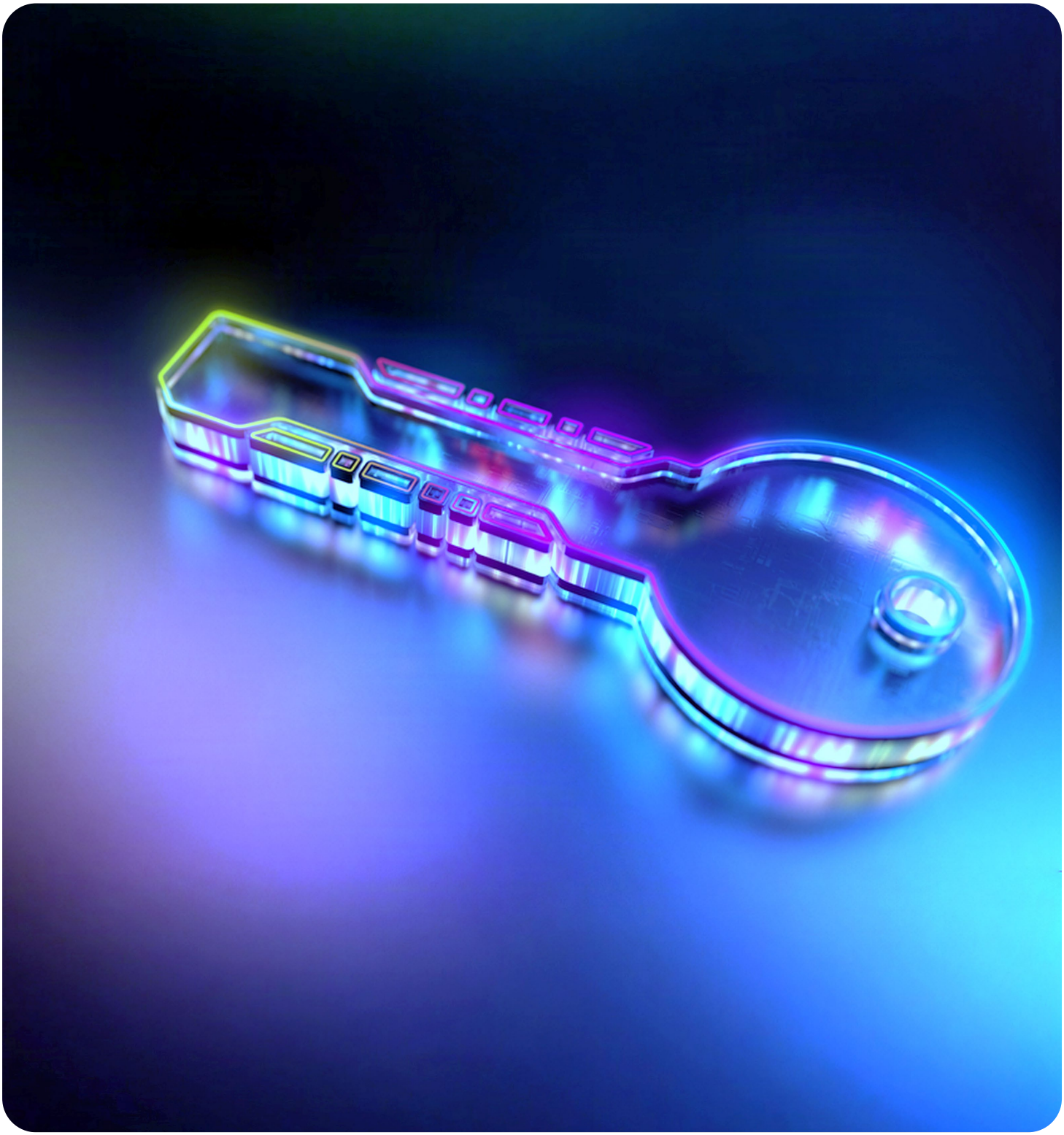
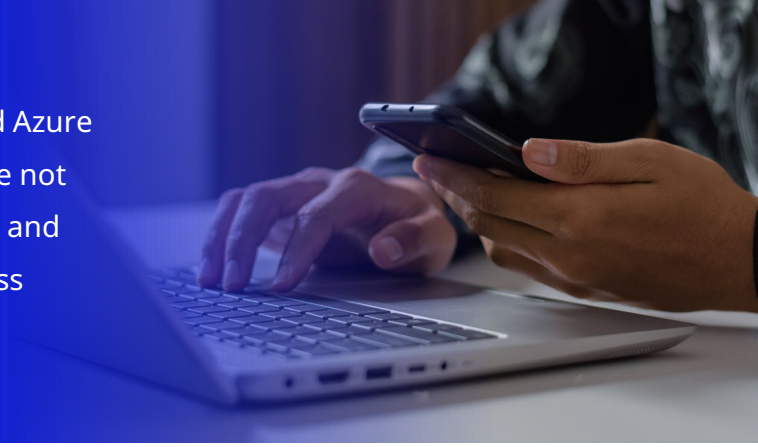


NEC Cyber Defence Services

Build resilient cyber defences with intelligent, 24/7 protection

NEC \Orchestrating a brighter world

Many organisations already invest in Microsoft 365 and Azure security technologies. However, security tools alone are not enough. Threats continue to evolve, alerts accumulate, and critical warning signs can be overlooked before business operations are affected.



NEC Cyber Defence Services

NEC helps organisations strengthen their security posture through continuous monitoring, threat investigation, and response support. Combining Microsoft-native security technologies with experienced cybersecurity specialists, we help organisations identify suspicious activity earlier and respond with confidence.

Why Early Detection Matters

Most cyber incidents do not begin with sophisticated attacks.

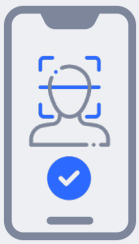
A routine email is opened. Credentials are compromised. An attacker gains access and begins moving through the environment. By the time systems become unavailable or operations are disrupted, the incident may already have escalated significantly.

NEC Cyber Defence Services help organisations increase visibility across the attack lifecycle and identify suspicious activity before it develops into a larger business disruption.

Our Approach

Monitor

- Continuous security monitoring
- Alert review and triage
- Threat visibility



Investigate

- Threat analysis
- Activity correlation
- Risk assessment

Respond

- Incident support
- Escalation management
- Remediation guidance

Improve

- Security recommendations
- Operational insights
- Continuous enhancement

Key Capabilities

24/7 Security Monitoring

- Continuous monitoring of security events and alerts
- Early detection of suspicious activities
- Escalation and investigation support

Threat Detection & Investigation

- Identification of potential threats
- Correlation of security signals
- Rapid incident assessment

Incident Response Support

- Investigation and containment guidance
- Security event analysis
- Coordinated response workflows

Actionable Security Insights

- Prioritised recommendations
- Operational visibility
- Risk-informed decision support

Microsoft-Native Security

- Leverages existing Microsoft security investments
- Integrates with Microsoft 365 security ecosystem
- Enhances existing capabilities

Local Cybersecurity Expertise

- Regional support teams
- Experienced security analysts
- Business-aligned engagement

Ideal Use Cases

Mid-Market Enterprises

Organisations running Microsoft 365 and Azure that want managed SOC coverage without setting up an in-house team.

Security Leaders Without an SOC Team

CISOs or IT directors who own the security mandate but need an operational partner for round-the-clock coverage.

Small SOC Teams Needing Surge Capacity

In-house SOC team leaders who want a partner for after-hours, weekends, or specialised detection development.

Why NEC

Local Support

Dedicated analysts based in Singapore provide monitoring and support aligned to local business hours and regulatory requirements.

Microsoft Ecosystem Expertise

Existing Microsoft 365 and Azure security investments are extended rather than replaced, maximising the value already committed.

Operational Clarity

Service coverage, escalation procedures and support responsibilities are defined and agreed before the engagement begins.

Strengthen Your Cyber Defence Capabilities

Talk to our team about a security posture review.

SINGAPORE
NEC Asia Pacific Pte Ltd
(Regional Headquarters)
sg.nec.com

Scan the QR code for more information on our solutions and products.

NEC \Orchestrating a brighter world