Cloud Security

A Dell Point of View

Executive summary

Today, IT organizations focus more on services that deliver bottom-line results and less on the procurement and management of systems. As the pressure increases on IT to provide on-demand services that are agile, elastic and secure, more and more organizations are turning to the cloud. Cloud allows organizations to reinvent the way they deliver IT services to drive better business results.

According to Gartner, private cloud has moved from an aspiration to a reality for nearly half of large enterprises in the past few years.[1] And hybrid cloud computing isn't far behind. While enterprises crave the resiliency, predictability, data integrity, resource pooling, virtualization, elasticity and cost transparency of private cloud, they also want the flexibility to connect with public clouds. According to a recent survey, 82 percent of enterprises have a hybrid cloud strategy — up from 74 percent in 2014.[2]

But while cloud grows in popularity, it also introduces new security challenges. To protect mission-critical applications and data stored in the cloud, organizations need a comprehensive cloud security strategy. This white paper will explore Dell Managed Security Services end-to-end security solutions and how they safeguard critical data from external attacks and inside security breaches, reducing the risk of lost, damaged or stolen information.

Demystifying cloud and cloud security

According to the National Institute of Standards and Technology (NIST), cloud infrastructures come in a variety of deployment models, including public, private, community and hybrid. They also define three distinct cloud delivery models: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS).[3]

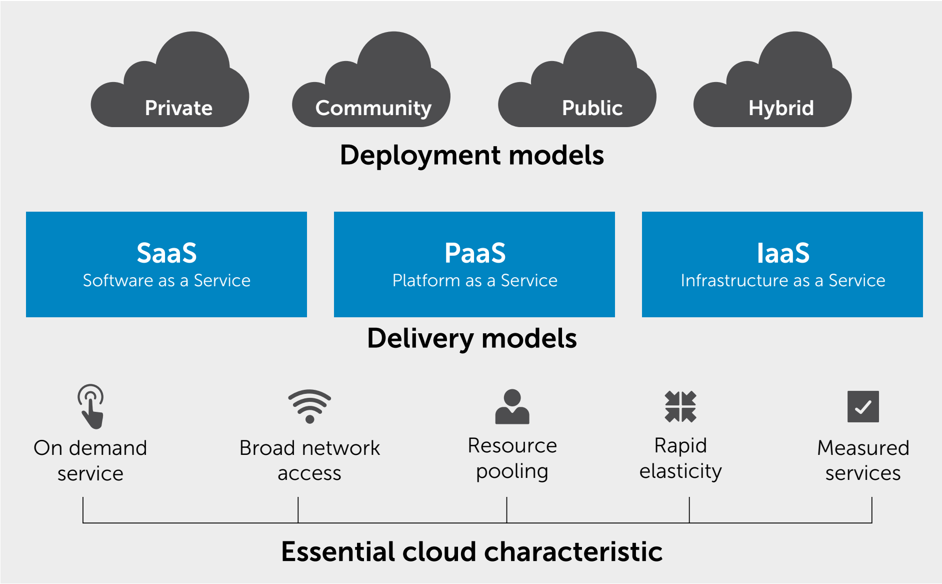


Figure 1: Cloud deployment and delivery models

Cloud solutions provide organizations with on-demand, self-service capabilities that include broad network access, resource pooling, rapid elasticity and measured or billable services. Multi-tenancy, another key aspect of cloud deployments, can help reduce capital expenditure and operating costs, but it also increases the need for cloud security.

Multi-tenancy enables the sharing of available resources by multiple consumers. This can lead to the possibility of another tenant having access to an organization's residual data or operational information, posing a significant security risk.

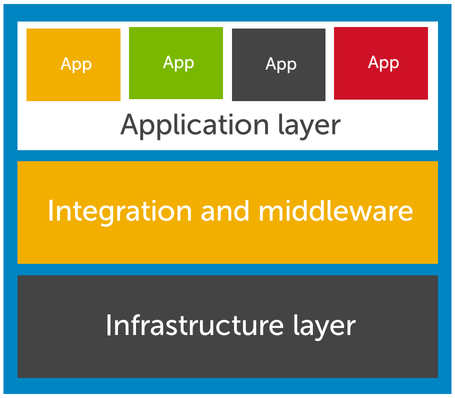


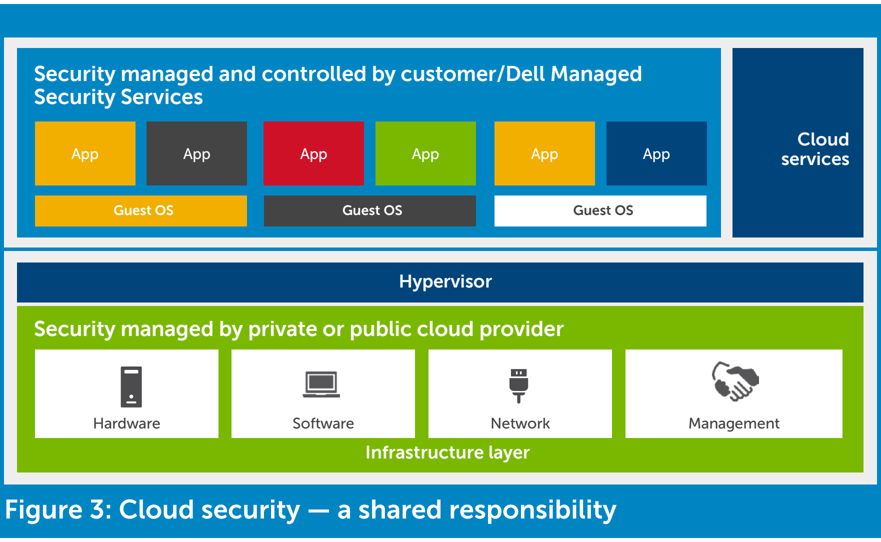
Figure 2: The cloud reference model

While a public cloud can have several tenants, a private cloud is often dedicated to one enterprise or organization, making workload isolation less of a security concern than in public cloud.

In a cloud environment, cloud providers and tenants have varying degrees of control over computing resources, and both parties share the responsibility of providing adequate protection for their cloud-based systems. This shared responsibility has been acknowledged by leading standards organizations, such as NIST and the Cloud Security Alliance, as well as major private and public cloud providers.

Cloud services provide flexibility, fast provisioning and quicker go-to-market appeal. However, because of the cloud service models employed and the technologies used to enable cloud services, cloud computing presents different security risks and challenges to an enterprise when compared to a traditional IT environment.

If you are planning or are already taking advantage of cloud deployment, are you confident that you have the right security measures in place?



Security managed and controlled by customer/Dell Managed Security Services
App
App
App
App
App
App
Guest OS
Guest OS
Guest OS
Cloud services
Hypervisor
Security managed by private or public cloud provider
Hardware
Software
Network
Management
Infrastructure layer

Figure 3: Cloud security — a shared responsibility

The Dell point of view on cloud security

Cloud security is a comprehensive set of policies, processes and tools used to protect data and applications running on private and public cloud infrastructures.

While security is a shared responsibility, Dell Managed Security Services can help organizations take the complexity out of cloud deployment. We provide seamless management and support for cloud security, backed by in-depth experience, proven tools, and certified trained consultants and security experts. Our services analyze, design, deploy, manage and extend enterprise security policies on behalf of the enterprise — from on-premises to private and public cloud deployments.

> “Across the entire spectrum, we are embedding security in everything that we do.”
>
> **— Michael Dell, Chairman and CEO, Dell**

With innovative intellectual property, such as Dell Cloud Manager and Dell Transformation Manager, as well as industry-accredited security tools, Dell Managed Security Services enable proactive monitoring, log and event analysis, incident reporting, and rapid containment and eradication of threats. Our solutions can significantly minimize the duration and impact of a security breach in a private or public cloud environment.

Key pillars of cloud security

There are two critical security challenges when moving workloads to a cloud environment. The first is how to safely and securely access workloads in a cloud environment, while the second and bigger challenge is how to extend the on-premises enterprise security policies to the cloud. Dell Managed Security Services utilizes the following strategies to overcome these challenges:

- **Host defense:** Whether workloads are running on-premises or in the cloud, an organization needs to harden the virtual machine (VM) by using host-based protection such as anti-virus, anti-spyware and host intrusion prevention system (IPS) software. This can be further complemented by providing web content filtering and host log monitoring capabilities.
- **Visibility and access control:** Manage user accounts and provide authentication, authorization and accounting, providing an added layer of protection in securing network infrastructure and application workload.
- **Encryption:** Encrypt if it’s relevant at the data, workload and transport levels. Encryption provides a new boundary that secures enterprise assets wherever they are. But at the same time, too much encryption may lead to additional compute overhead and may prevent benefits derived from technologies such as wide-area network (WAN) optimization.
- **Operational simplification and visibility:** Security needs to be consistent, transparent and operationally simple to manage — whether workloads are running in the data center, in a private cloud or on a public cloud infrastructure.

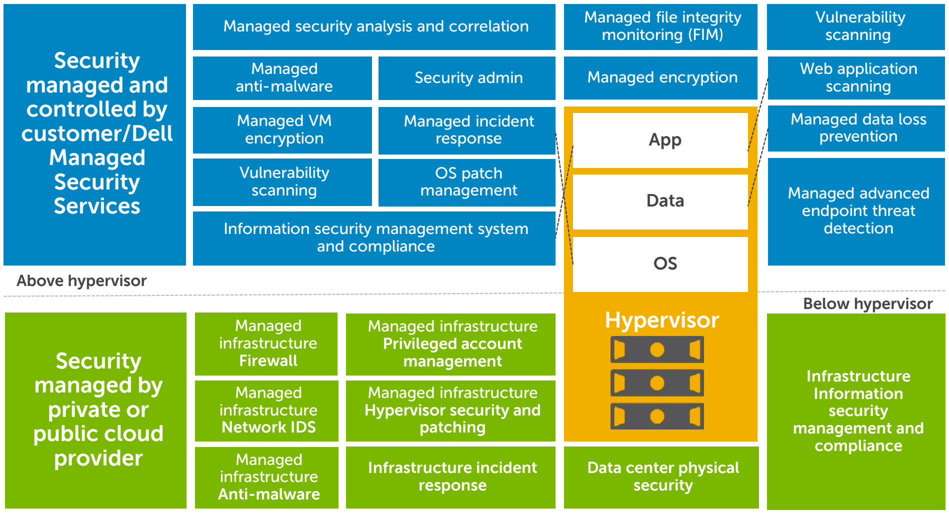

Security managed and controlled by customer/Dell Managed Security Services
Managed security analysis and correlation
Managed file integrity monitoring (FIM)
Vulnerability scanning
Managed anti-malware
Security admin
Managed encryption
Web application scanning
Managed VM encryption
Managed incident response
App
Managed data loss prevention
Vulnerability scanning
OS patch management
Data
Managed advanced endpoint threat detection
Information security management system and compliance
OS
Above hypervisor
Below hypervisor
Hypervisor
Security managed by private or public cloud provider
Managed infrastructure Firewall
Managed infrastructure Privileged account management
Managed infrastructure Network IDS
Managed infrastructure Hypervisor security and patching
Managed infrastructure Anti-malware
Infrastructure incident response
Data center physical security
Infrastructure Information security management and compliance

Figure 4: Our suite of managed cloud security services

Managed cloud security capabilities

As cloud security is a collaborative responsibility, from infrastructure to application security, Dell Managed Security Services works with organizations to empower them to take full control of security management of everything above the hypervisor in a cloud environment — from anti-malware and security administration to OS patch management and encryption.

Identity and access management

Identity and access management (IAM) is a critical aspect of running a secure cloud environment. Dell Managed Security Services use Dell One Identity Manager as well as Active Directory tools provided by industry-accredited vendors such as Microsoft and SailPoint to offer a role-based access control (RBAC) scheme for cloud administrators based on their job function, privilege and duties. Along with RBAC, a centralized auditing and logging solution is also offered to track all aspects of user and role management.

Guest operating system patching

Dell Managed Security Services offer a comprehensive patch management solution by utilizing tools, such as Dell KACE and Microsoft System Center Configuration Management, to optimize patching schedules. This allows organizations to download patches only when and as needed, optimizing the overall OS and application performance, and eliminating the need to manage patches that are not applicable.

Encrypting data at rest and in motion

Encryption can protect data in motion (also referred to as encryption in transit) as well as data at rest or in storage. Through strategic partnerships, Dell Managed Security Services offer organizations a scalable solution that can easily encrypt any file, database or application anywhere it resides on supported operating systems and file systems at the workload or transport level. This means organizations aren't sacrificing application performance with complex management processes — while also ensuring all user data is completely opaque to underlying providers and other tenants.

Transport-level encryption complements application-level encryption by implementing a virtual private network using either IPsec or SSL for connecting the enterprise on-premises network with the cloud infrastructure.

Vulnerability scanning

Vulnerabilities emerge every day within networks, web applications and databases, whether they are on-premises or in a cloud environment. Assessments help pinpoint vulnerabilities arising from system software shortfalls and system misconfigurations.

Dell Managed Security Services include a vulnerability assessment using tools, such as Critical Watch and Qualys, to provide programmatic identification, analysis and reporting of technical security vulnerabilities that an unauthorized person could use to exploit the confidentiality, integrity and availability of data and information systems.

Auditing and logging

Dell Managed Security Services assist organizations with securing their access control using high-performance security information and event management (SIEM) technology for enhanced log analysis and event monitoring. We also help organizations analyze logs generated by public cloud services, such as Amazon Web Services, AWS CloudTrail and Amazon CloudWatch. This includes logs for events such as configuration, hardening and patching of the OS and applications, as well as all events related to the access of applications running in a cloud environment. Proactive monitoring and auditing ensure compliance, change control and auditing, and improve operations and development processes.

Applications, infrastructure and network monitoring

Dell Managed Security Services offer operational awareness of applications, infrastructure and networking elements with continuous monitoring, correlation and assessment of alerts in real time.

We monitor applications using SIEM tools, such as Dell InTrust and Splunk, and integrate SIEM interfaces with strategic partner tools to perform infrastructure monitoring. Our process uses the cloud provider's application programming interfaces (APIs) to monitor, log and control all aspects of the organization's cloud infrastructure.

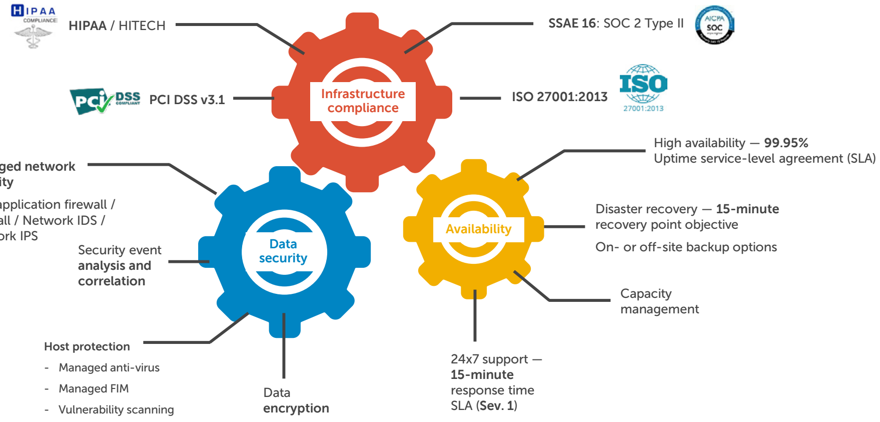

HIPAA / HITECH
SSAE 16: SOC 2 Type II
PCI DSS v3.1
Infrastructure compliance
ISO 27001:2013
High availability — 99.95%
Uptime service-level agreement (SLA)
Managed network security
Web application firewall / Firewall / Network IDS / Network IPS
Security event analysis and correlation
Data security
Availability
Disaster recovery — 15-minute recovery point objective
On- or off-site backup options
Capacity management
Host protection
- Managed anti-virus
- Managed FIM
- Vulnerability scanning
Data encryption
24x7 support — 15-minute response time SLA (Sev. 1)

Figure 5: Dell Cloud Dedicated integrated cloud security

Endpoint security

Dell Managed Security Services also offer managed anti-virus, data encryption, host IPS and vulnerability assessments to protect endpoints and workloads from spyware, trojans, viruses and worms, as well as prevent unauthorized access to an organization's data by utilizing enterprise-grade host anti-malware solutions. In addition, we provide host-based firewalls for mitigating the risk of unauthorized access across workloads running on the same hypervisor.

Firewall

Provide a first line of defense between the organization, the internet and their cloud environment. Dell Managed Firewall Services send firewall events to the SIEM for review and correlation with other events in the environment. Our certified engineers perform periodic firewall rules optimization to ensure the complex firewall rule sets provide the expected protection of an organization's cloud environment.

Intrusion detection and prevention

A managed intrusion detection system (IDS) and IPS help protect against attacks originating from the internet and ensure that other public cloud tenants don't gain unauthorized access to an organization's cloud workloads or data. The IDS and IPS can also send event information to the SIEM, providing our security operations center analysts with additional information that allows them to properly evaluate security events and threats.

Security strategy and risk management

Dell Managed Security Services can also assist enterprises with information security managers (ISMs), certified professionals who oversee cloud security programs and orchestrate the delivery of information security services. ISMs act as an organization's trusted partner, collaborating with the organization to understand, anticipate and recommend risk mitigation strategies, while providing information security protection for the organization's assets.

Dell Cloud Dedicated

Dell can help organizations confidently navigate complex cloud landscapes with Dell Cloud Dedicated, hosting a private cloud in either the organization's data center or a secure Dell data center. This allows the most sensitive, mission-critical workloads to run in a highly secure, dedicated IT environment — without daily management and maintenance.

Dell Cloud Dedicated is designed to serve as an extension of an organization's data center. With familiar management tools, an organization can quickly begin using the service without having to learn new interfaces or modify processes. Common data center tasks, such as OS management and backup and recovery administration, have never been easier. Our services provide a managed cloud infrastructure that is compatible with the IT Infrastructure Library-based operational processes an organization currently has in place. Our global onboarding team collaborates with the organization's staff to provide an effortless onboarding experience. Our expert project managers and technical consultants are also available to guide organizations and provide technical support.

Security in Dell Cloud Dedicated

Information security is one of the main components of Dell Cloud Dedicated. IT security services provide protection across the network, safeguarding the perimeter, critical internal assets, data, remote users, customers and partners. Dell security teams provide key controls for regulations, including the Gramm-Leach-Bliley Act, the Payment Card Industry Data Security Standard, the Sarbanes-Oxley Act, the Health IT for Economic and Clinical Health Act, the Health Insurance Portability and Accountability Act and ISO 27001/27002.

Information security for Dell Cloud Dedicated acts as a mature and integrated program that constantly evolves in order to fight against new threats and protect an organization's assets.

1

Prioritize cloud and cloud security plans

Look for business needs that require flexibility, resource pools and a rapid, dynamic response.

2

Maintain agility

Utilize open technology and standards so you can enable the technology you want, when you want it.

3

Choose the right partner

Ensure your needs are met with a committed, outcome-focused solution provider.

The recipe for cloud readiness and security

Dell believes that better security leads to better business. Designed to protect an organization's key information assets across cloud, networks, hosts and applications, Dell Managed Security Services offer the industry's broadest portfolio of security services to assist IT security and help IT organizations take full advantage of public and private cloud deployments. Our highly trained security experts become an extension of an organization's in-house IT staff and provide security analysis, device and technology configuration, alert management and 24x7 monitoring.

For more information, visit our Managed Security Services page or contact a Dell representative.

> "Cloud is not a destination or singular path, but a transformation that places IT squarely at the center of the enterprise as both a leader and enabler of value creation."
>
> **— Michael Dell,
> Chairman and CEO, Dell**

References

[1] Gartner Says Nearly Half of Large Enterprises Will Have Hybrid Cloud Deployments by the End of 2017. Gartner press release. October 1, 2013. http://www.gartner.com/newsroom/id/2599315

[2] Cloud Computing Trends: 2015 State of the Cloud Survey. RightScale. February 18, 2015. http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2015-state-cloud-survey

[3] Definitions, National Institute of Standards and Technology (NIST). http://www.nist.gov/

Further reading

1. Dell Infrastructure Managed Services: http://www.dell.com/en-us/work/learn/infrastructure-managed-services
2. Dell Cloud Dedicated Service: http://www.dell.com/en-us/work/learn/dell-cloud-dedicated-service
3. A guide to Dell Cloud Dedicated Services: http://i.dell.com/sites/doccontent/business/solutions/brochures/en/Documents/guide-to-dell-cloud-dedicated-services.pdf
4. White paper: Wanted: A Trusted Provider for Public Cloud Services: http://www.dell.com/learn/ie/en/iechn1/business~solutions~whitepapers~en/documents~idc-survey-trusted-cloud-providers.pdf
5. Dell Cloud Manager: http://software.dell.com/products/cloud-manager/
6. Infographic: Your Cookbook: Rapidly detecting and remediating advanced and evasive threats: http://www.secureworks.com/assets/pdf-store/other/infographc-detecting-advanced-and-evasive-threats-cookbook.pdf
7. Cloud Security Alliance: https://cloudsecurityalliance.org/
8. Federal Risk and Authorization Management Program (FedRAMP): https://www.fedramp.gov/

Scan or click this code to learn how Dell Services can help your organization.

Product and service availability varies by country. To learn more, customers and Dell Channel Partners should contact their sales representative for more information. Specifications are correct at date of publication but are subject to availability or change without notice at any time. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell's Terms and Conditions of Sales and Service apply and are available on request. Dell and the Dell logo are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims proprietary interest in the marks and names of others.