PAULO VALADARES

Toronto, ON | (416) 833-5315 | paulo@dnatechnology.ca | linkedin.com/in/paulovaladares
Interactive CV: paulovaladares.web.app | Company: dnatechnology.ca | IAM Initiative: identityatcore.org

IAM Engineering Manager ● Privileged Access Management ● Identity Governance ● AD and Entra ID Security

SKILLS AND KNOWLEDGE

Security

- PAM Solutions (CyberArk SaaS, SIA, PMP and BeyondTrust)
- IGA (SailPoint)
- Privileged Identity Management (PIM), JIT and Zero Standing Privilege
- MFA (Microsoft, Okta, RSA) and phishing-resistant passkeys
- Conditional Access Policy design and hardening
- Next-gen Device Protection (MS Defender ATP and CrowdStrike)
- SIEM (Splunk, QRadar and SumoLogic)
- Certificate Lifecycle Management (Venafi)
- Email Security (Mimecast ATP and Azure ATP)
- Network Access Control (FortiNAC and Tanium)
- Active Directory Review and Auditing
- Vulnerability Scanning and Management (Nessus, Tenable, DNA Scan)
- Password Enforcement (PPE, PMP, CyberArk Vault)
- Asset Security Management (Absolute and Microsoft Device Management)
- Phishing Awareness (Cofense and ADTP)

Years of Experience in Core Functions

- Active Directory: 9 years
- Microsoft 365: 9 years
- Azure AD (Entra ID): 8 years
- PowerShell: 9 years
- Security: 7 years
- Leadership: 6 years

Soft Skills

- Strong communication skills in both English and Portuguese
- Highly adaptable to evolving security landscapes and technologies
- Analytical problem solver with attention to detail
- Customer-centric approach to IAM services and support
- Continuously learning to stay current in IAM practices
- Effective time management and task prioritization
- Inspires teamwork and drives results through decisive leadership

PROFESSIONAL EXPERIENCE

IAM Engineering Manager

Apr. 2024 to Present

Sobeys Inc., Toronto, ON (Hybrid)

Program Leadership and Strategy

- Direct the enterprise IAM engineering function covering PAM, IGA, Active Directory/Entra ID and Automation, owning the roadmap, vendor strategy and program priorities, and reporting performance and risk posture to senior leadership.
- Built the IAM engineering team from scratch, hiring 12 engineers across PAM, AD/Entra, Automation and IGA, and leading 3 project managers and a business analyst. Retained 100% of hires while replacing low-performing contractors.
- Developed IAM talent through training, certifications, detailed SOPs, video sessions and shadowing, creating a strong culture of knowledge transfer within the team and across departments.
- Trusted decision-maker on enterprise initiatives beyond the IAM program, including the CIAM migration.
- Recognized as a top-performing leader in 2024 and 2025.

Vendor and Commercial Management

- Own the review of multimillion-dollar contracts covering CyberArk licenses and modules and SailPoint IGA, as well as multimillion-dollar statements of work with partners such as Deloitte and Accenture.

- Negotiated more than $6M in license discounts with CyberArk on a 3-year agreement, creating the budget room to expand the program into machine identity, secrets management and endpoint protection.
- Challenged previous vendor engagements and uncovered major architecture gaps that would have made the implementation impossible, saving the company millions in change orders.
- Reduced the CyberArk ticket SLA from 3 weeks to 4 days by establishing a consistent escalation path and close working relationships with the account team. Maintain strong partnerships with CyberArk, SailPoint and CrowdStrike.

Privileged Access Management (CyberArk)

- Directed the redeployment of the entire CyberArk SaaS solution and the migration of legacy connectors such as PSM to Secure Infrastructure Access (SIA).
- More than tripled the number of users connecting securely through CyberArk and raised the compliance status from 27% to 96%.
- Reduced the privileged account risk rating from Critical to Medium and remediated more than 7,000 privileged accounts.
- Introduced automated discovery and onboarding so newly created privileged accounts are enrolled into the vault without manual effort.
- Expanded Just-in-Time (JIT) access and Zero Standing Privilege (ZSP) to all Tier 0 and Tier 1 accounts in both on-prem AD and Entra ID, and secured access for more than 700 external users and 500 internal employees.
- Sustained zero platform incidents in the last fiscal year, with all recurring updates and upgrades delivered without downtime.
- Created and defined the enterprise Break Glass policy and procedures.
- Onboarded Venafi and automated the certificate renewal process through workflows.

Active Directory and Entra ID Security

- Delivered the multi-year AD Hardening program, closing long-standing security gaps: disabled SMBv1, created hardening GPOs for service accounts, strengthened the password policy, defined incident response playbooks, enhanced audit logs and SIEM alerts, and drove the decommission and upgrade of end-of-life systems.
- Rotated the DSRM and KRBTGT accounts and defined a repeatable process for upcoming rotations; created dedicated testing domains on-prem and in the cloud.
- Migrated the legacy RSA MFA to Microsoft MFA with phishing-resistant passkeys, enabled Microsoft and Windows SSPR, and reviewed and hardened the Conditional Access policies in Entra.

Identity Governance and Administration (SailPoint)

- Led the IGA program from pre-implementation through implementation, designing the infrastructure and application integration architecture, including unsupported end-of-life systems and custom workflows.
- Re-engineered the identity lifecycle events for all target applications and defined the access review process in cooperation with IAM Compliance.

Automation and Operational Efficiency

- Led the creation of the Azure Automation environment and delivered more than 10 high-end automations, including complete terminations driven by the HR system, onboarding, movers, inactivity and expired accounts, saving more than 500 hours of operational work across teams.
- Automated the onboarding and termination processes with custom PowerShell scripts, saving more than 200 hours for IAM Operations and Compliance.

IAM Technical Lead Engineer

Apr. 2021 to Apr. 2024

Aviva Canada, Toronto, ON (Remote)

- Technical lead for IAM Operations and Engineering teams.
- Led automation projects, integrating and automating workflows from the ticketing system, Workday and email.
- Collaborated with security leaders in Canada and the UK to design and implement security strategies aligned with industry best practices from Microsoft and other technology leaders.

- SME for projects such as the AD migration, Azure AD MFA/SSPR, the PIM rollout and company-wide M365 application deployments.
- Technical expert leading the IAM transformation program to implement a new IGA platform (SailPoint).
- SME assigned to work closely with the CyberArk and BeyondTrust vendors for implementation, configuration and upgrades.
- SME assigned to apply the principle of AD tiering for user objects in AD for privileged accounts, based on Microsoft guidelines.
- Provided the recommendation and action plan for deploying CrowdStrike to all servers.
- Developed a native PowerShell automation tool for cross-functional processes.
- Delivered several training sessions for the Operations and Engineering teams, covering basic and intermediate PowerShell, Exchange Online, Azure AD and other topics.
- Awarded Employee of the Year and Hackathon winner.

Security Architect **Sept. 2019 to Apr. 2021**

Stikeman Elliott LLP, Toronto, ON (Hybrid)

- Successfully implemented Privileged Identity Management, significantly improving the organization's security score.
- Led the implementation and management of critical security systems, including Network Access Control (FortiNAC), a password management system (PMP), next-gen antivirus (CrowdStrike) and Defender ATP.
- Developed a comprehensive playbook for the SecOps team, enabling rapid and effective response to security incidents.
- Customized SIEM alerts to optimize incident response and proactively prevent new security threats.
- Led multiple projects, including the Mail Flow migration, Datacenter migration, backup, onboarding automation, and other system implementations and upgrades.
- Managed and audited Azure applications and integrations, such as Single Sign-On, auto-provisioning and Conditional Access policies.
- Configured, monitored and maintained policies for the email systems (Exchange and Mimecast).
- Conducted periodic phishing exercises and compiled reports for the CISO, improving phishing awareness among users.
- Collaborated closely with auditors from Deloitte and major banks, providing evidence and ensuring compliance.
- Worked closely with external penetration test consultants to ensure the delivery of high-quality security assessments.

Access Management Analyst **Mar. 2018 to Sept. 2019**

Aviva Canada, Markham and Toronto, ON

- Managed a complex Active Directory structure with more than 5,000 users.
- Worked with IT Information Security, monitoring user access levels and generating daily reports.
- Developed automation scripts that cut the time spent on Active Directory account creation, deletion, edits and reporting by an average of 95%.
- Built automation tools used across multiple departments.
- Produced knowledge-base articles used by the entire team and end users.
- Trained newcomers through daily exercises, driving fast performance improvement.

EDUCATION

Hanson Cambrian College, Toronto, IT, Mobile Application Development — Sept. 2017 to Dec. 2018

IBT College, Toronto, IT, Network Administrator — Nov. 2015 to Nov. 2016

Mackenzie Presbyterian University, São Paulo, Bachelor of Sciences — July 2007 to June 2012