

Amulet Hotkey

Delivering the six layers of an ultra-secure
remote working environment

Deliver ultra secure client devices and infrastructure for
remote working environments.

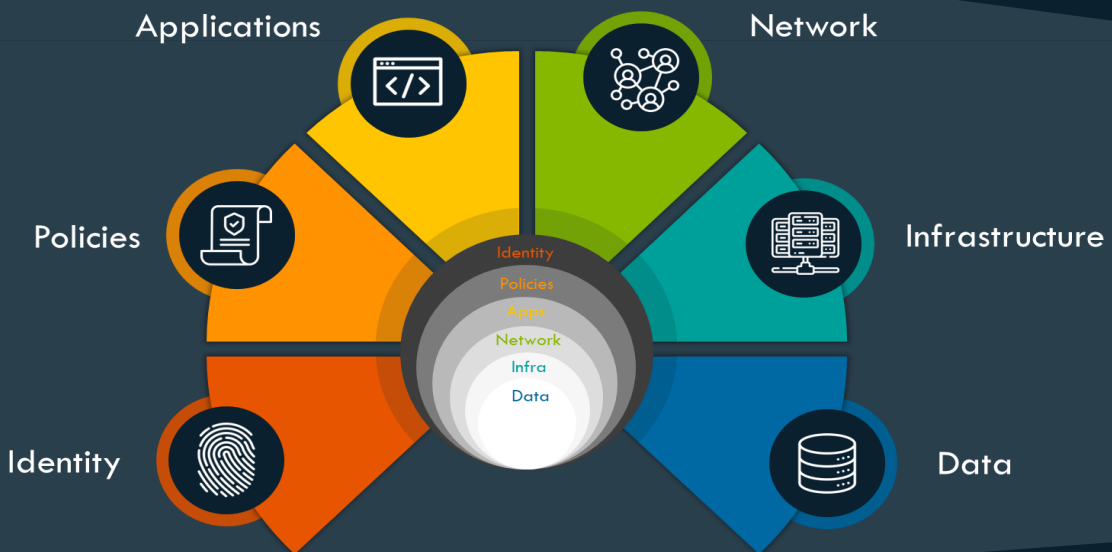
Designed by defense, for defense and beyond

Executive summary

Defense organizations operate in one of the most demanding security environments in the world. They face persistent cyber threats from nation-state actors, insider risks, supply-chain vulnerabilities, and the operational challenges of securing distributed, mission-critical systems.

To maintain readiness and protect sensitive information, defense agencies rely on a six-layer security model; a structured, defense-in-depth approach that ensures resilience even under sustained or sophisticated attack.

Six-layer security framework



Identity

The Identity Layer enforces multi-factor authentication (MFA) and considers risk factors for adaptive access control. Risk factors include location, device, and resource sensitivity.



Policy

Framework for defining rules, guidelines, and procedures protecting organizational assets. Enforces user responsibilities, aligns controls with password policies and access controls.



Applications

Application access control utilizes firewalls, web apps, and API protection. Used to filter app traffic, to prevent common web attacks (SQL injection, XSS), and enforce access restrictions.



Network

Network layer implements firewalls and intrusion Detection/Prevention systems (IDS/IPS) to enforce segmentation, block unauthorized traffic, and detect network-based attacks.



Infrastructure

Infrastructure includes vulnerability management. It prioritizes rigorous patch management and vulnerability scanning across servers, operating systems, firmware and applications.



Data

Data layer leverages encryption to protect sensitive data at rest and in transit. It implements data loss prevention (DLP) to monitor and prevent unauthorized data movement

Use case reference architecture

Amulet Hotkey solutions for defense are based on reference architectures that securely lock data away centrally, and then, based on the six-layer security model, enables users to access apps and data, independent of location, remotely, or even across different domains for true multi-agency collaboration.



Secure office

Replace traditional desktops with centrally managed thin clients to reduce attack surface and ensure the security of sensitive data with no local storage.



Field operations

Respond swiftly to field deployments by deploying thin client devices in the field without the need for infrastructure.



Cross-domain coalition

Enable Multi-agency collaboration securely with centrally managed desktops.

Secure Office



Domain #1 Hosting Infrastructure
Server-based hardware and software to support physical and virtual desktops and workstations



Management Infrastructure
Centralized management of thin client devices; delivering OS, patches, onboarding and deployment



Thin client devices deployed in field locations that use the internet to connect securely to desktop resources

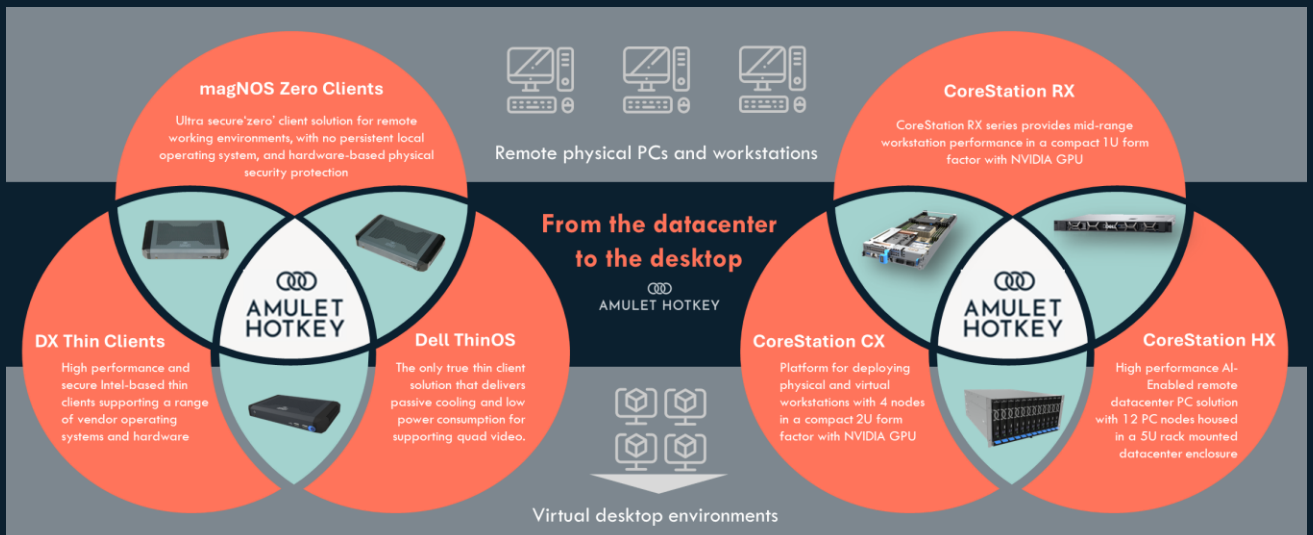
Field Operations



Domain #2 Hosting Infrastructure
Third-party agency server-based hardware and software to support physical and virtual desktops and workstations

Cross Domain

Amulet Hotkey defense portfolio



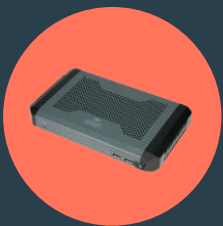
In summary

With 30 years of experience in deploying defense solutions, Amulet Hotkey solutions for defense are based on reference architectures that securely lock data away centrally, and then, based on the six-layer security model, enables users to access apps and data, location locally, remotely, or even across different domains for multi-agency collaboration.

By deploying Amulet Hotkey solutions, you can ensure the security of your data as it never leaves the secure confines of the data center. Traditional desktops are replaced with thin client devices that have low power requirements, passive cooling, and more importantly, have no local data storage, plus the addition of advanced security features to keep them protected even during shipping.

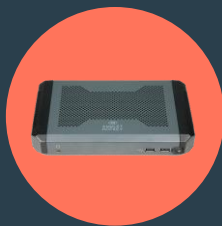
Find out more

To find out more about the range of Amulet Hotkey thin clients, or Amulet Hotkey AI-enabled PCs, workstations, and server solutions, all designed to deliver a complete end-to-end ultra-secure environment for high performance virtual desktop infrastructure, click the icons below:



DX Thin Clients

Versatile design to adapt to your remote access requirements. OS agnostic to run local apps and virtual desktops.



MagNOS Ultra-Secure Clients

The most secure client solution in the portfolio, designed by defense customers with zero local storage and no local OS.



Dell ThinOS Clients

Thin client solution (with passive cooling and low power consumption) that can support quad video outputs with Dell ThinOS.



CoreStation

Datacenter-class infrastructure to host virtual desktops and physical rack mounted AI PCs and workstations.

Alternatively, talk to us directly by phoning or emailing your local sales office listed below.

Contact Us

EMEA Sales

+44 (0) 20 7960 2400
emeasales@amulethotkey.com

N America Sales

+1 212 269 9300
ussales@amulethotkey.com

APJ Sales

+61 409 930 884
apsales@amulethotkey.com



www.amulethotkey.com

Six-layer security

Solution overview


AMULET HOTKEY