DEFEND

Dicker Data NZ – Partner Enablement

DEFEND Guardian XDR for Business

Who are DEFEND

Committed to ensuring that every dollar invested in cybersecurity provides the most effective and measurable return

- New Zealand owned and operated
- Award winners in our field
- Pure play cybersecurity service provider
- Microsoft focused
- Nationwide coverage
- Customer focused across the full range of cybersecurity outcomes

Microsoft
Solutions Partner
Security

Specialist
Cloud Security
Identity and Access Management
Data Security
Threat Protection

Microsoft
Microsoft Partner
Winner
2025 Partner of the Year
Security Award

Member of
Microsoft Intelligent Security Association
Microsoft Security
Microsoft Verified Managed XDR Solution

DEFEND Operations

World-Class Expertise. Regional Insight.

Operations Team
50+ FTE

NATIONAL NETWORK OF CYBERSECURITY EXPERTS

655
Microsoft Certs

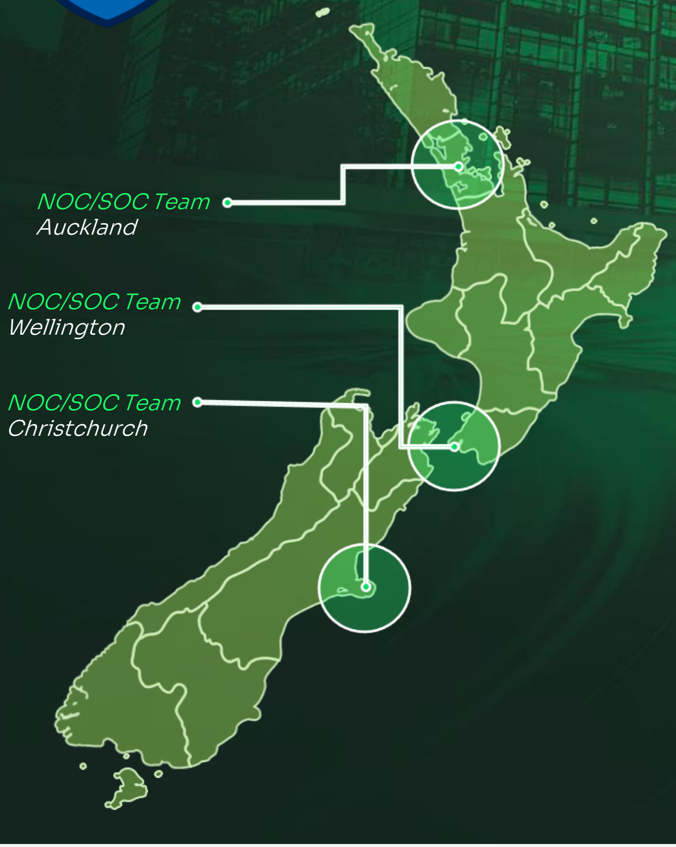
121
Microsoft Exams

Microsoft Intelligent Security Association

Microsoft

Microsoft Verified Managed XDR Solution

Microsoft CERTIFIED EXPERT



Strategic Partners

- Microsoft
- One NZ
- NZ NCSC
- Palo Alto Networks
- Zscaler

- ISO 27001 Certified
- ISO 27701 Certified
- SOC2 Type II Accredited

DEFEND Guardian XDR for Business Value Proposition

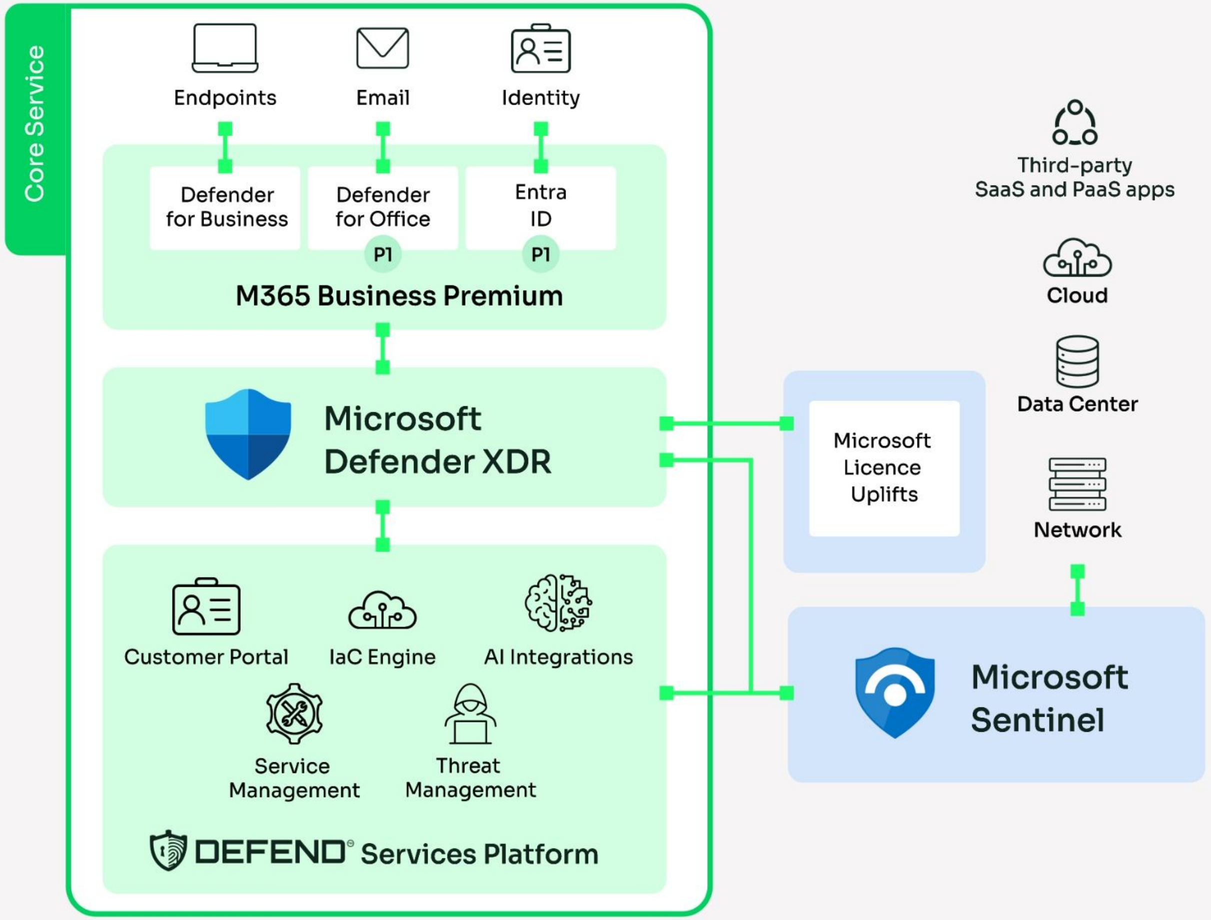
Comprehensive Security. Local Expertise. Transparent Delivery

24/7 Response	• 24/7 automated response backed by DEFEND's SOC team for manual intervention, escalation, and support
Local Expertise	• Delivered by local, capable, and accessible staff
Team Extension	• Complements Partner and Customer IT teams
Microsoft Value	• Leverages existing customer investments in Microsoft security capability
NZ Threat Intel	• NZ-specific threat intel from the NCSC (MFN & PDS) integrated to protect against threats specifically targeting NZ businesses
Data Residency	• Customer data stays in the customer environment
Transparent Ops	• Transparent to customer (and partner if approved by customer)

Solution Components

Delivering Cyber Resilience, Value, and Expertise - backed by Service Excellence

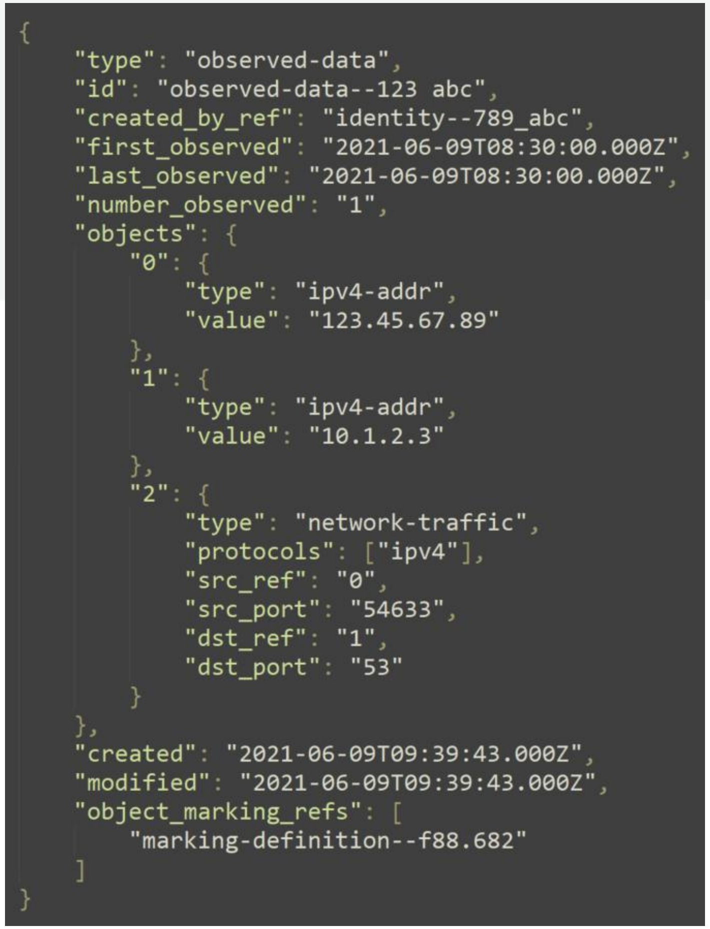
- **Security Event Monitoring**
- **Security Event Triage and Analysis**
- **Security Incident Response and Remediation**
- **Threat Detection Optimisation & Alert Tuning**
- **MFN and PDS Threat Protection**
- **Continuous Improvement**
- **Reporting & Meetings**



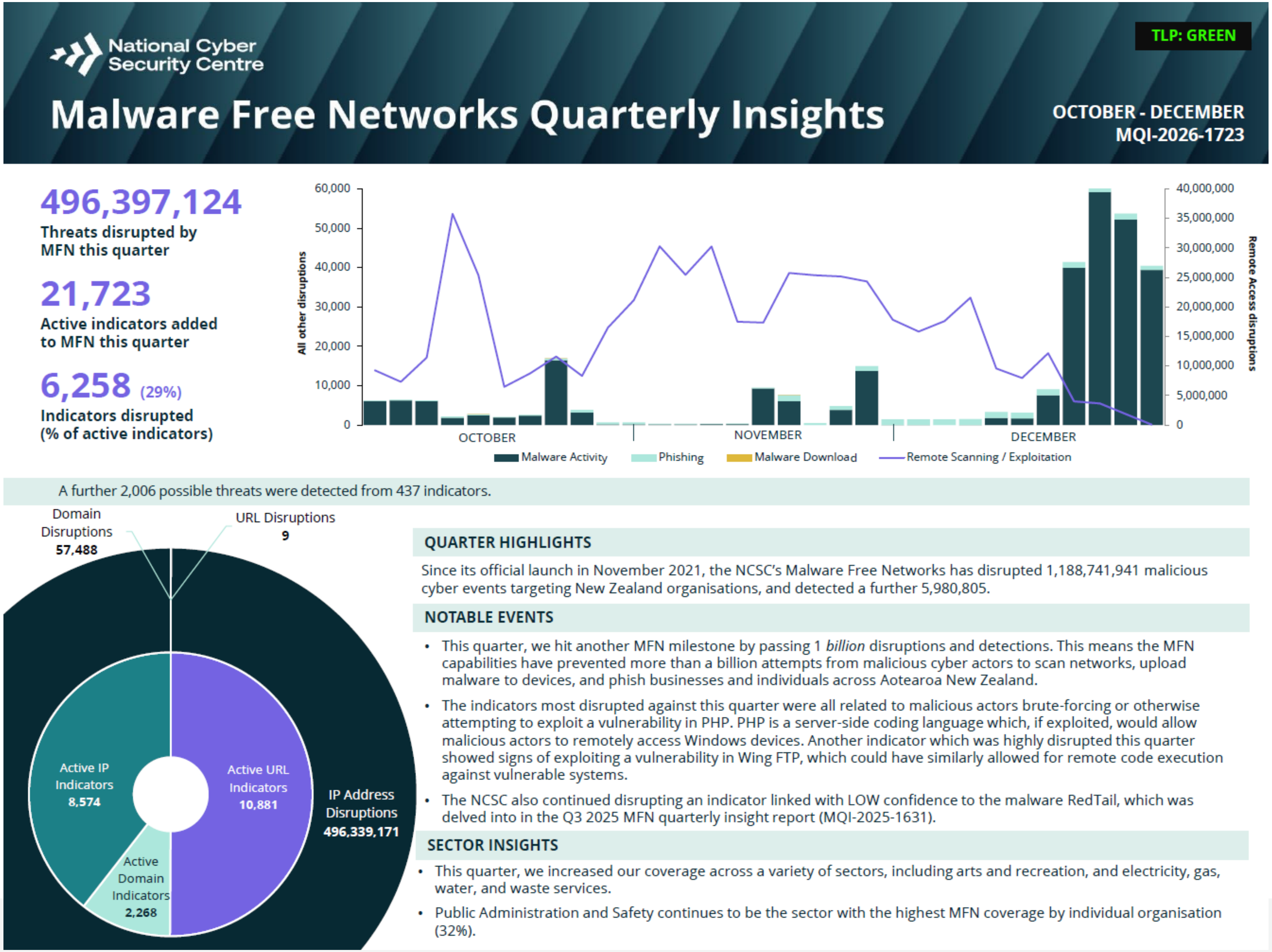
SHERLOCK Threat Intelligence

*Enhance your existing security solutions to **disrupt threat actors actively targeting NZ organisations**.*

Threat Feeds	• NCSC's MFN (Malware Free Networks) – Indicators associated with threats against critical infrastructure • NCSC's PDS (Phishing Disruption Service) – Indicators associated with phishing
Indicators	• IP (network) addresses, domain names, URLs
Integrations	• Sentinel SIEM • Defender for Business & Endpoint • Network infrastructure (Fortinet, Palo Alto, Zscaler) *Separate paid service
Telemetry	• Return telemetry to the NCSC of detected indicator metadata



```
{
    "type": "observed-data",
    "id": "observed-data--123 abc",
    "created_by_ref": "identity--789_abc",
    "first_observed": "2021-06-09T08:30:00.000Z",
    "last_observed": "2021-06-09T08:30:00.000Z",
    "number_observed": "1",
    "objects": {
        "0": {
            "type": "ipv4-addr",
            "value": "123.45.67.89"
        },
        "1": {
            "type": "ipv4-addr",
            "value": "10.1.2.3"
        },
        "2": {
            "type": "network-traffic",
            "protocols": ["ipv4"],
            "src_ref": "0",
            "src_port": "54633",
            "dst_ref": "1",
            "dst_port": "53"
        }
    },
    "created": "2021-06-09T09:39:43.000Z",
    "modified": "2021-06-09T09:39:43.000Z",
    "object_marking_refs": [
        "marking-definition--f88.682"
    ]
}
```



National Cyber Security Centre

TLP: GREEN

Malware Free Networks Quarterly Insights

OCTOBER - DECEMBER
MQI-2026-1723

496,397,124
Threats disrupted by MFN this quarter

21,723
Active indicators added to MFN this quarter

6,258 (29%)
Indicators disrupted (% of active indicators)

A further 2,006 possible threats were detected from 437 indicators.

QUARTER HIGHLIGHTS

Since its official launch in November 2021, the NCSC's Malware Free Networks has disrupted 1,188,741,941 malicious cyber events targeting New Zealand organisations, and detected a further 5,980,805.

NOTABLE EVENTS

- This quarter, we hit another MFN milestone by passing 1 *billion* disruptions and detections. This means the MFN capabilities have prevented more than a billion attempts from malicious cyber actors to scan networks, upload malware to devices, and phish businesses and individuals across Aotearoa New Zealand.
- The indicators most disrupted against this quarter were all related to malicious actors brute-forcing or otherwise attempting to exploit a vulnerability in PHP. PHP is a server-side coding language which, if exploited, would allow malicious actors to remotely access Windows devices. Another indicator which was highly disrupted this quarter showed signs of exploiting a vulnerability in Wing FTP, which could have similarly allowed for remote code execution against vulnerable systems.
- The NCSC also continued disrupting an indicator linked with LOW confidence to the malware RedTail, which was delved into in the Q3 2025 MFN quarterly insight report (MQI-2025-1631).

SECTOR INSIGHTS

- This quarter, we increased our coverage across a variety of sectors, including arts and recreation, and electricity, gas, water, and waste services.
- Public Administration and Safety continues to be the sector with the highest MFN coverage by individual organisation (32%).

Threat Coverage

Protect, Detect, & Respond against common threats to your organisation using Microsoft capability

Coverage Component	**Guardian XDR for Business**	***Guardian XDR for Business Plus*** ***(roadmap service)***	**Guardian XDR for Enterprise**
Email	Defender for Office	*Defender for Office*	Defender for Office + Custom Email Security Platforms
Cloud Identity	Entra ID + Entra Logs	*Entra ID + Entra Logs*	Entra ID + Entra Logs + Custom Identity Platforms
On-Prem Identity (AD)	–	*Defender for Identity*	Defender for Identity + Custom Log Sources for AD/Infrastructure
Endpoint (User Devices)	Defender for Business/Endpoint	*Defender for Business/Endpoint*	Defender for Business/Endpoint + Custom EDR
Server	Defender for Business/Endpoint (Server licensing required)	*Defender for Business/Endpoint (Server licensing required)*	Defender for Server - Extended server coverage + custom server log integrations (AMA)
SaaS / Cloud Applications	– Risky App Detection *	*Defender for Cloud Apps* **	Defender for Cloud Apps + Custom SaaS Log Ingest
Cloud Workload (Azure / Multicloud)	–	*Defender for Cloud - CWPP*	Defender for Cloud - CWPP + Custom Cloud Log Sources
Custom Log Sources incl. Network Infrastructure	–	–	As agreed, and aligned to identified threats

** Risky App Detection scoped to Cloud App Security feature limitations*

** *Note: Data exfiltration controls are treated here as detection/response in cloud apps (alerts, governance, session controls). Formal data protection & compliance (DLP/IRM etc.) remain out of scope*

Service Features

Service Levels That Scale With You

Service Component	Guardian XDR for Business and Business Plus	Guardian XDR for Enterprise
24x7 Security Operations	Included	Included
Security Incident Monitoring, Detection and Response	All events triaged and responded to automatically 24x7 with critical exceptions requiring manual intervention.	High and Medium severity events triaged automatically and analysed manually 24x7.
Threat Hunting	Not Included	Included
Microsoft Defender Threat Detection Optimisation and Alert Tuning	Included (Standard only)	Included (Standard and Customised)
Continuous Improvement	Included (Regular standard updates only)	Included (Regular standard updates and customised improvements as identified)
Assistance for Major Security Incidents	Incident Response Assistance (T&M)	Advanced Incident Response, integrated into customer MIM process (T&M)
Reporting	Monthly	Weekly and Monthly
Meetings	Quarterly	Fortnightly
Incident Response Retainer	Included: 2 Hours per incident then T&M	Included: 2 Hours per incident then T&M
Service Requests	T&M Only	Included (Fair Use applies)
Threat Intelligence	Bundled - Critical Threat Protection (Sentinel and MDfB/MDE) only	Optional - Critical Threat Protection (Sentinel and MDE) plus optional Extended Threat Protection (Firewalls, Zscaler, Prisma Access)

Customer Pre-requisites & Requirements

Environment configuration settings and licensing

Requirement	Description
Environment Licensing	- Microsoft 365 for Business Premium (minimum license requirement)
Azure Subscription	- Provision of an empty Azure subscription to contain Sentinel and related solution components
Defender Deployment	- Defender for Business/Endpoint deployed on all endpoints
Defender Configuration	- Defender for Business/Endpoint Policies - Windows - Remediation action for High severity threats set to Block - Windows - Remediation action for Severe threats set to Block - Windows - Remediation action for Moderate severity threats set to Quarantine - Windows - Remediation action for Low severity threats set to Clean
MFN Telemetry Agreement	- Acceptance of the MFN Telemetry agreement to enable provision of SHERLOCK Threat Protection
Provisioned Access	- Access provided for our operations team and Enterprise application as per the Access Requirements guide

Pricing & Costs

Service price and direct Microsoft costs

Component	Description
Guardian XDR for Business MDR Service	• Priced per user (or server) per month • RRP: $22.50 • Minimum 50 users • Maximum 300 users (aligned to M365 Business Premium limits) • Quarterly user count true-up/adjustment
Microsoft Infrastructure & Consumption Costs	• Paid directly to the customer's Microsoft CSP • Covers Sentinel, Data Lake (if enabled) and associated automations • Variable, based on consumption but expect: • 50 Seats ~ $100/month • 300 Seats ~ $200/month
Log Retention	• Microsoft charges based on standard 30 (Defender XDR) and 90 (Sentinel) day retention. • Extended retention in Sentinel Data Lake can be enabled as a standard MAC. • Allow for up to a 50% increase in Microsoft costs if retention extended to 12 months.

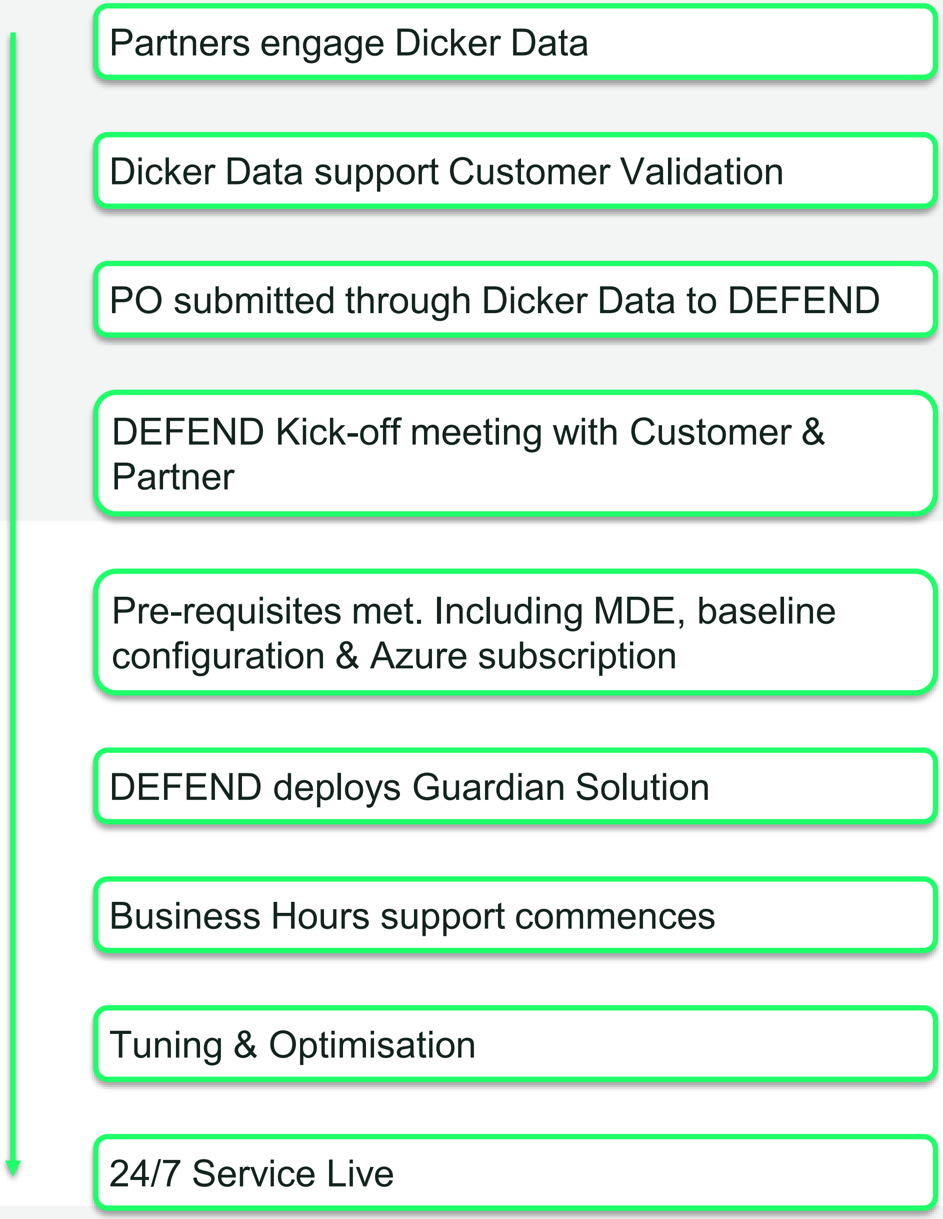
Collateral Guide

Documents and agreements for review and approval

Document	Description
NDA	- Signed by partner and by customer (separate documents) - required prior to service engagement
MFN Consent Agreement	- Signed by customer – required prior to service start to enable MFN & PDS integration
Customer Agreement	- Signed by customer – required prior to service deployment. Contains service details
Customer Contact Form	- Completed by customer – required prior to service go-live. Details escalation and approvals
Datasheet	- High-level service overview and summary
Quick Reference Guide	- Operational guide for customer teams to refer to during service delivery
Access Requirements	- Technical document specifying activities to be performed by customer (partner) to enable DEFEND to deploy and configure service components

Onboarding Process

- Onboarding takes 3-4 weeks from PO submission
- DEFEND will arrange Kick-off meeting once PO is received



Partners engage Dicker Data

Dicker Data support Customer Validation

PO submitted through Dicker Data to DEFEND

DEFEND Kick-off meeting with Customer & Partner

Pre-requisites met. Including MDE, baseline configuration & Azure subscription

DEFEND deploys Guardian Solution

Business Hours support commences

Tuning & Optimisation

24/7 Service Live

Other Services

1.

Assess

We provide an outside in view on cybersecurity effectiveness and maturity. We align these assessments with international industry standard frameworks such as NIST CSF, ISO27001, and can assess compliance with PCI-DSS, SOC2, and GDPR requirements.

2.

Advise

We enhance your cybersecurity function with our skilled specialists. We fast track our clients by providing advice, IP, and proactive thought leadership.

We advise on Governance, Risk, Policy, Incident Management, Information Management, and Compliance. We provide strategy leadership and architectural advice.

3.

Transform

We are experts in securing your network, cloud, modern desktop, and application development.

Our delivery teams have deep expertise across the cybersecurity ecosystems of Palo Alto Networks and Microsoft. We deliver user awareness training to companies – board, executives, and general staff.

4.

Operate

Our DEFEND Network and Security Operations teams provide 24×7 Measuring, Monitoring and Management of your entire environment to enable your organisation to profile effective controls that secure your business.

5.

Assure

We provide on-going measurement of cybersecurity effectiveness and maturity.

We provide on-going attendance of steering committees as independent advisors.

We provide vulnerability and penetration testing through our Professional Services team.

Sales/Pre-sales Support

More information can be found at https://www.dickerdata.co.nz/managed-security