Version Control

When any part of this document is amended, a record is made in the Amendment Log shown below.

**To add a new version, please insert a row below, drag the 'version' document property down to your new row and enter your new version. Make sure you refill the issue number in the row above with the previous version number.*

Issue	Issue Date	Additions/Alterations	Initials
1	22/01/2025	Final Draft	TO

Trust Cloud Service

Lot1

January 2026

Contents

Executive Summary

The following document outlines a “Trust Cloud Hosting” Infrastructure as a Service (IaaS) for a hosting customer workload, including development, testing and production systems. The service comprises a complete infrastructure with an accompanying base managed service platform delivered by Trust Cloud. The service is designed to provide customers with a complete base infrastructure solution without them having to invest in the technology, the management platforms, services and personnel associated with traditional IT IaaS solutions – allowing customers to focus on their business targets.

The service is an Infrastructure as a Service offering, based on a shared network solution, with customers utilising one of three pre-sized Hyper-Converged Platforms.

Additional “Trust Cloud Managed Services” are available to provide:

1. Professional Services for Planning, Set-up and Migration, Security Services
2. Packaged Enhanced Silver and Gold Managed Services, for example Antivirus
3. Additional service options, here Trust will manage the elements of that service, including the technology and the operation of it, for example Managed Antivirus

Service Introduction

The holistic service is comprised of the following key elements:

- **Platform** = The productised offering, including all sub-elements/components required for delivery
  - **Managed Services**: The specific managed service element of the platform, sized based on a single theoretical workload
  - **Technical Solution:** The technical elements of the platform that directly comprise the customer systems access:
    - Hyper-Converged infrastructure – Dedicated Hyper-Converged, with customers choosing from one of three base levels
    - Secure Data Centre Hosting - all managed in Crown Hosting facilities
    - Network Infrastructure – Shared switch Platform (VRF/VXLAN)
    - Firewall infrastructure – Virtual, single firewall, Edge based landing (flexible for MPLS, SD-WAN, IPSec VPN, Nutanix Flow or DCI connectivity from customer) on shared hardware solution
  - **Management Platform**: The Management platform that supports the service for Trust to be able to operate
    - Management Compute and Platform
    - Management Network and Firewall

Service Summary

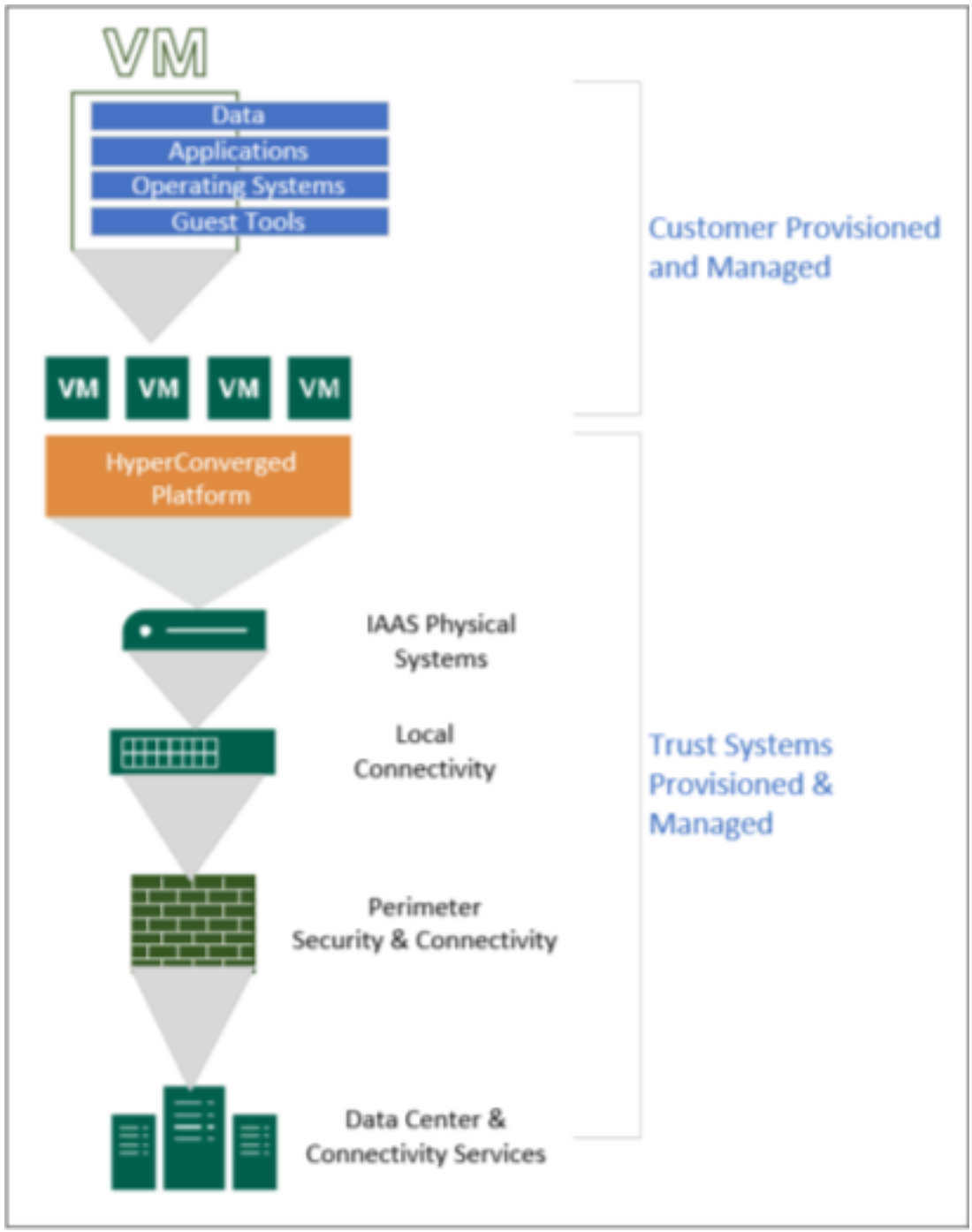
The Trust Cloud Hosting Service will consist of an Infrastructure as a Service (IaaS) offering to clients, using (dedicated, per customer) Hyper-Converged, (shared) Edge Landing,

intermediate/Core LAN (network) and (dedicated) perimeter security Firewall technologies. Additional options are included for specific features on a case-by-case basis.

This Hosting Service includes a Bronze base managed service. Enhanced Managed Services for Silver, or Gold levels are available, each with options delivered by either Trust of trusted third-party providers. These will include the optional services such as BaaS and DRaaS.

With multiple edge landing options available, Trust recommends using Nutanix Flow, however this may require a supported termination device at a customer location, or the ability to deploy a Nutanix virtual appliance to support connectivity.

The service is designed for customer management, but only from the ability to manage customer specific resources (networks, VMs, ISO, snapshots). Using the mandatory Bronze Managed service Trust manage all underlying components and configuration:



The service is a (customer) production ready, IaaS platform only, with a base operating model allowing for three sizes of customer solution:

Description	Platform Components

Dedicated IaaS Platform	1. Provision virtual machines on Windows or RHEL based on Bring your own licensing* or Trust CSP/ASP resell 2. Dedicated Hyperconverged (HCI) platform comprising a base tier with additional nodes if requirement exceeds the base tier provision 3. HCI Sized identified per needs of customer in presales engagement 4. Scalability in terms of growth based on demand; No scale down option is available 5. Single site provision of platform and customer VM's 6. Local snapshots of VM's, encryption of snapshots (as platform is encrypted), no 'off host backup' by default of snapshots (BaaS optional service provides this feature) 7. Encryption optional based on native HCI software with local key platform/management 8. Provisioned on Nutanix AHV, 9. Customers must provide (if only consuming platform with 'Bronze service'): a. VM OS update toolsets and updates b. VM OS update management (unless using Silver/Gold service) c. Anti-Virus must be provisioned by customer unless Silver/Gold Service options taken out, in which case the toolset and management is provided by Trust 10. Nutanix default security baselining (with auto-remediation) (SCMA) using Nutanix STIG is included in the platform operations
Shared management Self-service portal	1. Integration with customers AD, iDP, SAML, or other source for authentication 2. MFA based portal – Customer provided MFA or Trust Cloud can provision this 3. Either BYOL licenses or CSP/SPLA inclusion. Custom ISO's or VM images can be brought to the service for consumption with valid licenses 4. Limits defined on overall usage – CPU, RAM, Disk – utilisations at 85% for best practises 5. Trust managed capacity alerts to notify customer in case of expansion 6. Overview of usage based on provisioned resource for customer 7. Non-internet accessible SSP portal 8. Patched within 30 days for standard patches, every14 days for more critical patches (from patch release date)
Shared Perimeter landing	1. Default is resilient Edge Landing switches, using IP based landing on customer dedicated virtual firewall with

		bandwidth limited share of incoming Point of Presence connection 2. Dedicated virtual Firewall for site-to-site VPN, limitation to maximum 5Gbps throughput (no IPS, AV or other security scanning by default, but optional) 3. Dedicated virtual firewall in non-HA configuration with underlying system being HA 4. No additional IPS/Anti-virus or other features (Optional purchase and scope in performance) 5. Shared Edge landing switches, with VLAN separation and additionalsecurity features 6. Virtual Domain separation of customers on firewall 7. Firewall ruleset manages base Ingress/Egress traffic flow 8. Base set of rules based on “minimum trust” model 9. Firewall monitored for MDR/SIEM by Trust third-party (Alert Logic) 10. Patched within 30 days for standard patches, every 14 days for more critical patches (from patch release date) Impacting patching/operational outages communicated to customer via change management and Trust Service Delivery teams 11. Edge Firewalls based on FortiGate technologies, switches on Mellanox
Network Infrastructure		1. Shared switch stack, VRF segmentation 2. Based on Mellanox/NVIDIA technologies up to 100GbE 3. Trust provision and managed network configuration 4. Layer 3 Routing at switch level (firewall to provide base access management via policy set for egress/ingress traffic) 5. Patched within 30 days for standard patches, every 14 days for more critical patches (from patch release date) Impacting patching/operational outages communicated to customer via change management and Trust Service Delivery teams
Management Compute		1. Hyper-Converged platform 2. Separate Active Directory for management operations with default auditing via Windows Event logs and with Alert Logic MDR/SIEM service management 3. Windows based RDS for management, MFA via Duo for access 4. Windows based PKI platform (3 tier design) 5. Windows based NPS for RADIUS and other authentication 6. Windows Update services 7. Secured with NIST/DoD standard principles (i.e. Active Directory servers cannot access internet, secure

	web based NTP source, Domain Admin accounts renamed and locked until use (least Privilege)) 8. Least Privilege admin model with approvers for elevated permissions 9. Site to site VPN to connect from Trusts UK based, 24/7/365 central support offices 10. SSL based VPN for remote management with DUO 2FA for access 11. Hosted self-service application with load balanced publishing 12. Patched within 30 days for standard patches, every14 days for more critical patches (from patch release date) Patched within 30 days for standard patches, every 14 days for more critical patches (from patch release date)
Management Network Platform:	1. Technology based on Mellanox and Out of Band Management via OpenGear 2. VRF and VLAN design for management networks 3. Separated with firewalls from production platform, with out of band access 4. Patched within 30 days for standard patches, every 14 days for more critical patches (from patch release date)

IaaS Platform

The following platform tiers have been defined for a base customer purchase, with DRaaS being offered by purchase of a second cluster of the same size.

IaaS Platform
Small Nutanix Platform up to 75 Virtual machines (Theoretical Workload)
Bronze Managed Service (Default)
Silver and Gold Service Options
Based On Nutanix NX-NX-3060-G9 Cluster of 3 nodes

NX-3060-G9	
Model Type	All SSD
Chassis	NX-3060-G9
CPU Type	2 x Intel Xeon-Gold 5415+ processor (2.9 GHz/ 8-core/ 150W) (16 Cores)
RAM	8 x 64GB Memory Module (4800MHz DDR5 RDM)
SSD	6 x 3.84 TB SSD
HDD	N/A
NIC LOM (Onboard)	1 x 1GbE Dedicated IPMI
NIC LOM/AIOM (Add-on)	1 x LOM Module: Broadcom 10GbE, 2-port, Base-T NIC (BCM 57416)
NIC (Add-on)	None
GPU	None

Expansion Options:

- Expansion via additional compute nodes once 85% utilisation of a single resource at N+1 availability

Management Platform

The Management Platform will comprise the following elements/services, which although largely are transparent to the end customer, are key for platform operations.

Design Element	Consideration/Design Detail	Additional notes
Separate Platform for	Based on Nutanix AHV with secure FortiGate firewall and	

Hyper-Converged	Mellanox switch implementation	
Management Active Directory	Secured by GPO to NIST/DoD selected standards, based on Windows 2022. Domain controllers have no internet access except for items like NTP, and firewall policy managed	Will undergo Cyber Essentials + and accredited third-party penetration testing (bi-annual) using NESSA or similar ISA toolsets
Windows Update services	Dedicated and allowed internet access for SUS updates	All systems will be Windows based except for specific functions such as Load Balancer, updates occur automatically with approval by managed services team
Internal PKI/SSL Cert platform	Provides internal PKI SSL requirements by managing certificates for integrity	
External PKI provider for web services	Provided by GoDaddy, for customer and additionalexternal facing SSP provision (such as portal)	
Windows NPS Servers	Provide features such as Active Directory integrated authentication for devices	Additional logging and security provided by triple A logon approach
Load Balancer for SSP	Progress based virtual load balancer	Publishes SSP portal with SSL encryption, and WAF
Auditing and security	Managed Defence Response (MDR)and SIEM provided by Alert Logic for management platform	Additional penetration testing scheduled bi-annually
Windows RDS platform for service desk management	Provided with Duo 2FA integrating into management AD	Audited via MDR service

Optional Services

The following shows included available for Bronze included in Trust Cloud Hosing and optional encryption service. Also, the enhanced Silver or Gold levels available as part of the “Trust Cloud Managed Service Description”.

Features included in the Service	**BRONZE** (Included in Trust Cloud)	**SILVER** (Service Upgrade)	**GOLD** (Service Upgrade)
IaaS Platform Hosting, WAN Management	✓	✓	✓

IAAS platform Reporting	✓	✓	✓
IAAS platform Monitoring	✓	✓	✓
IAAS platform Service Mgmt.	✓	✓	✓
IAAS platform Service Desk	✓	✓	✓
IAAS platform Back end infra Mgmt.	✓	✓	✓
IAAS platform Firmware Mgmt.	✓	✓	✓
IAAS platform Break Fix Mgmt.	✓	✓	✓
Virtual Firewall MGMT.	✓	✓	✓
VM OS Mgmt. & AV	×	✓ For 25 VMs	✓ For 50 VMs
Backup - On box Snapshot	✓	✓	✓
SIEM MDR (Managed Detect and response)	×	×	O
Vulnerability Scan	×	×	✓
Encryption (Software)	✓	✓	✓
BAAS - Backup – Off host (HYCU)	×	O	O
DRAAS – DR as a Service	×	×	O
Web site publishing and load balancing	×	O	O
Web Application Firewalls - Security	×	O	O

O=Option

Solution Default Sizing

The Hyper-Converged Platform provides the following in terms of scalability and availability options.

Platform Size

The small platform is considered ‘entry’ level for smaller customers, offering the same core technologies and operational.

Bespoke IaaS Managed Cloud Requirements

To ensure Trust Cloud meets base requirements for varied customer service requirements outside G-Cloud specific services, a tailored and bespoke solution design and provision can be included in addition the above default, templated offerings.