
Better Security
for Better Business
Enabling business strategy with simpler,
more connected IT security.

Better Security for Better Business

Enabling business strategy with simpler, more connected IT security

No one needs another reminder of the strategic importance of information security. For that, one need only to scan the headlines, which regularly feature major brands that are losing customers, investors, and even their chief executives in the wake of high-profile data breaches or compliance breakdowns. The threats are real. The consequences are dire. Even board members are now painfully aware of these new realities.

So if we're all sufficiently terrified, what is the relentless tide of bad news telling us that we don't already know? Put simply, it is telling us that the technology and approaches we are using to secure our information and systems are not working. It is telling us that despite spending more than ever to protect our systems and comply with internal and regulatory requirements, something is always falling through the cracks.

There are several reasons for this lack of success. One is the fact that the IT security market is highly fragmented. There are dozens of "best-of-breed" solutions addressing narrow aspects of security -- from intrusion detection to application security to identity and access management. Each solution requires a single specialist to administer the software. And they leave gaping holes between them that make exploitation or compliance violations a matter of time. Many organizations find themselves with great confidence in certain areas of security, but others that they fear are woefully lacking.

"Patchwork solutions that combine products from multiple vendors inevitably lead to the blame game," says Bill Evans, director, product marketing, Dell One Identity solutions for identity and access management. "You get the antivirus company pointing a finger at the firewall company, who points the finger at the identity management vendor. Each of them is responsible for only part of the problem. It's not a system. It's not efficient. And it's not very secure. It's got to stop."

There are monolithic security frameworks that attempt to address every aspect of security in one single solution, but they are inflexible and extremely expensive to administer. They are also completely divorced from the business objectives of the organizations they're designed to support.

We live in a connected world, in which data is the lifeblood of business. But for data to be valuable, it must be secure everywhere it resides and everywhere it needs to go. Some security solutions restrict the flow of that data, making it less useful to the organization. Some are burdensome to end users, which creates risks when well-intended employees fail to comply with security practices. And some are not tailored to the unique needs of a specific company or industry. In fact, according to one Gartner study, executives rank security, governance and compliance as one of the top three barriers to realizing the full potential of information technology.

"It would be hard to estimate just how much productivity is lost and how much innovation is stifled due to poorly designed security products and protocols. It's just bad business."

- *Elliot Lewis*
Chief Security Architect
Dell Software

"It would be hard to estimate just how much productivity is lost and how much innovation is stifled due to poorly designed security products and protocols," says Elliot Lewis, chief security architect, Dell Software. "It's just bad business. It's bad business because it costs more than it has to. It's bad business because you're not protected as well as you should be. And it's bad business because it restricts the very capabilities that information technology was designed to enable."

At Dell, we have studied the shortcomings of today's IT security with a fresh perspective. We have seen the fractured nature of the solutions, and the absence of security strategies that align with business needs. And as we have done in the past – first with personal computers, then servers and then storage -- we have architected a better, more efficient approach that we believe will rapidly fortify this fragmented market.

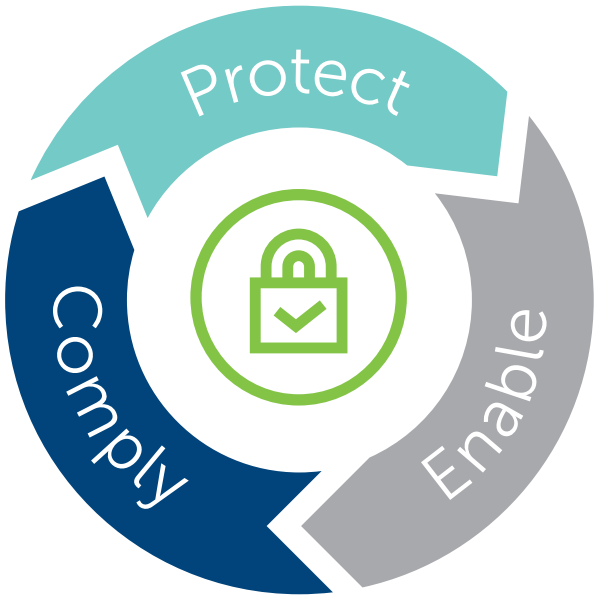
Better Security for Better Business

Dell's approach to security is based on simplicity, efficiency, and connectivity that tie together the splintered aspects of IT security into one, integrated solution, capable of sharing insights across the organization. It adds a critical layer of guidance from Dell experts, who help businesses focus their security efforts. And it makes security simpler, so that business users can manage the rules and policies, and end users can easily comply. Together these enhancements can radically change the culture of compliance within organizations. And strengthen the overall security posture, allowing easier adoption of disruptive technologies -- like cloud and mobile– so your organization can refocus on doing what it does best.

"The nature of data has changed, but the security solutions designed to protect it have not," says Lewis. "In order for data to be useful, it needs to be available. It needs to move whenever, wherever it is needed. And that's a good thing. Most vendors try to wall it off, keep it in silos. But we're connecting all of the siloed security solutions, so firewalls are sharing information with identity and access management software and so on. In this environment, data still moves freely, but threats are more readily detected, and we move from reactive to proactive to predictive."

Our approach is built around the three foundational imperatives of IT security:

- **Protect** – the whole enterprise, from end-to-end, inside and out, with efficiency
- **Comply** – with internal governance policies and external regulations using a consistent, reliable approach that doesn't compromise business agility
- **Enable** – the confidence to adopt new technology and pursue innovation and operational efficiency



By bringing solutions to market that address each of these three pillars, and giving them common DNA so that they can be connected together end to end, we believe that IT security can be better, easier to use, and less expensive. And most importantly, it can become a driver of innovation, rather than an obstacle to it.

Protect

Protecting the IT infrastructure is, of course, the most basic requirement of any IT security system. The current approach to protection for most organizations is to buy a firewall solution, some intrusion detection software, identity management, anti-virus, and more, and try to follow some best practices and keep all the software up to date.

"The problem is that threat actors are always changing their approach based on whatever the best practices are," says Jon Ramsey, chief technology officer, Dell SecureWorks, and Dell Fellow. "They study them, and design ways to get around them. So the more pervasive the best practices, the more likely they are to be targeted, and eventually overcome, by the bad guys."

One way to break this vicious cycle is to employ managed security services and to train employees on simple, easy-to-understand procedures. AZUR SPACE Solar Power is a German company that makes high-performance solar cells for extraterrestrial applications, from the Hubble Space Telescope to Mars Express. Its clients demand extremely rigorous security around product and launch plans. And Azur Space has chosen to partner with Dell to provide continuous monitoring of their networks and advice on the best ways to protect them.

"Security gaps can arise through conceptual errors, irregular system maintenance or changes made to the application environment," says Martin König, Director of IT Services at AZUR SPACE Solar Power. "It's difficult for our company to identify these gaps because we implemented the original system deployment and made the subsequent configurations. This is why we need an external security expert to conduct our testing."

AZUR SPACE uses Dell SecureWorks to conduct regular penetration testing of its networks. The service probes all access points and core applications for vulnerabilities, and the Dell team of security and risk experts cross-references the findings against its database processing 76 billion cyber events a day. The risk assessment is then translated into actionable recommendations, written specifically to address key business requirements.

"We have a level of detailed security information that can be understood by our technical team as well as at management level," says König. "It highlights issues that may be important for risk assessment and company liability."

Comply

"Customers don't care if your company was compliant," says Ramsey. "All they care about is whether their data was stolen."

Today, many organizations manage their security environment to comply with regulations. They assume that if they meet all the checklists, their networks are secure. But this is backward thinking. "The C-suite doesn't know enough about what it means to be secure, so they adopt the language of compliance," says Ramsey. "They often fail to develop risk-management strategies that are articulated by governance policies, all of which is informed by strong IT security. They take a compliance approach to security. But they need to take a security approach to compliance."

"Customers don't care if your company was compliant. All they care about is whether their data was stolen."

- *Jon Ramsey*
Chief Techology Officer
Dell SecureWorks

That's precisely what Virginia Commonwealth University (VCU) did following a security audit at its school of medicine. The VCU Medical Center provides care in more than 200 specialty areas, and is the only Level-1 trauma center in the Richmond area. As such, it is required to comply with several stringent regulations on federal, state, and local levels, including HIPPA, the Federal Information Security Act, and the Family Educational Rights and Privacy Act, among others.

To meet, and exceed, these demanding requirements, VCU took a security approach to compliance. They chose to encrypt the data on endpoint devices, from laptops to desktops to mobile devices. Like many organizations, VCU allows its employees to bring their own devices into the workplace, making it difficult to standardize security across the workforce. Encrypting the data solves this problem, but can quite often be too expensive or too burdensome to use. The Dell Data Protection | Encryption solution is neither, and VCU's end-users report no disruption to their work. A simple, easy-to-use solution that spans multiple devices across a distributed workforce without sacrificing speed or agility.

Enable

For decades, IT security has been viewed as an inhibitor of business agility; a well-deserved reputation. In many cases, it constricts, slows, and outright prohibits some business functions. These limitations have come to be accepted by most organizations, presumed to be an unavoidable cost of doing business. But when done right, security can actually enable a business, giving an organization the confidence to aggressively

pursue new capabilities that can have a direct impact on revenue, profits and the customer experience. It can give users the confidence to work anywhere, anytime, on any device.

"When you trust your security solution, it encourages the adoption of new technology," says SecureWorks' Ramsey. "That opens the door to innovation, both inside and outside the company firewall."

Take the Denver Broncos, for example. One of the most successful franchises in the history of the NFL, the Broncos support a staff of about 300 employees during the week. But on game days, they support 76,000 fans at Sports Authority Field at Mile High, the Broncos stadium, which becomes the 15th largest city in the state during home games.

"The fans all bring smartphones and they all want to see instant replays," says Chris Newman, IT Architect for the Denver Broncos. "Our goal is to give the fans a game-day experience that will exceed what they have at home."

To do that, the organization supports wireless broadband throughout the 13-acre sports complex, protected by the SonicWALL SuperMassive next-generation firewall and a secure remote access device to secure the network while boosting performance, efficiency and insight. "We're very visible and we can't have any intrusions or have

"When you trust your security solution, it encourages the adoption of new technology. That opens the door to innovation, both inside and outside the company firewall."

- *Jon Ramsey*
  Chief Techology Officer
  Dell SecureWorks

anything go awry," says Newman. "With the Dell solutions, we can customize the interface, it's easy to deploy, and it's much easier for the users. Even our employees are more productive." Another example of enabling an organization through better ecurity is the Wake County, N.C. Sherriff's Office, with responsibility for the public safety of nearly one million citizens in and around Raleigh. The public safety agencies in Wake County promote data and intelligence sharing based on the belief that doing so enhances their ability to detect, prevent and respond to public safety issues across the county and beyond. The Sherriff's Office acts as the central repository for the county's criminal justice data, which is accessed by all public safety divisions within the county. But access to the system was restricted for security reasons, which resulted in mounting requests to the Sherriff's Office, and a backlog of frustrated end users. "Many of the agencies wanted some autonomy to be able to manage their own records without having to rely on us every time they needed to change something," says Christopher J. Creech, manager of Information Technology for the Wake County Sheriff 's Office. "We have a lot of novice IT people. They did not understand how the system worked — they just wanted to be able to go to one place and update their department information."

Ultimately, the cumbersome processes affected the entire public safety community. When the Sheriff 's Office became overwhelmed, critical data could not be added or changed in a timely manner. But with an Dell One identity and access management solution, the Sherriff's Office was able to allow more access to the system, without compromising security.

"The program allows agency personnel to use the system but prevents them from getting native access within the application, which would grant them a broader set of privileges that we wouldn't be comfortable with," says Creech. "The ability to quickly update and share data is a huge factor in enabling us to do our jobs better. Ultimately, it allows us to more effectively serve and protect the public."

"The ability to quickly update and share data is a huge factor in enabling us to do our jobs better."

- *Jon Ramsey*
Chief Techology Officer
Dell SecureWorks

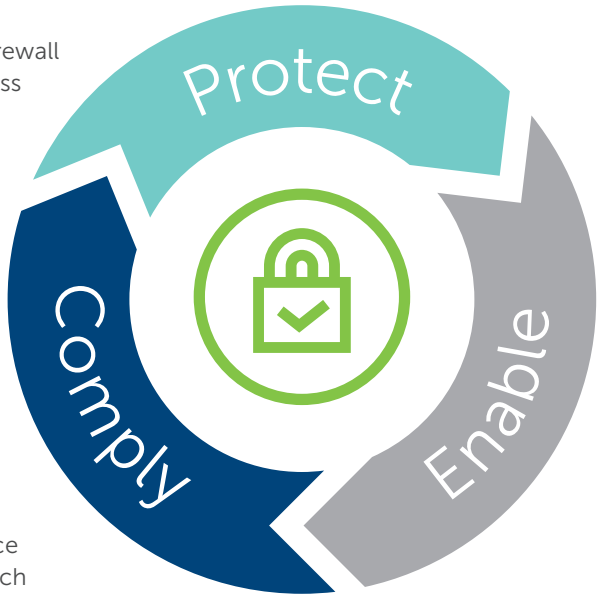
Capabilities

Dell has always been inspired by finding ways to improve IT and lower costs to customers, especially in markets where customers are locked in by the status quo. If there is a better way, Dell finds it. By architecting solutions that have common DNA, Dell is taking the first steps toward more connected, holistic security. The promise is that this approach will be more efficient, more secure and more easily adopted. Most importantly, it will work with the business, not against it.

To this end, we have developed or acquired the best solutions in the market, covered every aspect of IT security, and built common components into each that allow seamless integration. The solutions fall under four key areas of security infrastructure, and cover an enterprise's end-to-end needs:

The Dell Security Solution

Network
Next-Generation Firewall
Secure Mobile Access
Email Security



Identity & Access
Management
Identity Governance
Privileged Management
Access Management
Compliance & IT Governance

Data/Endpoint
Encryption
Protected Workspace
Configuration & Patch Management
Secure Cloud Client

Security Services
Incident Response
Managed Security Services
Security & Risk Consulting
Threat Intelligence

But the vision doesn't end there. Dell is already working on next-generation approaches to security, investing in solutions that secure data wherever it goes. "In the future, we'll not be securing enterprises or even systems. We'll be embedding rules and policies into the data itself that can sense when it has fallen into the wrong hands. Data needs to be free to move, but safe," says Dell's Elliot Lewis.

"This is the future we're working toward. This is the future we're creating."

Learn more about Dell Security solutions at **Dell.com/security**

Become a member of the **Dell Security community on LinkedIn**