data, guiding rightsizing, reservation, and storage-lifecycle reviews that surfaced practical savings opportunities.
- Coordinated **incident response**, vulnerability remediation, external audit evidence, **cybersecurity awareness** reporting, and GRC tracking through documented runbooks and ownership controls.
- Partnered with operations, **development teams**, vendors, privacy leaders, and legal stakeholders on cloud controls, third-party risk, contract review, and security decisions.

Cloud Engineer

Redwood Advisory Group | January 2023 - June 2025 | Oak Brook, IL

Administered Azure subscriptions, Microsoft 365 services, virtual networks, application platforms, databases, identity services, and backup resources for a multi-location professional services environment. Delivered migrations, deployment automation, security monitoring, cost reporting, vendor assessments, and compliance support with a strong focus on reliable business operations.

- Migrated 18 on-premises workloads to Azure through dependency mapping, phased cutovers, rollback planning, application-owner reviews, and post-migration validation, reducing transition risk.
- Automated provisioning with Terraform and Azure DevOps pipelines across development, test, and production subscriptions, improving configuration consistency and release readiness.
- Implemented **Microsoft Defender**, Microsoft Sentinel, endpoint protection, firewall rules, DLP policies, and **file integrity monitoring** aligned with internal security standards.
- Prepared monthly security, availability, utilization, and cost reports, translating technical findings into concise recommendations for senior stakeholders and budget owners.
- Supported vendor **security assessments**, privacy contract reviews, access recertifications, and GRC risk treatment plans covering **HIPAA/HITECH**, PCI, and GDPR obligations.
- Worked with development teams to **troubleshoot Azure App Services**, Azure SQL, Key Vault, virtual networks, and backup resources, restoring stable application delivery.

Vulnerability Remediation

Architecture Documentation

Executive Reporting

Disaster Recovery

LANGUAGES

English — Native

Spanish — Intermediate

MY CAREER

- Senior Cloud Security Engineer at Lakefront Health Network (1.1 Years)
- Cloud Engineer at Redwood Advisory Group (2.4 Years)
- Systems and Cloud Administrator at Blue Prairie Technology Services (2.2 Years)
- IT Infrastructure Analyst at Midwest Community College (2.2 Years)

Systems and Cloud Administrator

Blue Prairie Technology Services | September 2020 - December 2022 | Naperville, IL

Managed Windows Server, Azure IaaS, Microsoft 365, VPN, DNS, backup, endpoint, and mobile device services across 30 client sites. Supported migrations, monitoring, recovery planning, Intune administration, security investigations, awareness programs, and audit documentation for varied business environments.

- Managed **Windows Server**, **Azure virtual machines**, Microsoft 365, VPN, DNS, backup, and endpoint environments across 30 client sites, maintaining documented service and recovery procedures.
- Created monitoring dashboards and alert thresholds for compute, storage, identity, backup, and network health, shortening triage paths for recurring **cloud resource issues**.
- Supported on-premises-to-Azure migrations by inventorying applications, validating connectivity, coordinating maintenance windows, and completing acceptance testing with business users.
- Administered Intune MDM enrollment, compliance policies, application deployment, encryption settings, and device retirement for a mobile workforce, improving device governance.
- Contributed to phishing simulations, **cybersecurity awareness training**, incident investigations, and **vulnerability remediation** using Microsoft Defender, Sentinel, and service-management workflows.
- Created architecture diagrams, operating procedures, recovery runbooks, and audit evidence, improving handoffs among infrastructure, development, **vendors**, and compliance reviewers.

IT Infrastructure Analyst

Midwest Community College | May 2018 - August 2020 | Des Plaines, IL

Supported identity, endpoint, server, network, Azure, backup, and security services for faculty, staff, students, and administrative systems across three campuses. Built early experience in cloud administration, incident troubleshooting, access management, security awareness, continuity planning, and control documentation within structured change processes.

- Provisioned **Azure virtual machines**, storage, backups, and test application services under established change-control and access-management procedures, supporting dependable campus operations.
- Resolved infrastructure incidents through log analysis, Microsoft monitoring tools, firewall review, and structured escalation, documenting root causes and preventive actions.
- Assisted with endpoint **antivirus**, **content filtering**, vulnerability scanning, and file-integrity controls for shared computer labs and administrative devices.
- Maintained asset inventories, topology diagrams, access review records, and recovery documentation used during internal risk reviews and continuity exercises.
- Delivered security awareness sessions and quick-reference materials covering phishing, password hygiene, device protection, and privacy practices for more than 200 employees.
- Supported business users and technology teams during maintenance windows, testing, and service recovery, keeping communication clear during shifting priorities.

PROJECTS

Healthcare Cloud Security Roadmap 2026

A roadmap became useful when leadership could see decisions, dependencies, and risk in one place. Created a quarterly Azure and Microsoft 365 plan covering PHI protection, IAM governance, monitoring, backup, migration sequencing, cost controls, and security investment choices.

Azure Workload Migration Factory 2024

Eighteen workloads moved in stages, with each cutover backed by dependency maps, rollback steps, owner validation, and recovery checks. Built a repeatable migration approach for Azure IaaS and PaaS services that helped teams reduce disruption and make post-migration support clearer.

Cloud Cost and Security Dashboard 2025

A billing conversation changed once utilization, security posture, and service ownership appeared together. Created dashboards using Azure usage and billing data to guide rightsizing, reservations, storage lifecycle reviews, control follow-up, and leadership reporting.

LEADERSHIP & AWARDS

- Technology Services Excellence Award, Midwest Community College, 2020
- Azure Migration Delivery Recognition, Redwood Advisory Group, 2024
- Security Improvement Recognition, Lakefront Health Network, 2026
- Quarterly Cloud Strategy Roadmap Leadership, Lakefront Health Network, 2026

EDUCATION

Bachelor of Science in Information Technology

Illinois Institute of Technology GPA: 3.8 2018 Chicago, IL

Coursework: *Cloud computing, network security, database systems, systems administration, information assurance*

CERTIFICATIONS

- Microsoft Certified: Azure Administrator Associate 2021
- CompTIA Security+ 2022
- Microsoft Certified: Azure Solutions Architect Expert 2024
- Microsoft Certified: Cybersecurity Architect Expert 2025

TECHNICAL SKILLS

- **Azure Services:** Azure Virtual Machines, Azure App Services, Azure SQL
- **Microsoft Identity:** Microsoft Entra ID, Privileged Identity Management, Access Reviews
- **Infrastructure as Code:** Terraform, Azure Resource Manager, Azure DevOps
- **Security Monitoring:** Microsoft Defender, Microsoft Sentinel, SIEM
- **Network Security:** Azure Firewall, IDS/IPS, VPN
- **Data Protection:** DLP, Azure Key Vault, File Integrity Monitoring
- **Endpoint Management:** Microsoft Intune, MDM, Endpoint Protection
- **Cloud Operations:** Azure Monitor, Log Analytics, Application Insights
- **Resilience Services:** Azure Backup, Disaster Recovery, Recovery Runbooks
- **Compliance Frameworks:** HIPAA/HITECH, PCI, GDPR
- **Risk Management:** GRC Tools, Vendor Risk Assessments, Risk Treatment Plans
- **Administration Tools:** PowerShell, Windows Server, DNS

PROFESSIONAL AFFILIATIONS

- Azure Chicago User Group, Professional Member, September 2021 - Present
- ISACA Chicago Chapter, Cloud and Information Security Volunteer, January 2023 - Present
- Healthcare Information Security Community Roundtable, Participant, January 2025 - Present

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST