

## Telstra Cyber Detection and Response - Endpoint Feature Comparison Table

Phase	Activity	Telstra CDR – Endpoint	TrustWave	Rapid7	Secureworks	CrowdStrike Falcon Complete	FireEye	CheckPoint SandBlast
Endpoint Support								
	Defender for Endpoint	$\subseteq$	$\subseteq$		$\subseteq$		$\subseteq$	
Microsoft Support	MISA Membership	$\subseteq$						
	Microsoft Gold Partner for Security	$\subseteq$						
Detection/ Investigate	Automated Triage	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	
	Full Alert Investigations	$\overline{\mathbf{Y}}$		$\square$			$\square$	
	Automated Response	$\subseteq$	$\square$	$\square$	$\square$	$\square$		$\subseteq$
	Full Remediation and Eradication of Threats	$\subseteq$	$\subseteq$		$\subseteq$	$\subseteq$		
	Active Threat Hunting	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	
	Proactive Threat Hunting	$\subseteq$		$\subseteq$			$\subseteq$	
	Custom Policy Development	$\subseteq$			$\subseteq$	$\subseteq$		$\square$
	Customized Security By Asset Class	$\square$			$\subseteq$			
	Unlimited Remote Incident Response	$\subseteq$			$\subseteq$	$\overline{\checkmark}$	$\overline{\checkmark}$	
	Remote Root Cause Analysis	$\overline{\checkmark}$		$\subseteq$		$\overline{\subseteq}$		
	Continuous Security Alert Monitoring	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\overline{\lor}$	$\subseteq$
	Security Alert Triage and Prioritization	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\overline{\checkmark}$	$\subseteq$	$\square$
Respond	Guided Response	$\overline{\checkmark}$	$\subseteq$		$\subseteq$	$\subseteq$	$\subseteq$	$\overline{\searrow}$
	Managed Remediation: Isolate Endpoint	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\square$
	Managed Remediation: Eliminate Persistent Threats	$\subseteq$		$\subseteq$	$\subseteq$	$\subseteq$		
	Managed Remediation: Remove Artifacts Endpoint	$\subseteq$	$\subseteq$	$\overline{\mathbf{Y}}$	$\overline{\checkmark}$	$\subseteq$	$\subseteq$	
	Managed Remediation: Eradicate Threat without business impact	$\subseteq$				$\subseteq$		
	Managed Remediation: Tune Policies Endpoint	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\overline{\checkmark}$	$\overline{\subseteq}$	$\subseteq$
	Managed Remediation: Automated and or Human action taken on client technology outside Endpoint (e.g. disable account, block IP, quarantine, etc.)	¥			$\subseteq$			
	Sample acquisition & Malware Analysis	$\subseteq$		$\subseteq$	$\subseteq$	$\subseteq$	$\overline{\mathbf{Y}}$	$\subseteq$
	Incident Response Retainer	$\subseteq$				$\subseteq$	$\overline{\mathbf{Y}}$	
Recover	Implement improvements based on security incidents	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\leq$	$\overline{\checkmark}$	$\subseteq$
	Continuous Improvement led by Technical Account Manager	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\leq$	$\subseteq$	$\subseteq$

Phase	Activity	Telstra CDR – Endpoint	TrustWave	Rapid7	Secureworks	CrowdStrike Falcon Complete	FireEye	CheckPoint SandBlast
Recover	Incident Response Coordination	$\subseteq$			$\subseteq$	$\subseteq$	$\subseteq$	
Customer Experience	Onboarding	$\subseteq$	$\subseteq$	$\overline{\mathbf{Y}}$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$
	Quarterly Executive Briefings	$\subseteq$	$\subseteq$	$\overline{\mathbf{Y}}$	$\subseteq$	$\subseteq$	$\overline{\mathbf{Y}}$	$\subseteq$
	Staffing to Specific Client Needs							
	Proactive Check-Ins with Client Success Manager	$\subseteq$						
	Defined SLAs with Full Reporting							
	Tailored Reports and Briefings	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$
	Transparent View in to Analyst Activities via Rich Client Portal Experience with Solution Specific Dashboards, Metrics and Reports	$\subseteq$		$\leq$		$\subseteq$		
Managed Technology	Custom Solution Design and Technology Implementation	$\subseteq$						
	Proactive Tuning	$\subseteq$		$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	
	Release Management (software upgrades, patches, agent updates)	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$oxed{oxed}$
	Configuration Backups	$\subseteq$	$\subseteq$	$\overline{\checkmark}$	$\overline{V}$	$\overline{\mathbf{Y}}$	$\overline{\checkmark}$	$\subseteq$
Threat Intelligence	Integrated Threat Intellligence	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$
	Daily, Weekly, Monthly and Advisory Intelligence Publications	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	
	Threat Detection in the wild powered by exclusive use of the world's largest internet traffic metadata set	$\subseteq$						
Additional Features	Custom Use Cases	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	$\subseteq$	
	Customized Automation and Response Use Cases	$\subseteq$				$\overline{\checkmark}$		
	Client access to technology	$\subseteq$				$\subseteq$		
	Alerts Enhanced, Correlated and Prioritized with Business Context and Log Source Variation	$\subseteq$		$\subseteq$				
Data	Event and Alert data collected	$\subseteq$				$\subseteq$		
	Event and Alert data stored and archived for up to 365 days	$\subseteq$						

Contact your Telstra account representative for more details.