Security

Better security for a better enterprise

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.dell.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dell.com
Refer to our Web site for regional and international office information.

Table of contents

Better security for a better enterprise

In today's connected world, Dell believes that current approaches to security fall short. They work best for addressing security risks in only parts of the enterprise – the network or the endpoint, the user or the data. Because they operate in silos, these approaches create gaps, forcing the organization to manage each silo separately. This challenges everybody, especially users, with pointless and inefficient complexity. Plus, instead of reducing costs and risks, they have the opposite impact. Worse yet, security is seen as a process of restriction and denial, rather than a business enabler.

Dell™ knows there is a better way.

What if a single solution could help you:

- Eliminate proprietary islands of information that create risky security gaps
- Secure the enterprise from endpoint to datacenter to cloud without the burdensome complexity of administration
- Enable the enterprise to more efficiently meet its IT compliance and auditing requirements
- Empower--not impede--end-user productivity

Dell Security protects your organization from endpoint to data center to cloud, helps you achieve your most stringent compliance requirements, and enables rapid adoption of new technologies such as cloud, BYOD and more All of which moves security away from a process of restriction and denial, and toward a business enabler for the enterprise.

Challenges

Accessing data from outside the firewall

For IT groups and chief information security officers (CISOs), providing secure data access to authorized users beyond the firewall is one of their most difficult challenges. Employees — and in some cases, external partners — now access and disseminate enterprise data more frequently, and in more diverse ways, from outside the traditional firewall. Web- and cloud-based applications accommodate this freedom, but they can also introduce new risks for data security. Social media applications, which blur the line between business and entertainment, account for a notable amount of big data growth, but are an ever-present risk zone when it comes to protecting confidential information.

> "The point of origin today is less predictable — attacks can emanate from beyond the firewall or within."

The use of public cloud storage services is also on the rise. These file-sharing services may hold much more sensitive data than users realize, yet new users are often given access to these repositories without formal review. Users frequently access data through public WiFi hotspots, which introduces additional risks. IT groups need to provide fast, easy access for remote and mobile users while securing critical information.

Bringing your own device

The BYOD trend can present additional challenges. Workers today are accessing company data from a variety of mobile devices such as tablets and smartphones in a cloud-centric environment. A large percentage of these devices are owned by employees and are outside of IT management, yet they now hold and access data that belongs to the organization. Banning the use of personal devices for work is both impractical and counterproductive for many organizations — but securing those devices and its use for business purposes is also no easy feat.

Another challenge that would have been difficult to anticipate only five years ago: company data might be processed by unsponsored applications used across the cloud or shared via cloud-based storage by workgroups, individuals and departments. IT might be unaware of particular applications and devices handling company data. This eclectic access environment makes for a very complicated IT security scenario.

Addressing new security threats and improving governance

Organizations are also facing a larger number and greater variety of security threats. Criminals are devoting more resources to data theft. The point of origin today is less predictable — attacks can emanate from beyond the firewall or within. Many of these newer threats cannot be addressed with traditional technologies.

Attacks today are often hidden within traffic that previously was allowed into the network, such as web traffic. Business traffic often enters on the same ports used for web browsing. Legacy firewalls cannot determine if this seemingly benign traffic is carrying dangerous malware. Moreover, much of the traffic coming into the network is encrypted using the Secure Sockets Layer (SSL) protocol, so smart attackers have figured out how to leverage the same encryption technology to launch attacks.

Increasingly, organizations are also facing data access threats from inside the network. Imagine the damage that a user with unregulated access rights and bad intentions could inflict on an organization. In fact, this scenario is played out almost daily in the news and business media. Organizations need solutions that can help business managers as well as IT administrators effectively and efficiently govern what users have access to and how they gained that access.

Combating advanced persistent threats (APTs), modern malware, risky employee behaviors and internal theft can be challenging. Ensuring security today is more complex than it was five years ago — and the complexity will only increase. Organizations need effective solutions for overcoming threats that are also easy to administer and enable users to maintain their productivity.

Solutions

Dell helps organizations mitigate risks to enable success. How do we do it? We deliver:

A comprehensive portfolio, end to end: Core elements of the Dell Security portfolio include network security to protect the ever-shifting perimeter, endpoint security and encryption to protect data wherever it goes, identity and access management to reduce complexity and enable compliance, and security services for lower total cost of ownership. Dell solutions work together to protect your whole business, from the data center to the furthest endpoint and all along the networks and clouds in between, reducing unnecessary administration and complexity. With Dell, you can fill gaps created by legacy security silos and simplify management. You'll discover that securing everything can be much easier than you might think.

> "Put key security functions into the hands of line-of-business personnel."

Shared intelligence: Dell gathers, analyzes, reports on and shares context-aware analysis system-wide. This eliminates islands of security information and enables better decision making by working together to proactively prevent and even predict attacks.

Security that is built for humans: Dell Security solutions are engineered to be embraced, not just tolerated. Our deep experience and commitment to usability ensures security is embraced, not circumvented. It all adds up to security that stands in the way of threats, but stays out of the way of your people.

Trust: With 2,000 security professionals worldwide, an award-winning industry-validated portfolio, and millions of users, appliances and customers managed, Dell has the scale and expertise to be your trusted security advisor.

Identity and access management

Dell One Identity solutions empower you to achieve easier accountability and greater transparency, while placing the business in control of those things that matter most. Specifically, Dell One Identity addresses the entire range of IAM needs – from the most tactical access management requirements, to the most strategic, business-enabling governance initiative.

Identity governance: Achieve complete governance without sacrificing management and operations. Dell One Identity is unique in that it empowers line-of-business personnel to drive identity, data, and privileged access governance. One Identity's modular and integrated foundation marries visibility and control with the administration and management needs that are prerequisites to building strong governance.

Privileged management: Take a holistic approach to solving the challenges of securing privileged credentials. This is achieved with secure and efficient management of full credentials (when necessary), granular delegation and command control for least privileged access, and the ability to log, monitor and report on all activity for auditing and compliance.

Access management: Simplify and achieve secure access management for users and groups while controlling costs. Dell One Identity automates account creation, assigns access, streamlines on-going administration, and unifies identities, passwords and directories. Dell One Identity's modular and integrated approach to access management provides rapid time-to-value. This is achieved with comprehensive functionality that builds on existing investments and increases security, helping you meet compliance demands and getting access right the first time.

Compliance and IT governance: Ensure the integrity, confidentiality and availability of sensitive information while also providing audit-worthy proof of compliance in day-to-day operations.

Related products:

- ActiveRoles Server
- Defender
- Enterprise Single Sign-on
- Dell One™ Identity Manager
- Dell One™ Identity Manager - Active Directory® Edition
- Dell One™ Identity Manager - Data Governance Edition
- Dell One™ Quick Connect
- Dell One™ Privileged Password Manager
- Dell One™ Privileged Session Manager
- Dell One™ Identity Cloud Access Manager
- Privileged Access Suite for Unix

Network security

Dell network security solutions help you secure your network while sustaining performance and simplifying management.

Next-generation firewall: Implement a comprehensive layer of defense that combines malware prevention, intrusion prevention, SSL decryption and inspection, and application control with real-time traffic visualization and inspection to achieve a deeper level of network security against the evolving threats. Scan every byte of every packet for the deepest level of network protection without compromising performance. Scale to extend state-of-the-art security to growing and distributed enterprise networks.

Unified threat management: Designed for small businesses, retail deployments, government organizations, remote sites and branch offices, our unified threat management solutions allow you to move beyond consumer-level products by providing anti-malware, intrusion prevention, content/URL filtering and application control capabilities along with broad mobile platform support for laptops, smartphones and tablets.

Clean wireless: Dell wireless security solutions deliver outstanding performance for employees, customers and corporate visitors while protecting the corporate network. Plug-and-play deployment and centralized management of wireless access points allow you to provide the connectivity that users expect while avoiding administrative complexity. You can combine these appliances with firewall security to make sure wireless traffic is scrutinized with the same intensity as wired network traffic.

WAN acceleration: Improve WAN application performance and enhance the end-user experience for distributed organizations with remote and branch offices. You can reduce application latency and conserve bandwidth by transmitting only new and changed data across the network. Combine with firewall security, application intelligence and control service capabilities to optimize performance.

> "Implement a comprehensive layer of defense that combines intrusion prevention, SSL decryption and inspection and application intelligence with real-time traffic visualization and inspection."

Security and analytics management: Dell offers management and reporting solutions to help simplify security solution administration and analytics reporting. With these solutions, you can centralize management of security policies and appliance-based solutions. Use real-time monitoring and alerting capabilities to optimize the performance, utilization and security of your network.

Related products:

- Dell™ SonicWALL™ SuperMassive E10000 Series
- Dell™ SonicWALL™ SuperMassive™ 9000 Series
- Dell™ SonicWALL™ Network Security Appliance Series
- Dell™ SonicWALL™ TZ Series
- Dell™ SonicWALL™ Clean Wireless
- Dell™ SonicWALL™ WAN Acceleration Appliance (WXA) Series
- Dell™ SonicWALL™ Global Management System Series
- Dell™ SonicWALL™ Scrutinizer
- Dell™ SonicWALL™ Analyzer

Secure mobile access

Supporting today's remote and mobile workforce requires secure access to enterprise networks from a diverse array of devices and platforms often running different operating systems. With Dell secure mobile access solutions, you can offer your employees and extranet business partners SSL virtual private network (VPN) access to allowed mission-critical resources from virtually any endpoint — including smartphones, tablets desktop and laptops without compromising security. Select from a portfolio of scalable solutions designed to support organizations of any size, from small and medium-size businesses to the largest global enterprises.

Enable secure mobile access and role based privileges for users with managed and personal BYO devices for up to 20,000 concurrent users - from a single appliance. Control access and authorization to corporate resources by authenticating the user and checking the identity and security profile of the endpoint allowing only trusted users and devices to gain access.

Restrict VPN access to the set of trusted mobile apps allowed by the administrator, and prevent unauthorized apps from accessing VPN resources. The solution is mobile app agnostic. It supports standard apps without requiring any modification, speeding time to deploy and reducing costs.

Mobile workers get the fast, simple access to the enterprise data and resources that they demand, and the corporate network is protected from mobile security threats, such as unauthorized access to data and malware attacks.

Related products:

- Defender
- Dell™ SonicWALL™ E-Class Secure Remote Access (SRA) Series
- Dell™ SonicWALL™ SRA Series
- SonicWALL™ MobileConnect
- Dell™ Enterprise Mobility Management

Email security

Securing email is critical for maintaining productivity, combating a wide range of potential threats. Further, the secure handling of email can impact compliance and e-discovery mandates. Dell Email Security solutions protect your organization from viruses, zombies, spam, phishing and other attacks by leveraging multiple threat detection techniques, along with a unique worldwide attack identification and monitoring network. Multiple deployment options enable you to address your specific requirements while simplifying management and controlling costs.

Dell Email Security solutions also help you better understand email usage, archive for compliance, perform e-discovery without overburdening your administrators and audit all mailboxes and access controls to prevent violations. In addition, it also prevents confidential data leaks and regulatory violations. Advanced compliance scanning and management includes integrated email encryption cloud service to ensure secure exchange of sensitive data.

You can implement a flexible and scalable security solution that provides complete inbound and outbound email protection for an organization of any size. Cloud-based email security enables you to reduce upfront deployment time and costs as well as ongoing administration expenses. On-site security solutions can be deployed as hardware appliances, virtual appliances or software, including software optimized for Microsoft® Windows Server® or Small Business Server (SBS). On-site solutions scale easily and cost-effectively from 10 to 100,000 mailboxes. Add the Comprehensive Anti-Spam Service (CASS) to Dell firewalls to virtually eliminate inbound junk email at the gateway before it enters the network.

You can also reduce risk and improve security with powerful reporting and auditing solutions that detect and ease the investigation of suspicious communications, as well as provide real-time alerts and standard compliance reports for critical configuration and permission changes to Microsoft Exchange. Email archiving and recovery solutions protect your organization by ensuring email is available when needed. Granular search and recovery options that export results into a variety of formats simplify and speed your response to e-discovery requests.

Related products:

- Archive Manager
- ChangeAuditor™ for Exchange
- Dell™ SonicWALL™ Email Compliance and Encryption Service
- Dell™ SonicWALL™ Comprehensive Anti-Spam Service
- Dell™ SonicWALL™ Email Security Appliance, Virtual Appliance and Software

- Dell™ SonicWALL™ Hosted Email Security
- MessageStats™
- Recovery Manager for Exchange
- Security Explorer
- Dell™ Email Continuity Service

Endpoint security

Ensuring tight protection for desktops, laptops and other endpoint systems is crucial for maintaining user productivity and preventing hackers from gaining access to your network and enterprise data. Dell solutions for endpoint security can block annoying spam and malware, find potential endpoint vulnerabilities and encrypt the enterprise data residing on endpoints. Designed to streamline management, Dell solutions enable you to keep your data and network safe without adding administrative complexity.

Dell anti-virus and anti-spam solutions can help protect your servers, desktops and laptops from a broad range of threats. These solutions help ensure that all endpoints have the latest versions of anti-virus and anti-spyware software installed and active. They enable you to stop the spam and phishing emails that can introduce security issues and sap productivity.

Solutions for endpoint control help you identify and remediate vulnerabilities on your endpoints with an easy-to-use, cost-effective appliance. You can manage and enforce compliance with company policies across desktops, laptops, tablets, smartphones and servers from a single console with simplified configuration and patch management. Dell solutions for endpoint encryption and data protection allow you to employ endpoint encryption to protect data wherever it rests — without affecting user performance. Support for multiple platforms enables you to apply effective data protection across your enterprise. A single set of management tools for all encryption functions helps simplify administration.

Related products:
- Dell™ Data Protection and Encryption
- Dell™ SonicWALL™ Anti-Spam Desktop
- Dell™ SonicWALL™ Enforced Anti-Virus and Anti-Spyware
- KACE K1000 Systems Management Appliance
- Dell™ Enterprise Mobility Management

Security services

IT organizations are facing growth in advanced threats and attackers, more attack surfaces to protect, a greater number of regulatory requirements and an increased desire to do business on an OPEX model instead of a CAPEX approach – all while contending with continued shortages in qualified security staffing. In some cases it can be easier and more effective for a managed security services provider to help.

Dell SecureWorks helps you reduce risk by providing Managed Security Services, Security and Risk Consulting services, Incident Response services and Threat Intelligence services. Dell SecureWorks' global visibility, effective correlation and analysis capabilities, and vendor agnosticism provides the most complete managed security services solution in the marketplace. With a two-way flow of information between the Counter Threat Unit and other services, you will benefit and minimize risks from the knowledge gained from any single event.

Related products:
- Managed Security Services
- Security and Risk Consulting
- Incident Response
- Threat Intelligence services

Case studies

Simplifying identity and access management

Challenge

Williams Energy is one of the leading integrated natural gas companies in the United States. The company wanted to reduce the costs and complexity of its identity and access management (IAM) solution. The company also wanted to add an access request capability that was lacking in the existing solution.

Solution

The company decided to implement a Dell One Identity Solution to help substantially simplify tasks and reduce costs. Process orchestration married to governance delivered the access request functionality that the company wanted.

Results

- Secured the entire population of Unix and Linux systems efficiently through Microsoft Active Directory® and Dell One Identity Solutions
- Provided self-service capabilities for end users and managers
- Created an identity and access management environment that is business-driven, security- and compliance-optimized, and future-proofed

Implementing a clean VPN and saving US $1 million annually

Challenge

Aaron's Inc. — a leading retailer and lease-provider of residential and office furniture, consumer electronics, home appliances and accessories — needed new ways to securely connect its growing enterprise while maintaining compliance with Payment Card Industry Data Security Standard (PCI DSS) regulations. Networking engineers had no visibility into the type of traffic traveling across the public gateways. Aaron's also wanted to install internet access at its 1,800-plus stores.

> "The more granularly we can manage and prioritize social networking traffic like Facebook with Dell SonicWALL's application intelligence, control and visualization feature, the better we can manage our network, boost employee productivity and protect our organization."
>
> —Jason Tate, director of network services, Aaron's Inc.

Before doing so, it needed to implement a firewall that could govern traffic appropriately while ensuring core business functionality was not hampered.

Solution

Aaron's selected Dell appliances, which the company used to establish a private distributed VPN for uploading data securely from its thousands of locations. The company implemented firewalls in its corporate center and regional fulfillment centers, and deployed more than 1,600 firewalls at its retail locations.

Results

- Saved the company more than US$500,000 per month by enabling the use of high-speed broadband instead of T1 lines
- Delivered more services to stores while helping to ensure tight security of sensitive information — SonicWALL appliances provide access to authorized users while clearing out malware attacks and quarantining affected locations

To learn more about the SonicWALL implementation at Aaron's Inc., visit: www.software.dell.com.

Conclusion

Reducing risk and enabling new business initiatives from the endpoint, to the data center, to the cloud

CISOs and IT groups face three simultaneous imperatives: protect critical data and systems efficiently and effectively, comply with regulations in a consistent manner without impacting business agility, and enable end users and the enterprise to move faster and do more.

The Dell Security solution addresses these priorities:

- Eliminating proprietary islands of information that create risky security gaps
- Securing the enterprise from endpoint to datacenter to cloud without the burdensome complexity of administration
- Enabling the enterprise to more efficiently meet its IT compliance and auditing requirements
- Considering the human factor by not impeding end-user productivity

With Dell Security, you can reduce your risk profile and meet your most stringent compliance and security requirements.

For more information about Dell Security solutions, contact your Dell sales representative or visit: dellsoftware.com/solutions/security.