Dell Security Services for Cloud – High-Level Overview

1. Dell's Cloud Security & Resilience Vision

Dell delivers **security and resilience services** that span on-premises, private cloud, public cloud and SaaS, anchored in **Zero Trust principles**, strong **data protection**, and **modern incident response and recovery** capabilities.

Core ideas:

- **Zero Trust by design** – identity-centric controls, least privilege, micro-segmentation and continuous verification applied across endpoints, data center, and multicloud environments.
- **Shared responsibility in the cloud** – Dell services and platforms are built to complement hyperscaler controls (AWS, Azure, GCP) with additional layers for data protection, monitoring and recovery.
- **Cyber resilience over just 'security'** – emphasis on being able to **withstand, respond and recover** from attacks, including ransomware and cloud misconfigurations, not just blocking threats at the perimeter.

---

2. Advisory & Assessment Services for Cloud Security

Dell offers **consulting services** to assess cloud security posture, align with frameworks, and build roadmaps:

- **Advisory Services for Cybersecurity Readiness** – evaluates identity, data, endpoints, and **cloud workloads** (AWS, Azure, GCP) for misconfigurations, exposed assets, and threats; benchmarks against NIST CSF, CIS, ISO 27001 and delivers a prioritized roadmap.
- **Cloud Security Health Check** – technical assessment of cloud security configurations, vulnerabilities, permissions and active/past threats in cloud platforms and containers.
- **Zero Trust and Data Security Advisories** – services to assess and design **Zero Trust maturity**, data security and privacy controls, and **identity & access management** across hybrid and multicloud environments.
- **Ransomware Readiness Assessment** – evaluates defenses and recovery capabilities, including cloud workloads and data protection solutions, providing recommendations to improve ransomware resilience.

These services are typically used to:

- Establish a **baseline of cloud security maturity**
- Identify misconfigurations and gaps across multicloud estates
- Build a **phased roadmap** and investment plan for cloud security and resilience

---

3. Multicloud & Private Cloud Security

Dell combines **infrastructure platforms** with consulting services to secure private and multicloud architectures:

- **Dell Private Cloud – "Security by Design"**
    - Secure development lifecycle, supply-chain risk management and continuous security processes applied to the platform.
    - Built-in **cryptographic protections**, UEFI Secure Boot, encryption, and hardened images.
    - Integrated **identity and access management**, authentication, authorization and audit capabilities for the private cloud control plane.
    - Infrastructure observability to detect anomalies and support incident response in the private cloud environment.
- **Multicloud Services**
    - **Advisory and operating model services** to design and run secure multicloud environments across core, edge and public cloud, aligning people, process, and tools.
    - Support for major ecosystems (e.g. Microsoft Azure, VMware, Red Hat OpenShift) including secure network architectures, automation, and governance.

Outcome: customers get a **cloud-by-design architecture** with security embedded from hardware through orchestration and operations.

---

4. Cloud-based Data Protection & Cyber Resilience

Dell provides **cloud-delivered backup and recovery services** with strong security controls:

- **PowerProtect Backup Service / APEX Backup Services** (SaaS)
    - Cloud-native data protection built on secure **AWS infrastructure**, providing air-gapped protection, data immutability and strong encryption in flight and at rest.
    - Supports on-prem, virtual infrastructure, **cloud workloads**, SaaS applications and endpoints from a single platform.
    - Implements **Zero Trust architecture** with separate storage and control planes, SSO, MFA and RBAC for administrative access.
    - Shared-responsibility aligned design: hyperscaler secures infrastructure; Dell provides application-level security, governance and backup data protection.
- **Cyber Recovery & Business Continuity Services**
    - Design and implementation of cyber-recovery vaults and BC/DR solutions for workloads running on-prem and in public cloud.
    - Advisory Services for **Workload Recovery Planning** and **Recovery Readiness**, including runbooks and testing exercises for cloud workloads.

Outcome: ability to **quickly recover clean data** after incidents (including ransomware) across hybrid and multicloud environments, with immutability and strong encryption as defaults.

---

5. Managed Detection & Response and Cloud Threat Operations

Dell's **Managed Detection and Response (MDR)** and related services extend security operations into cloud environments:

- **Managed Detection and Response** – 24x7 threat detection and response services using leading SIEM/SOC and XDR platforms, covering endpoints, network, and **cloud security centers** (e.g., Defender for Cloud, Sentinel, etc.).
- **Penetration Testing & Attack Simulation Management** – including continuous breach and attack simulation to validate that cloud controls and policies are effective.

- **Vulnerability Management Services** – continuous scanning and remediation guidance for infrastructure and applications, including cloud platforms and exposed services.

These services help customers:

- Detect and contain threats that traverse **cloud and on-prem** environments
- Validate the effectiveness of controls and policies across multicloud
- Offload day-to-day security operations to Dell experts where desired

---

6. Cloud-Specific Implementation Services (Examples)

Dell offers targeted **implementation services** to securely deploy and integrate cloud technologies (especially with Microsoft and AWS):

- **Implementation Services for Microsoft Azure Public Cloud** – design and build secure, future-ready Azure environments, including landing zones, network security, identity integration, and governance.
- **Implementation Services for Microsoft Azure Network Security & Defender Cloud/IoT** – deployment and tuning of Azure network security, Microsoft Defender for Cloud and IoT for hybrid and multicloud environments.
- **Implementation Services for Cyber Recovery on Microsoft Azure** – extends Dell cyber recovery architectures into Azure, enabling secure vaults and recovery These offers complement the advisory and MDR services to provide an **end-to-end path from design to build to operate** for cloud security.

---

7. End-User, Endpoint and Access Security for Cloud

Because cloud access is only as secure as the endpoint and identity, Dell also provides:

- **Trusted Workspace & Endpoint Security** – hardware-assisted protection (Dell Trusted Device, SafeBIOS) combined with leading endpoint security partners (e.g., CrowdStrike, Absolute, Zscaler) to secure devices and the connections they make to cloud services.
- **Identity & Access Management Advisory** – evaluates directory services, identity providers and access policies used to connect users to cloud applications and workloads.

Outcome: stronger **device trust** and **identity controls** supporting Zero Trust access to SaaS and cloud workloads.

---

8. How to Position Dell Cloud Security Services with Customers

When talking with customers, you can frame Dell's security services for cloud around three outcome pillars:

- **Secure the cloud environment**
    - Multicloud and private cloud design with security by design
    - Cloud security posture assessments and Zero Trust roadmaps
- **Protect and recover data in the cloud**
    - SaaS-delivered backup (PowerProtect/APEX Backup) with immutability and strong encryption
    - Cyber recovery vaults and tested cloud recovery plans
- **Detect, respond and continuously improve**
    - MDR for hybrid and cloud workloads
    - Vulnerability, penetration testing, and attack simulation to validate cloud controls

Together, these capabilities help customers **reduce risk, meet compliance requirements and improve resilience** across their entire hybrid and multicloud estate.