TPO Technologies

Capability Statement

Who We Are

TPO Technologies is a purpose-built, cyber security company servicing government departments and large enterprise organisations.

We are here to flip the narrative on the way you deliver Cyber Security outcomes to your business. We offer start-to-finish engagements, **solution advice**, i**mplementation services, ongoing platform management and procurement services.**

Regardless of your preferred infrastructure platform, cloud, hybrid or on-premise, TPO has the required expertise to ensure your project success.

We are proudly a Queensland based company, employing Queenslanders, in support of Queensland businesses.

Trusted Partners

F5, SentinelOne, zscaler, proofpoint, BeyondTrust, paloalto NETWORKS, Guardicore (Now part of Akamai), FORTINET, Abnormal SECURITY, SpyCloud, SailPoint, ARISTA, FORCEPOINT, CHECK POINT, tenable

Why TPO

A Safe Pair of Hands

TPO's leadership team encompasses over a century of business and technology experience, delivering outcomes to ICT and Cyber Security Teams in Queensland, and around the world.

From the Ground Up

Reimagine how technology can drive your business or department forward. Deliver better outcomes faster and more reliably with our team.

Trust. Provide. Outcome

Building trust one engagement at a time. Words don't build trust. Outcomes, partnership and transparency is what sets our business apart and what we demand of ourselves in every interaction.

Why Now

The Right People

Accessing the 'right' Cybersecurity resources is critical to the operational protection of businesses. Specialist expertise is required to maximise technology platform performance.

Growing Industry Noise

Internal teams are being bombarded with industry noise due to the buzzing vendor landscape. We replace the noise with focused relevance.

Eroding Industry Flexibility

Small technology partners provide flexibility, large partners struggle to accommodate. Most technology projects have challenges and need agile thinking and timelines. We adapt and evolve.

Social Procurement Policy Alignment

- Queensland staff / Queensland focus
- Small business status with the Queensland Government
- Queensland Government ICT Panels in process
- Team hiring based on technical prowess, business acumen and passion

TPO Technologies

Introduction from Chief Technology Officer

Dear Industry Peers,

Welcome to TPO Technologies, please find overview of our technical capabilities below. My name is Frazer Thompson, and I'm the CTO of TPO. I've been working, and learning, in the IT industry both in technical and leadership capacities for over 20 years... and I still love getting my 'hands dirty' pursuing the PERFECT outcome!

The TPO Professional Services team brings many decades of experience across numerous industry verticals. Sharing expertise in the areas of cyber security, complex application delivery, technology platform management and networking. We apply these capabilities to cloud, on premise and hybrid environments. We are passionate about maintaining extensive vendor certifications, ensuring we are always able to provide our clients with the best outcomes and most current advice.

Over the next few pages, you will get exposure to some of our delivery experience and capability. Whilst not exhaustive, these projects highlight the incredible skills we leverage to support our clients, repeatedly delivering world class outcomes. These examples demonstrate our position as a trusted partner for large enterprise, state and local government agencies throughout Queensland.

I look forward to meeting you and your technical team in the near future.

Regards,
Frazer

Key Project Interest

Application Delivery
Advanced Networking
Network Security
Endpoint Security
Secure SD WAN
SASE
SIEM Log Correlation, Tuning and Playbooks
Platform Management
Platform Tuning and Optimisation
Identity and Access Management
Operational Technologies Security
Microsegmentation

TPO Technologies

State Government – F5 and Palo Alto Networks

TPO Technologies' professional services staff successfully migrated 4 F5 BIG-IP instances from physical to virtual, decommissioned 2 additional F5 SSLO instances replacing with Palo Alto Networks based SSL decryption, migrating existing Palo Alto Networks physical firewalls from 3 vSYS instances to a distributed design of 4 virtual edition Palo Alto Networks firewalls, migrating all IPsec, NAT, routing, and a variety of other integrations, in a single successful weekend cutover.

This migration came about after 2 years of design with another party on a different solution, with 2 cutover attempts by the third party unfortunately failing, our engineers were asked to step in.

Working closely with the client the third-party an NSX based design was replaced with a Palo Alto Networks firewall design, pulling all layer 3 connectivity through various tiers of firewalls providing various next generation firewall functionality. Due to the timing of the previous project, license expiration and hardware support, our engineers were required to design and implement the migration in the space of four weeks, with cutover failure not being an option. A single successful migration attempt took place, cutting over the new dispersed virtual firewall systems, replacing F5 SSLO with Palo Alto Networks based SSL decryption, and migrating existing F5 LTM/APM instances across to newly deployed F5 BIG-IP installations hosted on new VMware security cluster infrastructure.

State Government – F5 Networks

TPO Technologies' professional services staff migrated out of warranty physical F5 BIG-IP devices including a version upgrade to a supported BIG-IP version, of various BIG-IP vCMP instances using a hard cut over migration methodology, with 20 seconds of downtime. This project also included extending a single vCMP guest into an HA cluster with zero downtime.

Our methods to migrated, upgrade, and mitigate risks leveraging offline testing and issue remediation, allowed for all issues to be identified prior to any production configuration. Some issues were able to be mitigated prior to the migration, whilst others were remediated during the migration. The only limitation to the methods used in this migration come down to network convergence, typically ARP timeouts if gratuity is not accepted by adjoining switching and/or routing infrastructure.

Healthcare – F5 Focus

TPO Technologies' professional services staff designed and deployed an F5 network security architecture as part of a large green field data centre redesign, deploying 36 F5 BIG-IP instances using LTM, GTM (DNS), APM, ASM, and AFM modules. The various F5 BIG-IP instances tied directly into the infrastructure, integrating into the routing of all network traffic, analysing traffic using SSL decryption zones, and load balancing across various data centre nodes. Access Policy Manager was implemented to replace legacy SSL VPN solutions, centralise authentication as an IdP, and secure remote application delivery.

The F5 devices are core to this network, providing routing and NAT functionality for all North/South and 50% of East/West traffic. Various zones provide a tiered configuration starting with DDoS and network level filtering at the edge, SSL decryption for all traffic offloading to firewalls for inspection and re-encryption, and service load balancing where required. The LTM module is used to steer traffic alongside routing protocols, merging with NSX South of the protection zones. F5 BIG-IP GTM, now known as DNS, is used for DNS inspection and dynamic control of data centre service selection, optimising path selection prior to internal LTM load balancing selection. Access Policy Manager integrates with over 100 SAML service providers using a single access policy, serving over 80 SAML Identity Providers customising available authentication methods including a variety of MFA options. Access Policy Manager also serves thousands of remote access endpoint options including remote desktop access, Portal Access, L3 VPN, and application tunnels.

Construction – F5 and Advanced Networking

TPO Technologies' professional services staff migrated legacy F5 BIG-IP deployments with LTM and APM instances, across data centers using GTM (DNS), upgrading and optimising the configuration while concurrently migrating legacy firewalls to NGFW's and reconfiguring the entire network connectivity solution. Abundant public addressing allowed for an inline migration methodology with a heavy focus on application delivery pre-production, user acceptance testing and finally production migration, on a per application basis. The client was previously at ease with downtime up to an hour as acceptable, Our professional services staff worked heavily with the client to optimise and further secure the national network allowing all network and security points to be self-healing to the point where downtime almost became a thing of the past.

The optimisation of the network configuration included full routing reconfiguration implementing BGP end to end, allowing integration into AWS, increasing automation of remote site builds, and creating an almost negligible failover solution between data centres. At the end of the migration zero static routes existed on this network. Access Policy Manager optimisation included creating a customised SAML Identity Provider, replicating the look and feel of the Microsoft login page to provide a simple and familiar end user experience. Authentication systems were extended to include Kerberos constrained delegation which required us to redesign and optimise the existing Microsoft AD DS infrastructure across all sites, this included the added benefit of optimised AD and DNS access for servers and endpoints which increased network performance substantially.

Banking – SD WAN Focus

TPO Technologies' professional services staff designed, implemented, and maintained a complex Fortinet SDWAN deployment for a 80 site banking institution, migrating from an existing simple 4G failover Cisco WAN. The deployment included 3 links per site, with 2 data centres, and several VRFs separating core banking systems. All configuration was automated and deployed via scripting methodologies using FortiManager, monitored using FortiAnalyzer and via an external SOC/SIEM.

The technical capabilities of this installation included 12 virtual links in total, across 3 physical links, catering for layer 3/4 and layer 7 application steering without the requirement of SNAT for symmetric return. All networking was BGP and BFD integrated with failover times or traffic steering decisions occurring in near real time. Once the deployment of the data centres was complete, the remote sites were meticulously organised to be cut over 2 per day, every consecutive day, until completion. The speed of the traffic failover and steering occurred quickly, catering for sites where the ISP had not yet provisioned all 3 links. Due to the complexity of existing legacy systems not all configurations could be automated, however after answering just a few questions the configuration of a replacement device or new site was as close to zero touch as possible. The deployment came prior to SD WAN provisioning technology from Fortinet became generally available (GA).

Meat and Food Processing – Advanced Networking

TPO Technologies' professional services staff redesigned the client's routing infrastructure, collapsing WAN edge, Internet Edge, and Core/Distribution networking, incorporating remote Riverbed SD WAN and MPLS sites, global connectivity and both AWS and Azure connectivity. The migration was implemented in 3 phases separating the WAN edge collapse, Internet Edge and Core/Distribution network zones. A variety of network protocols were already in place and required a complete redesign and convergence with zero down time. After the success of the WAN edge and Core/Distribution phases the client then used the organisations professional services staff to incorporate a migration from existing Cisco FTD firewalls to Palo Alto Networks firewalls, during the Internet edge redesign phase.

Prior to the redesign many routing protocols were in use, including static, PBR, OSPF, RIP, iBGP, eBGP and EIGRP. The design collapsed all routing protocols into eBGP barring a few static routes that were unavoidable due to systems owning IP addressing but not participating in routing protocol configuration. Each cutover phase required zero down time due to abattoir, administration, distribution, and warehousing operations across both Australia, but also in New Zealand and the US. After the success of the WAN edge and Core/Distribution network redesign, the Cisco FTD to Palo Alto Networks firewalls finalised the complete network reconfiguration.