EMPOWER MANAGED DETECTION & RESPONSE

DETECT SOONER.
RESPOND FASTER.
STAY RESILIENT.

blueAPACHE

WHY **MDR?**

Cyber threats don't keep office hours. From ransomware and phishing to identity-based compromise, attacks are growing in speed and sophistication. Traditional tools like antivirus and firewalls are no longer enough.

Managed Detection and Response (MDR) combines:

- Continuous monitoring across your IT environment
- Advanced analytics and threat intelligence to spot issues quickly
- Human expertise to investigate and remediate threats before they cause damage

With blueAPACHE MDR, you gain enterprise-grade protection, without the overhead of building and maintaining your own Security Operations Centre (SOC).

THE IDENTITY THREAT **LANDSCAPE**

Attackers don't break in, they log in. Identity is now the #1 target for cybercriminals. According to Rapid7's 2025 Access Brokers Report, privileged access aorganisations is being sold for as little as $1,000. VPN, RDP, and domain credentials are top targets.

TOP 5 IDENTITY THREATS **YOU CAN'T IGNORE**

1. **Credential Theft:** Stolen passwords give attackers full access
2. **Adversary-in-the-Middle (AiTM):** Hijacks sessions and bypasses MFA
3. **Shadow Workflows:** Stealthy email rules exfiltrate sensitive data
4. **Rogue Applications:** Malicious integrations escalate privileges
5. **Session Hijacking:** Stolen tokens give attackers uninterrupted access

BLUEAPACHE'S MDR **ADVANTAGE**

We go beyond standard MDR services by:

1. Providing 24/7 alert notification, triage, and remediation across your full IT environment and security stack

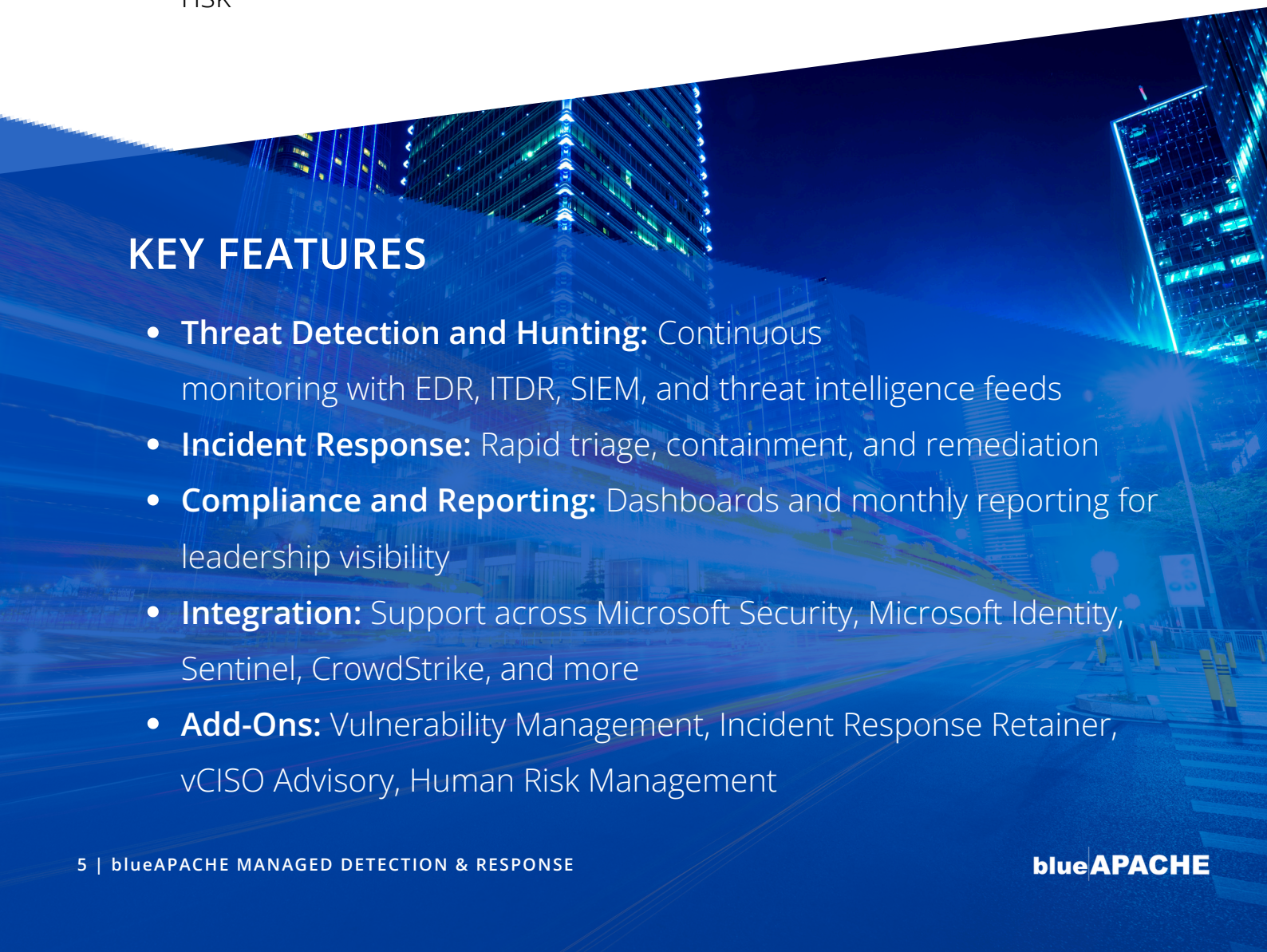
2. Bridging Security Operations and IT Operations to shorten response times and accelerate recovery

3. Offering scalable solutions that fit different business needs, maturity levels, and budgets

WHO IS IT **FOR?**

blueAPACHE MDR is ideal for organisations that need enterprise-grade protection without the overhead of building and maintaining an in-house SOC. It's designed for:

- Businesses seeking proactive protection against cyber threats
- IT teams looking to reduce operational burden across security.
- Organisations needing to demonstrate compliance
- Leadership teams seeking visibility and assurance around cyber risk



KEY FEATURES

- **Threat Detection and Hunting:** Continuous monitoring with EDR, ITDR, SIEM, and threat intelligence feeds
- **Incident Response:** Rapid triage, containment, and remediation
- **Compliance and Reporting:** Dashboards and monthly reporting for leadership visibility
- **Integration:** Support across Microsoft Security, Microsoft Identity, Sentinel, CrowdStrike, and more
- **Add-Ons:** Vulnerability Management, Incident Response Retainer, vCISO Advisory, Human Risk Management

USE CASES **WE SOLVE**

- A brute-force attack on a remote desktop service is detected at 2:00am. Our SOC isolates the endpoint and blocks the attacker before lateral movement begins.

- A compromised Microsoft 365 account is used to send phishing emails. We detect the rogue OAuth app, disable the identity, and guide your team through remediation.

- A ransomware payload is dropped on a user's device. Our EDR quarantines the file and prevents execution-before encryption can begin.

OUTCOMES YOU **CAN EXPECT**

- Reduced risk profile and stronger compliance
- Faster incident detection, containment, and remediation
- Continuous visibility into security threats
- Lower burden on IT teams, with expert-led guidance
- Demonstrable effort in protecting sensitive data and meeting regulatory requirements

WHY **BLUEAPACHE**

As an ISO 27001 certified organisation with ASD Essential 8 Level 3 maturity, blueAPACHE is trusted by organisations across Australia and beyond.

Our MDR service is backed by:

- Expert SOC analysts and threat hunters
- Industry-leading platforms and threat intelligence
- Proven ITIL-aligned processes for incident management
- Long-term partnerships that keep our customers ahead of evolving threats

COMPLIANCE-ALIGNED WITH:

ISO/IEC 27001 • Australian Privacy Principles • Essential Eight (ASD) • NIST CSF • SOC 2 Type II • GDPR

TAKE BACK CONTROL OF YOUR SECURITY

Protect your business with 24×7 Managed Detection and Response from blueAPACHE. Our team will work with you to assess your environment, align the right MDR solution, and provide ongoing protection tailored to your business.

Visit www.blueapache.com/mdr/ or contact us to get started.