SECURE CENTRAL
A Pioneer Infotech Company

REGIONAL DISTRIBUTION & SUPPORT
ASIA PACIFIC · SOUTHEAST ASIA

MANAGED DETECTION & RESPONSE

HUNTRESS

Managed cybersecurity that finds and stops threats.

Enterprise-grade protection built for the lean IT teams running **Southeast Asia's** small and mid-sized businesses — powered by a **24/7 AI-centric SOC**, delivered, deployed and supported in-region by SecureCentral.

24/7	5M+	15M+	277k+
AI-CENTRIC SOC COVERAGE	ENDPOINTS PROTECTED	IDENTITIES PROTECTED	ORGANISATIONS SECURED

DELIVERED & SUPPORTED ACROSS

Singapore · Malaysia · Indonesia · Thailand · Philippines · Vietnam · Australia · New Zealand

01

THE SOUTHEAST ASIA THREAT REALITY

A growth market for your business — and for organised cybercrime.

Southeast Asia is digitising faster than almost anywhere on earth — cloud-first operations, Microsoft 365 everywhere, hybrid teams across six time zones, and IT departments of three people. Attackers have noticed, and they now run standardised, profit-driven playbooks at industrial scale.

277%

Surge in RMM tool abuse

Year-on-year growth in attackers weaponising the remote management tools your IT team already trusts — now 24% of all observed incidents.

37.2%

Identity attacks from stolen access

Access-policy and trust-boundary violations — shady logins from risky locations, malicious infrastructure and unauthorised VPNs.

18.9%

AiTM phishing that beats MFA

Adversary-in-the-middle attacks able to bypass multi-factor authentication, with mailbox manipulation a further 19%.

51.3%

Ransomware from just four crews

Akira, Medusa, Qilin and RansomHub together account for over half of all ransomware incidents observed.

WHY IT LANDS HARDEST ON SEA BUSINESSES

- **Lean IT teams.** One or two generalists carrying servers, helpdesk, networks — and security.
- **Microsoft 365 saturation.** Rapid cloud adoption without matching identity monitoring.
- **Multi-country footprints.** Operations spanning SG, MY, ID, TH, PH and VN with no 24-hour watch.
- **Budget reality.** Enterprise SOC pricing simply does not fit an SMB cost base.
- **Tightening regulation.** PDPAs, Cyber Security Act obligations and customer security audits.

WHAT BREAKS FIRST

- **Business email compromise.** A finance mailbox is silently rewired to divert supplier payments.
- **Account takeover.** Credentials bought cheaply from an access broker, used to look like staff.
- **Ransomware.** Encryption on a Friday night; discovery on Monday morning.
- **Living-off-the-land.** Legitimate admin tools abused, invisible to signature antivirus.
- **Silence.** The average intrusion goes unnoticed until the damage is already commercial.

Source: Huntress 2026 Cyber Threat Report — a 12-month analysis of proprietary telemetry from more than 4.6 million endpoints and 9.4 million identities across 230,000+ protected organisations worldwide.

ANATOMY OF A TYPICAL MID-MARKET INTRUSION

HOUR 0	HOUR 0–2	HUNTRESS ACTS	DAY 1–5	DAY 5+
Initial access	**Foothold**	**Detection & response**	**Escalation** (avoided)	**Impact** (avoided)
Phished credential, AiTM session token or an access broker's stolen login.	Persistence planted; a trusted RMM agent quietly installed.	SOC investigates, isolates the host, disables the account and reports in plain English.	Privilege escalation and lateral movement across the domain.	Exfiltration, ransomware deployment, diverted payments, notification duties.

You don't need a bigger security team.
You need a SOC that never sleeps — and someone local to run it with you.

Exactly what Huntress and SecureCentral deliver together: enterprise-grade managed detection and response, priced for the mid-market, with regional deployment and first-line support in your time zone.

02

ONE PLATFORM · ONE DASHBOARD · ONE SOC

The Huntress Agentic Security Platform

A unified security fabric that weaves together telemetry from **endpoints, identities, logs and learners** — then puts a 24/7 expert-led SOC behind it. Deploy in minutes, see real threats, not noise.

OUTCOME 01

Endpoint Integrity

Uncover hidden footholds, neutralise attacks and keep operations running — without adding complexity.

OUTCOME 02

Identity Resilience

Stop account takeover and BEC in Microsoft 365 and Google Workspace before they disrupt the business.

OUTCOME 03

Operational Readiness

Evidence for auditors, insurers and boards — with log retention, reporting and human risk reduction.

ENDPOINT

Managed EDR

Complete endpoint detection and response — from the second a threat appears until it is eliminated. 24/7 continuous protection, investigation and remediation, handled for you.

- **Industry-leading MTTR · 5M+ endpoints**

IDENTITY

Managed ITDR

Identity is the new endpoint. Detects and resolves account takeover, business email compromise, unauthorised logins and session hijacking across Microsoft 365 and Google Workspace.

- **3-minute MTTR · 15M+ identities**

LOGS & COMPLIANCE

Managed SIEM

SIEM without the complexity or the bill shock. Smart filtering captures only security-relevant data, with long-term retention, search and reporting at a predictable price.

- **Fully managed by SOC experts**

HUMAN RISK

Managed SAT

Security awareness training people actually finish — episodic, threat-intel-driven content built by Emmy® Award-winning animators to build a genuine security culture.

- **98% learner completion rate**

POSTURE

Managed ISPM

Most attackers don't break in — they walk through messy settings and over-privileged accounts. Continuously finds and closes misconfigurations and policy drift in Microsoft 365.

- **Drift fixed in ~15 minutes**

POSTURE EARLY ACCESS

Managed ESPM

Proactive endpoint hardening against ransomware and infostealers. Visibility and control over configurations, applications and vulnerabilities in one place.

- **Shrink the attack surface**

DEPLOYMENT & COVERAGE

TIME TO VALUE

Minutes, not months

Lightweight agent, no on-premise infrastructure and no rip-and-replace of your existing AV.

OPERATING SYSTEMS

Windows · macOS · Linux

Consistent managed detection and response across a mixed regional endpoint fleet.

CLOUD & IDENTITY

Microsoft 365 · Google Workspace

Tenant-level identity and email protection connected in a few clicks.

ECOSYSTEM

RMM, PSA & ticketing

Integrates with the tools your MSP or internal IT team already runs day to day.

24/7
AI-CENTRIC SOC

Real analysts. Machine speed.

Huntress pairs **Athena**, its agentic AI analyst, with human threat hunters. AI handles the heavy lifting — correlation, timelines, log review — while seasoned analysts own the novel tradecraft and the judgement calls. You receive plain-English incident reports a tier-one technician can act on, not a queue of raw alerts. **No AI surcharge. No separate SKU.**

03

SOLUTIONS BUILT AROUND OUTCOMES, NOT LICENCES

What changes in the first 90 days

- **Detect threats faster.** Suspicious activity is identified and investigated before it escalates.
- **Respond, don't just alert.** Security experts investigate and act when a genuine threat is confirmed.
- **Close the gaps.** Coverage across endpoints, identities, email and Microsoft 365 in one platform.
- **Extend your team.** Managed security expertise without recruiting or building an in-house SOC.
- **Improve resilience.** Reduce the blast radius of ransomware and account compromise.
- **Simplify the stack.** Consolidate point tools into one managed, accountable approach.

WHO IT IS BUILT FOR

Small & Medium Business

Enterprise-grade protection without the cost of a large internal security team.

Managed Service Providers

Add a credible managed security line to your existing IT services portfolio.

Internal IT Teams

Extend your capability with 24/7 monitoring, investigation and expertise.

Microsoft 365 Estates

A dedicated layer around users, identities and cloud productivity.

SUPPORTING YOUR REGULATORY OBLIGATIONS ACROSS SOUTHEAST ASIA

MARKET	KEY OBLIGATIONS	HOW HUNTRESS HELPS
Singapore	PDPA · CSA Cyber Essentials & Cyber Trust · MAS TRM (FI supply chain)	24/7 monitoring, incident response evidence, endpoint & account protection, staff training records
Malaysia	PDPA 2010 (as amended) · Cyber Security Act 2024 for NCII entities	Continuous detection, breach-notification-ready incident reporting, log retention
Indonesia	PDP Law No. 27/2022 · OJK requirements for financial services	Identity threat detection, documented response timelines, security awareness programme
Thailand	PDPA B.E. 2562 · Cybersecurity Act B.E. 2562	Appropriate technical measures, monitoring and audit-ready reporting
Philippines	Data Privacy Act of 2012 · NPC breach notification rules	Rapid detection and forensic detail to support 72-hour notification duties
Vietnam	Decree 13/2023 on personal data protection · Cybersecurity Law	Access monitoring, protective controls and evidence of due diligence
Australia / NZ	Privacy Act & Notifiable Data Breaches · ASD Essential Eight · NZISM	Maturity uplift across monitoring, hardening, MFA assurance and user education

Indicative guidance only. Regulatory alignment depends on your scope, sector and implementation — SecureCentral can map Huntress capabilities to your specific obligations as part of a cyber risk assessment. This is not legal advice.

> **"Huntress combines cutting-edge technology with human expertise in a way no other solution does. It's reliable, cost-effective, and invaluable for any organisation looking to strengthen their cyber defences."**
>
> **Kevin Walker** · Founder, Black Swan Cyber Security Solutions — published Huntress customer review

04

WHY SOURCE HUNTRESS THROUGH SECURECENTRAL

Global technology. Regional accountability.

A licence is easy to buy. Getting value from it in Jakarta, Kuala Lumpur or Ho Chi Minh City is another matter. SecureCentral operates the full distribution lifecycle — market entry, pre-sales architecture, deployment and regional support — so Huntress works the way it should in your environment.

12+
Years of APAC distribution experience

8
Markets served across Asia Pacific

17+
Years of managed IT heritage since 2008

50+
Years combined team experience

Solution consulting
Certified pre-sales architects who scope, demonstrate and prove the solution alongside your team — not a quote and a PDF.

Managed support in your time zone
Regional first- and second-line support during SEA business hours, escalating to the vendor only when genuinely needed.

Marketing & demand generation
Co-branded campaigns, localised collateral and lead generation that resellers can run out of the box.

Channel & market development
We recruit, contract and activate the right reseller network in each country — with local commercial terms.

HOW WE GET YOU PROTECTED

1 **Discovery & risk review**
We map your environment, identity estate and regulatory exposure.

2 **Proof of value**
A time-boxed trial on real endpoints and tenants. You see actual findings.

3 **Deploy & tune**
Rollout, integration with your RMM/PSA, and policy tuning by our engineers.

4 **Managed run**
Ongoing support, reporting and periodic reviews with your team.

FOR MSPS & RESELLERS

Build a managed security line, not just a resale margin

Huntress was designed for outsourced IT. SecureCentral adds the regional layer — commercial terms in your market, enablement for your engineers, and campaigns your sales team can actually run.

WHAT YOU GET

- Multi-tenant management and per-client reporting
- Pre-sales architect support on your customer calls
- Co-branded collateral, campaigns and lead generation
- Regional first- and second-line escalation path

ONE PARTNER, ONE CONTRACT, ONE SUPPORT DESK

InvGate · ITSM & ITAM | **Scalefusion** · UEM | **SuperOps** · RMM & PSA | **Splashtop** · Remote support
Zimperium · Mobile security | **Fortinet** · Network security | **Cisco Meraki** · Networking | **HPE Aruba** · Wi-Fi
myCISO · Compliance | **Uila** · Observability

bsi ISO/IEC 27001 Information Security Management CERTIFIED

Backed by a certified, licensed security heritage

SecureCentral is a company of **Pioneer Infotech Singapore**, serving SME clients in banking, shipping, retail and logistics since 2008. Pioneer Infotech is **ISO/IEC 27001:2022 certified** and a Licensed Service Provider under Singapore's **Cybersecurity Services Regulation Office (CSRO)** for Managed SOC Monitoring (CS/SOC/C-2024-0407) and Penetration Testing (CS/PTS/C-2024-0522).

HUNTRESS

NEXT STEP

Find out what is already hiding in your environment.

Most organisations that run a Huntress trial find something. Let's start with a conversation about your environment, your obligations and your risk — then prove it on your own endpoints and Microsoft 365 tenant.

01

Book a discovery call

A 30-minute technical conversation with a SecureCentral solution architect — no obligation.

02

Request a proof of value

Deploy Huntress on a representative slice of your estate and review the real findings together.

03

Become a reseller or MSP partner

Add managed security to your portfolio with regional enablement, margin and marketing support.

TALK TO SECURECENTRAL

EMAIL
info@securecentral.net

WEB
www.securecentral.net

PHONE / WHATSAPP
+61 424 135 693

MARKETS SERVED

Singapore · Malaysia · Indonesia · Thailand · Philippines · Vietnam · Australia · New Zealand

Singapore engineering and service heritage through Pioneer Infotech, with distribution operations across Australia and Southeast Asia. In-region technical support and local commercial terms available.

SCAN OR CLICK

See the full Huntress solution page

Capability detail, use cases and enquiry form at **securecentral.net/huntress** — or reply to the email this brochure arrived in and we will arrange a time.

SECURE CENTRAL
A Pioneer Infotech Company