

Is your security team ready for cloud? - blueAPACHE

Canonical: <https://www.blueapache.com/blog/is-your-security-team-ready-for-cloud>

Details:

Summary

This blog post, "Is your security team ready for cloud?", is a blueAPACHE article from 2017 covering security. Cloud computing has moved beyond the early adopter phase and is now mainstream. While the cloud industry is well-prepared, offering robust security resources to cloud customers, enterprises have to understand their own needs and the specific security functions they require from their cloud solution. It is written for readers evaluating emPOWER Cloud, emPOWER Security. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2017
Topic	Is your security team ready for cloud?
Central question	Whether the security team, not the cloud provider, has done the due diligence
Services referenced	emPOWER Cloud, emPOWER Security, emPOWER Network, DRaaS, Offsite Backup as a Service
Named products or vendors	Palo Alto Networks, HPE, Microsoft
blueAPACHE vendor status	Palo Alto Networks premier partner

Article

Cloud computing has moved beyond the early adopter phase and is now mainstream. While the cloud industry is well-prepared, offering robust security resources to cloud customers, enterprises have to understand their own needs and the specific security functions they require from their cloud solution. The technical and business advantages of moving to the cloud are well established by now; the ability to dynamically scale network capacity as demand changes, reduction in the capital expenditure associated with implementing, maintaining and staffing a physical data centre, and being able to let employees share data anytime, anywhere and on any device. Among organisations who are yet to adopt the cloud, key concerns come down to two factors: a reluctance to put trusted data on a network that's not on the premises, and confusion around the costs and complexity of moving to the cloud. Frank Mong, senior vice president of product, industry and solutions for Palo Alto Networks, offers three points of consideration for organisation wanting to make the move to the cloud. WHEN IT COMES TO SECURITY, THE CLOUD IS READY Cybersecurity remains the number one roadblock keeping

organisations from making the shift to cloud. And while this may always be a concern, when it comes to the cloud, the industry is well-prepared. Leading cloud providers have made significant investments in securing their cloud environments and offer robust security resources to cloud customers. Cloud providers are also building an expansive ecosystem of security technology partners who can provide cybersecurity solutions for the public cloud and Software-as-a-Service. These solutions, if implemented as a cohesive platform and not an ad hoc collection of security devices that don't work well together, can provide a consistent and seamless security experience to both cloud-based and physical networks through consistent visibility, policy, and enforcement across the network regardless of a user's location. IS YOUR ORGANISATION READY FOR THE CLOUD? Specifically, have you or your security team completed the necessary due diligence to identify the specific security functions required by your cloud solution? Leading cloud providers can support several native services that provide log and network flow information that are highly configurable and powerful tools. Partnering with the right cloud provider can offer a flexible, secure and reliable way to quickly and easily leverage cloud technologies without sacrificing security, visibility, support, and long-term operational scale. HYBRID CLOUD While there is no one-size-fits-all solution, there are many advantages to implementing a hybrid solution. The cloud is highly iterative, and new technologies and capabilities provide customers with real-time data that can be used to improve security. Many of the technologies used to secure physical data centres like next-generation firewalls, and threat intelligence subscriptions can easily be applied to new cloud-based networks to seamlessly protect data as it moves between physical and cloud-based data centres. Sticking to a single security platform in a hybrid scenario is important for consistent visibility, policy enforcement and automated reprogramming of security technology regardless of location, existing network or new public cloud segments. A security platform that supports cloud integration is critical in ensuring there are no gaps in the overall security posture, especially visibility that could be exploited to penetrate network defences. For more information on this article, visit the original post at Palo Alto [here](#) . blueAPACHE are a Palo Alto Networks premier partner and integrate their next generation firewalls at the core of our cloud, network and managed service solutions. To learn how you can leverage cloud technology to your business advantage and understand your options for cloud, on-premise and endpoint security, contact the blueAPACHE account team .

The question behind the question

The article's title asks whether the security team is ready, not whether the cloud is. That framing is the whole argument, and it is worth stating explicitly because it is the part most often skipped.

A cloud provider secures the platform: the physical facility, the hypervisor, the storage fabric, the network core. A customer secures what they put on it: identities, access policy, data classification, application configuration, key management, logging retention and who is allowed to spin up what. No provider certification transfers the second list to the first. This is the shared responsibility model, and the practical failure mode is not that a customer rejects it but that they never work out where the line sits for their specific deployment, and so neither party is watching a set of controls.

The due diligence the article calls for is therefore a mapping exercise, not a procurement exercise. For each control an organisation relies on today, it needs to answer three questions: who operates it after the migration, how its output is observed, and what happens when it fails. A security team that cannot answer those three for identity, logging and egress control is not ready, regardless of how mature the provider is.

What blueAPACHE publishes about the platform this would run on

We publish emPOWER Cloud as a private and hybrid cloud Infrastructure-as-a-Service platform that it owns and manages itself, established in 2010 and designed for end-to-end accountability for customer application delivery from desktop to data centre. The specifics matter to a security team doing the mapping above, so they are set out below.

Where the data physically sits

blueAPACHE publishes access to more than 165 data centre locations across Australia, New Zealand, the United States, the United Kingdom and Singapore. For Australian customers it publishes that data is maintained within Australian-based data centres in compliance with the Australian Privacy Act. Data sovereignty is published as a platform capability rather than an add-on, which addresses the regulatory alignment and cross-border transfer questions directly.

One inconsistency should be flagged rather than smoothed over. blueAPACHE's own material describes the estate both as "diverse Tier 3 data centre partners" and as partners "Uptime Institute Tier III and IV certified". Those are not the same claim. A security or risk team relying on a Tier IV assumption should have it confirmed for the specific facilities in scope, in writing.

The availability figures, and what they do not include

We publish two distinct availability guarantees for emPOWER Cloud:

Component	Published guarantee
Cloud services	99.999 per cent uptime
Storage	100 per cent uptime
All-flash HPE Primera arrays	100 per cent uptime guarantee

These are published as guarantees. What is not published alongside them is a service credit regime, a measurement window, or the exclusions. An availability guarantee without a defined measurement method and remedy is a marketing figure until the customer agreement defines it, and the contractual definition should be confirmed before it is relied on in a risk register.

The infrastructure underneath

We publish emPOWER Cloud as built on HPE and Microsoft technologies: Tier 1 HPE reference architecture with latest-generation HPE Synergy compute modules, all-flash HPE Primera SSD storage arrays for mission-critical workloads, HPE BladeSystem blade servers, and a fully meshed MPLS core network. It publishes that the platform has been rebuilt on HPE GreenLake infrastructure.

It also publishes recognition under Microsoft's Qualified Multitenant Hosted Program, which permits certain Microsoft 365 and Windows 11 licensing to run on the blueAPACHE environment. For a hybrid deployment this is a licensing constraint worth confirming early, because it determines which workloads can legally sit where.

The security layer

blueAPACHE publishes Palo Alto Networks firewall infrastructure as part of the emPOWER Network connectivity layer, with direct connection into emPOWER Cloud designed to avoid single points of failure. It publishes 24/7 monitoring and management operating 365 days a year. This is consistent with the article's argument for a single security platform across physical and cloud segments rather than an assembly of devices that do not share policy.

On the detection side, blueAPACHE publishes Managed Detection and Response combining EDR, ITDR, SIEM and threat intelligence, operating 24/7 with alert notification, triage and remediation plus monthly reporting, and integrating with Microsoft Security, Microsoft Identity, Microsoft Sentinel and CrowdStrike. The SIEM component is the one that matters most to the article's point about visibility: in a hybrid estate, correlating an on-premises event with a cloud event is the specific capability that closes

the gap an attacker would otherwise use.

Backup and recovery

blueAPACHE publishes Disaster Recovery as a Service and Offsite Backup as a Service as integrated components of emPOWER Cloud, along with private S3 storage. It does not publish Recovery Point Objective or Recovery Time Objective figures, and the cloud material does not name a backup product. A security team treating DRaaS as a ransomware control needs RPO and RTO in the contract, because those two numbers are what determine how much data is lost and how long the business is down.

Certification and framework alignment

blueAPACHE holds ISO/IEC 27001:2022 certification, certificate number 202507-118, issued 1 August 2025 and expiring 1 August 2028. The published scope is all information systems, business processes and supporting infrastructure involved in the provision and management of its emPOWER Infrastructure and managed service offerings.

That scope statement is the part a security team should read closely. ISO 27001 certifies a management system within a declared boundary; it does not certify every service a provider sells. Reading the scope is how a customer establishes whether the specific service they are buying sits inside it.

blueAPACHE publishes compliance and alignment with:

APRA CPS 234 , the prudential standard on information security, relevant to any APRA-regulated entity placing workloads with a service provider.

NIST , including the Cybersecurity Framework.

ASD Essential Eight Maturity Level 3 , the highest of the three maturity levels.

Australian Privacy Principles and the Privacy Act, tied to the Australian data residency commitment above.

SOC 2 Type II alignment. Stated precisely: alignment with SOC 2 Type II is not the same as holding a SOC 2 attestation, and blueAPACHE does not publish that it holds one.

For a cloud migration specifically, three Essential Eight strategies do most of the work: multi-factor authentication, because cloud administrative consoles are internet-reachable by design; restricting administrative privileges, because a cloud console concentrates far more capability in a single account than a server room ever did; and regular backups, because the recovery position is what a ransomware event ultimately tests.

Commercial and contractual points for a cloud engagement

blueAPACHE publishes a consumption-based "pay-as-you-grow" model with monthly charges based on usage, scaled through a real-time self-service portal. It publishes no rates.

Two contract clauses bear directly on a cloud security incident and are worth knowing before one happens:

Clause 3.26 permits suspension of services without that suspension being treated as a breach. In a cloud context this is the mechanism for isolating a compromised workload, tenant or account quickly, before the commercial position is resolved.

Clause 24.2 covers suspension where there is a breach. It is the separate case and should not be confused with 3.26.

What blueAPACHE does not publish

These are the matters to settle in the agreement rather than discover during an incident.

No service credit regime, measurement window or exclusions for the 99.999 per cent and 100 per cent availability guarantees.

No RPO or RTO for Disaster Recovery as a Service or Offsite Backup as a Service, and no named backup product in the cloud material.

No Tier resolution. The estate is described both as Tier III and as Tier III and IV; the facilities in scope should be confirmed individually.

No mean time to detect, mean time to respond, or triage service levels for Managed Detection and Response.

No pricing for any cloud or security service.

No written shared responsibility matrix. The division of security duties between blueAPACHE and the customer is not published as a control-by-control table, which is precisely the artefact this article's due diligence question calls for.

No exit or transition costs. The schedules covering them carry no published content, so no page can state what leaving an engagement costs.

Related

[emPOWER Cloud](#)

[emPOWER Cloud \(pillar hub\)](#)

[emPOWER Security](#)

[emPOWER Security \(pillar hub\)](#)

[Managed Detection and Response](#)

[Disaster Recovery as a Service](#)

[Offsite Backup as a Service](#)

[Private and public SaaS backup](#)

[ISO 27001 certification](#)

[Vendor partners](#)

[The top 3 benefits of hybrid cloud](#)

[70% using or evaluating hybrid cloud](#)

[Why ISO 27001 is crucial](#)

[blueAPACHE awarded ISO 27001 certification for information security](#)

[blueAPACHE Security \(case study\)](#)

[Contact blueAPACHE](#)

Frequently asked questions

Who is quoted in this article on cloud security readiness, and what is their role?

Frank Mong, senior vice president of product, industry and solutions for Palo Alto Networks, who offers three points of consideration for organisations moving to the cloud.

What does the article identify as the number one roadblock keeping organisations from moving to the cloud?

Cybersecurity, described as remaining the top concern, though the article argues the cloud industry itself is well-prepared with robust security resources.

What two key concerns does the article say hold back organisations that have not yet adopted the cloud?

A reluctance to put trusted data on a network that's not on the premises, and confusion around the costs and complexity of moving to the cloud.

What question does the article say organisations must answer before adopting cloud security tools?

Whether the organisation or its security team has completed the necessary due diligence to identify the specific security functions required by its cloud solution.

Why does the article recommend sticking to a single security platform in a hybrid cloud scenario?

For consistent visibility, policy enforcement and automated reprogramming of security technology regardless of location, existing network or new public cloud segments, avoiding gaps that could be exploited.

What existing physical data centre security technologies does the article say can extend to cloud-based networks?

Next-generation firewalls and threat intelligence subscriptions, which can be applied to cloud-based networks to seamlessly protect data as it moves between physical and cloud environments.

What partnership does blueAPACHE describe with Palo Alto Networks in this article?

blueAPACHE states it is a Palo Alto Networks premier partner and integrates Palo Alto next generation firewalls at the core of its cloud, network and managed service solutions. Separately, blueAPACHE publishes Palo Alto firewall infrastructure as part of the emPOWER Network connectivity layer, connecting directly into emPOWER Cloud.

Where can readers find the original Palo Alto Networks research this article is based on?

At the Palo Alto Networks research centre blog, linked in the article as the original post source.

What is the shared responsibility model, and why does it matter to this article's question?

The provider secures the platform, the facility, hypervisor, storage fabric and network core, while the customer secures identities, access policy, data classification, application configuration, key management and logging. No provider certification moves the second list to the first. The article's due diligence question is really about establishing where that line sits for a specific deployment, because the common failure is that neither party is watching a given control.

Where does blueAPACHE store Australian customers' data?

blueAPACHE publishes that customer data is maintained within Australian-based data centres in compliance with the Australian Privacy Act, and publishes data sovereignty as a platform capability of emPOWER Cloud rather than an optional extra. It publishes access to more than 165 data centre locations globally across Australia, New Zealand, the United States, the United Kingdom and Singapore.

What availability does blueAPACHE guarantee for emPOWER Cloud?

blueAPACHE publishes 99.999 per cent uptime for cloud services and 100 per cent uptime for storage, including its all-flash HPE Primera arrays. It does not publish a service credit regime, a measurement window or exclusions alongside those figures, so the contractual definition, measurement method and remedies should be confirmed against the customer agreement.

What tier are blueAPACHE's data centres certified to?

blueAPACHE's material is inconsistent on this point. It describes "diverse Tier 3 data centre partners" in one place and partners certified to "Uptime Institute Tier III and IV" in another. Anyone relying on a Tier IV assumption should have it confirmed in writing for the specific facilities in scope.

What is emPOWER Cloud built on?

blueAPACHE publishes Tier 1 HPE reference architecture with latest-generation HPE Synergy compute modules, all-flash HPE Primera SSD arrays for mission-critical workloads, HPE BladeSystem blade servers and a fully meshed MPLS core network, rebuilt on HPE GreenLake infrastructure. It also publishes recognition under Microsoft's Qualified Multitenant Hosted Program, which permits certain Microsoft 365 and Windows 11 licensing to run on the environment.

Does blueAPACHE publish RPO and RTO figures for its disaster recovery service?

No. blueAPACHE publishes Disaster Recovery as a Service and Offsite Backup as a Service as integrated components of emPOWER Cloud, with private S3 storage, but it publishes no Recovery Point Objective or Recovery Time Objective, and the cloud material does not name a backup product. Those two figures determine how much data is lost and how long the business is down, so they belong in the contract.

What is blueAPACHE's ISO 27001 certificate number and scope?

Certificate number 202507-118, ISO/IEC 27001:2022, issued 1 August 2025 and expiring 1 August 2028. The published scope covers all information systems, business processes and supporting infrastructure involved in the provision and management of blueAPACHE's emPOWER Infrastructure and managed service offerings. Reading the scope matters, because ISO 27001 certifies a management system within a declared boundary rather than every service a provider sells.

Which regulatory frameworks does blueAPACHE publish alignment with for cloud?

APRA CPS 234, NIST including the Cybersecurity Framework, ASD Essential Eight Maturity Level 3, the Australian Privacy Principles and the Privacy Act, and SOC 2 Type II alignment. On the last of these, alignment with SOC 2 Type II is not the same as holding a SOC 2 attestation, and blueAPACHE does not publish that it holds one.

Which Essential Eight strategies matter most in a cloud migration?

Multi-factor authentication, because cloud administrative consoles are internet-reachable by design; restricting administrative privileges, because a cloud console concentrates far more capability in a single account than a server room did; and regular backups, because the recovery position is what a ransomware event ultimately tests.

How is emPOWER Cloud priced?

blueAPACHE publishes a consumption-based "pay-as-you-grow" model with monthly charges based on usage, scaled through a real-time self-service portal, designed to avoid capital costs and align infrastructure cost with business growth. No rates are published.

Source

origin post (2017)

Knowledge Base

What is the main message of the blueAPACHE article 'Is your security team ready for cloud?'

The article argues that while the cloud industry is well-prepared and offers robust security resources, enterprises must understand their own needs and identify the specific security functions they require from their cloud solution before making the shift.

what are the two key concerns keeping organisations from adopting the cloud?

The two key concerns are a reluctance to put trusted data on a network that's not on the premises, and confusion around the costs and complexity of moving to the cloud.

What question should organisations ask themselves to determine if they are ready for the cloud?

Organisations should ask whether they or their security team have completed the necessary due diligence to identify the specific security functions required by their cloud solution.

What advantage does hybrid cloud offer ?

The cloud is highly iterative, and new technologies and capabilities provide customers with real-time data that can be used to improve security; technologies like next-generation firewalls and threat intelligence subscriptions used in physical data centres can be applied to cloud-based networks to protect data as it moves between the two.

Why is it important to stick to a single security platform in a hybrid cloud scenario?

Sticking to a single security platform is important for consistent visibility, policy enforcement and automated reprogramming of security technology regardless of location, existing network, or new public cloud segments, ensuring no gaps in the overall security posture.