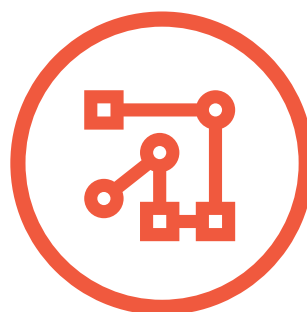




Dell Technology Outlook 2015



Executive Summary

Technology innovations once took considerable time to become mainstream; they are now doing so at an unprecedented pace. These innovations challenge how we work, think and plan for the future. Societal influences, the effects of globalization, and our own expectations all play a part in the rapid adoption of new and exciting technological advances.

These forces also have a fundamental impact on organizations, which today must be more responsive, more efficient, and smarter. Some organizations – and even entire

industries – will become irrelevant if they are unable to anticipate the changing expectations of customers and users, and the technical innovations that can enable these changing expectations.

This report contains predictions by Dell Research about ten technological events we believe will take place in the next five years. These technologies will be major catalysts for organizations to transform the performance, cost, and agility of their technology infrastructure to meet current and future needs.

Introduction

Technology is the backbone that powers most enterprises, and is often the determining factor for success or failure, relevancy or obscurity. Since our beginning, Dell has played a critical role in transforming the computing industry and making advanced technology more accessible and affordable to more people around the globe. And, because we have direct visibility to our customers, we focus our research and development efforts on real-world challenges where it matters the most, to deliver better results to their organizations. This is what we call “Practical Innovation” - innovation not for innovation’s sake, but derived from multiple components of ingenuity to directly address real customer issues today and into the future.

Practical Innovation is achieved through Dell’s ability to “skate to where the puck is going,” making investments in the right technologies at the right time, to provide the best customer experience possible and establish first-mover advantage. For example, we foresaw the industry moving to open IP-based iSCSI storage and were able to establish a presence in that business early enough to become and remain the number one technology company in IP-based iSCSI storage.¹

Dell’s approach to practical innovation incorporates four investment areas: human capital, partnership capital, financial capital and technology capital.

This paper has been written from the lens of Dell Research, a key element of the technology capital. Each year, Dell Research creates the Dell Technology Outlook (DTO): predictions about ten key disruptive technology inflection points that have the

potential to significantly affect organizations over the next five years. These forecasts and ideas inform and drive the Dell Research project selection, influence Dell technology strategy, and help us “skate to where the puck is going,” to better shape our advice and relationships with customers, partners and the industry at large.

The DTO is differentiated from other industry reports on technology trends because of our longer-range focus – we highlight the trends beyond what other reports present. For example, many technology trends reports discuss the Software-Defined Data Center (SDDC). In the DTO, we discuss the Software-Based Data Center (SBDC), which is the Dell Research view of what comes after the SDDC. This is because the SDDC has been widely discussed in other places, and we would rather discuss trends which are also fast-approaching but have been less widely-discussed. As you read our report, you will repeatedly see examples of the “next trend beyond today’s trend.”

We are pleased to share these predictions with you, which we believe will shape the industry over the next five years.

Sincerely,



Dr. Jai Menon
Chief Research Officer and
Vice President, Dell







In this report

Collaborative discussions with customers, industry experts, Dell technologists, analysts and academic researchers have informed and influenced the predictions contained within the Dell Technology Outlook 2015.

Dell's heritage is one that values and enables direct conversations with customers and partners. We find that discussions of technology and innovation frequently fall into four distinct categories:

- **Transforming the efficiency of IT:** This requires accelerating the transition toward a more efficient and effective enterprise computing environment—through modernization and an expanded use of virtualization, convergence and cloud technologies, services, and solutions.
- **Connecting the workforce:** An increasing number of employees are interacting and processing information through mobile methods, working remotely, and choosing to use their personal devices to connect to corporate IT resources. Dell helps organizations address access, management, and security challenges to enable their employees and customers to take full advantage of mobility.
- **Informing decisions:** The volume of data is skyrocketing, as is the number and variety of sources generating this data. Dell helps organizations more effectively store, manage and protect information, as well as derive more value from data and gain greater insight from it.
- **Protecting the organization:** Successful organizations are able to maintain a continued focus on overcoming evolving security threats and ensuring compliance. Dell delivers a seamless security strategy that works across the organization—from the device to the data center to the cloud.

<p>Transform the efficiency of your IT</p> 	<p>Connect your people for more productivity</p> 	<p>Inform by turning data into insights</p> 	<p>Protect everything everywhere</p> 
<p>Accelerate modernization with virtualization, convergence & cloud</p>	<p>Access resources anytime, anywhere, and on any device</p>	<p>Derive greater insights from information of all types</p>	<p>Safeguard against evolving and wide-ranging security threats</p>
<p>Enable IT services to be delivered more efficiently than ever before</p>	<p>Enable greater flexibility & productivity when, where, and how people work</p>	<p>Use new methods of storing & analyzing large & diverse sets of data for better decision making</p>	<p>Combat persistent threats to data & IT assets with less cost and complexity</p>

Ideally, every organization diligently works to make their technology infrastructure more agile, cost effective, and productive. However, since time, staffing, and funds are often limited, it is essential to understand which investments can produce the greatest value, benefit, and impact. Consider the DTO as a guide to the future that can help you make those critical decisions for your organization.

Following are predictions of 10 technological events that will take place between the years 2015 and 2020, segmented into the four customer imperatives that drive Dell and Dell Research's focus:

Dell Technology Outlook 2015 Predictions

Transform

By 2020, specialization via software will beat custom hardware.

By 2017, next-generation non-volatile memory will arrive.

Connect

By 2016, BYOD focus will shift from solely addressing security to addressing security with usability.

By 2016, an explosion of internet-connected devices will create new challenges and opportunities.

By 2018, user interfaces will evolve to understand more about user intent.

Inform

By 2020, analytics will evolve from descriptive to predictive to prescriptive faster than anticipated.

By 2020, the majority of real-time data analytics will be seamlessly integrated into business processes.

Protect

By 2018, security will shift from reactive to predictive and become context aware.

By 2019, cloud security will be strengthened by homomorphic encryption.

By 2017, there will be a paradigm shift in Data Loss Prevention (DLP) to self-protecting data.



1. By 2020, specialization via software will beat custom hardware.

Software-based data centers (SBDC) and high-velocity cloud (HVC) will emerge.



Today's data centers are very complex, containing rack after rack of custom-configured server hardware, network infrastructure, storage arrays, and other equipment. Fundamentally, these pieces are composed of different combinations of compute, data storage, and network components. Each rack is physically configured for a specific workload or function.

In a software-defined data center (SDDC), software is used to provision, manage, and orchestrate these server, storage, and networking resources. Each resource exposes application programming interfaces (APIs) that can be used to manage it. However the resources themselves often exist as specialized or custom hardware. A **Software-Based Data Center (SBDC)**, as defined by Dell Research, is a data center in which proprietary hardware resources are replaced by software running on standard servers, for reasons explained below.

Historically, custom hardware was used to deliver unique capabilities or improved performance that was not possible with general purpose, standards-based hardware. As time progresses, however, we find that standard hardware can provide the same capabilities at lower cost.

Proprietary, custom hardware has two distinct disadvantages compared to standards-based, general-purpose hardware:

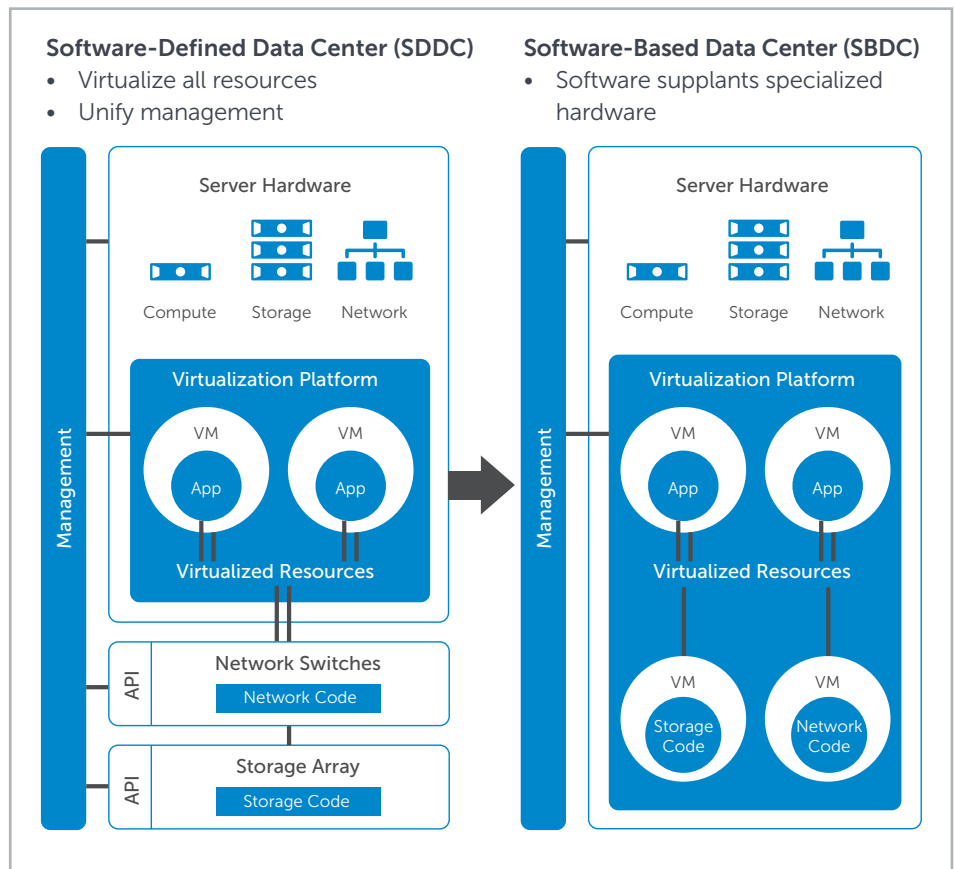
- Higher prices due to lower production volumes, usually due to a smaller serviceable market. Standardized hardware costs less over time.
- Proprietary lock-in and longer product cycles for technology which becomes increasingly difficult to migrate away from. Standardized hardware advances more rapidly and delivers more market-tested reliability and features.

As servers continue to advance in performance, memory capacity, and bandwidth capability, it enables more affordable commodity hardware and software to accomplish what previously required expensive, custom, highly specialized hardware. Such software-based solutions can be updated and

deployed rapidly, and can be repurposed for another function just by altering the software.

There are two different manifestations of this trend. One is in the simplification of the enterprise data center and the other is the transformation of the Telco industry.

Today's enterprise data centers have the usual servers, storage, networking and other hardware resources. By the year 2020, we predict that enterprise data center infrastructure will be largely simplified down to one piece: the server. Storage,



Software-defined data center vs. a software-based data center

networking and other data center hardware appliances will actually just become software running on servers. Proprietary hardware will no longer be required for most storage and networking needs.

2020 represents an inflection point where the standard hardware's advantages of cost and speed of software deployment overtake the performance benefit of proprietary custom hardware.



By the year 2020, we predict that enterprise data center infrastructure will be largely simplified down to one piece: the server.

Today's Telco networks include an even greater mix of proprietary technologies. Here too, we see these proprietary hardware appliances being replaced by software running on standard servers (and often deployed in a cloud model). In the future, carrier infrastructure might be physically indistinguishable from enterprise infrastructure as SBDC allows each to be customized via software to deliver different services.

We believe that SBDC in the Telco data center will be a 10-year journey, much like virtualization in the enterprise data center has been. Today, all Telco hardware is customized, but in 10 years, as much as 80 percent of that hardware will likely be

replaced by software on standard servers. This will be a major transformation of the Telco industry, and it will reduce capital (CapEx) and operating expenses (OpEx) for the carriers, while significantly improving operational agility. This transformation is called Network Function Virtualization (NFV) by the industry.

Dell Research has already created a proof-of-concept "High Velocity Cloud" (HVC) that optimizes standard Dell servers, networking gear, and adapters to create a solution capable of replacing proprietary telecom hardware. HVC is our unique and differentiated approach to NFV. We estimate that HVC will allow one quarter rack of standard hardware to handle all of the mobile voice, text and data traffic for a city the size of Austin (885,000 people). This is possible because HVC virtual machines (VMs) have 20 times greater capacity for handling network-intensive workloads as traditional virtual machines. HVC will also allow a workload to scale rapidly (in minutes – compared to the months it takes a carrier today to order and install new custom hardware boxes to handle growth). We expect this technology to be available and adopted by carriers in the coming years.

2. By 2017, next-generation non-volatile memory will arrive.

Flash will become the new high-performance disk and disk will become the new tape.

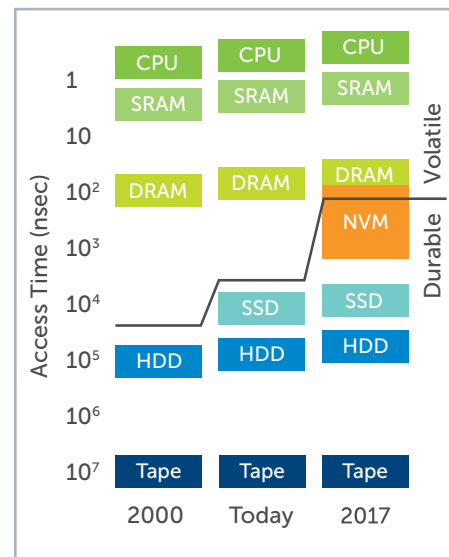
In current computers, access times for different types of data storage can differ by orders of magnitude depending on distance relative to the processor. Let's imagine it takes one second to access main dynamic random-access memory (DRAM). By that measure, it will take roughly an hour to retrieve information from solid-state drive (SSD)/flash memory. A spinning hard drive (HDD) won't complete your request for a week, and if you want to access data on a tape, it will take you the better part of a century.

This is why a clear hierarchy has emerged, with most accesses going to quick but volatile DRAM, and sluggish but durable tape being used only in the event of a disaster.

We predict that by 2016 (2017 at the latest), SSD should fully supplant high-performance (15k rpm) HDD as first-tier, high-performance storage. Slower-spinning, cost-optimized HDD will continue to grow in capacity and will approach tape costs for archival storage. This effectively shifts the hierarchy by one class, making Flash the new high-performance disk and cost-optimized disk the new tape.

By 2017, we believe that new kinds of non-volatile memory (NVM) will emerge that will be up to 50 times faster than flash. Although it will be slower than DRAM, NVM can be addressable as system memory. This will cause a paradigm shift in how

vendors will build servers, mobile devices, and the operating systems and software that run on them. Database code will also be significantly simplified, because data will no longer need to be persisted to disk.



Non-volatile memory emerges



As an example, picture an eCommerce site that is hosting a Black Friday sale. Through good luck and hard work, the sale draws four million customers who are all making their purchases at roughly the same time. Today, it isn't possible for the system to determine in real time, during this peak purchasing period, whether the credit cards being used are fraudulent or legitimate. If a fraudulent purchase is made, the credit card's owner, the bank, or the merchant will have to discover the questionable charge after the fact and work together to resolve the situation. With the new NVM, the same eCommerce site can have the ability to verify credit cards as they are used, even in high-traffic situations, avoiding the fraudulent purchase before they occur.

In addition, this super-fast, durable memory, being significantly cheaper than DRAM, will enable servers with many terabytes (TB) of addressable memory, making possible new kinds of real-time analytics, as well as new classes of applications and productivity enhancements such as instantaneous shutdown and reboot.

By 2017, we believe that new kinds of non-volatile memory (NVM) will emerge that will be up to 50 times faster than flash.

Although it remains to be seen which nascent technology will win the development race and make this new NVM a reality, Dell Research is currently examining and evaluating various technologies, including two promising candidates: phase change memory (PCM) and resistive random-access memory (RRAM). This project seeks to understand which technologies and approaches are most likely to succeed, determine how Dell servers, networking and storage products can take advantage of them, and study the implications of these technologies on future systems, workloads, and middleware and data centers.

3. By 2016, BYOD focus will shift from solely addressing security to addressing security with usability.

Mobile workforces will face fewer interruptions and limitations.



Much of the current focus concerning "bring your own device" (BYOD) has been about potential security issues created by the use of personal devices to access corporate data. However, Dell Research predicts that starting in 2016, there will be a shift from solely focusing on security to also enhancing BYOD productivity and user experience at the same time.

Currently, businesses are addressing the challenge of BYOD security by providing highly secure connections and procedures for accessing corporate networks from personal devices. The problem is that the procedures for logging in are often onerous for users, bringing productivity to a halt any time a new connection must be established.

Another common problem involves the limitations on the kinds of devices employees are allowed to use for BYOD. Some security processes are only compatible with Android devices, while other companies might only allow iOS, Windows Phone, or Blackberry. Clearly, this creates a problem of convenience for employees who have a strong preference for a device or don't happen to own the approved device. Dell Research predicts that in the future, these limitations will be removed through the development of network- and device-agnostic security processes, and that these solutions will be available to companies of all sizes.

The Dell Research **Seamless Mobility** project and our collaborators in Dell Client Systems are focused on creating secure internetworking between different types of mobile networks. For example, if an employee is using an enterprise app on her mobile device and moves from her office where Wi-Fi is available to the courtyard where only cellular is available, she will need to manually make the switch from Wi-Fi to the cellular network. Application use will be interrupted while the manual change is made, and the application must be restarted once the connection is re-established. With seamless mobility, the switch is automatically made when better network connectivity is detected, and a secure, encrypted connection is established so that the application use continues uninterrupted.

Dell Research predicts that starting in 2016, there will be a shift from solely focusing on security to also enhancing BYOD productivity and user experience at the same time.



Another way in which Dell Research is working to solve the problem of achieving both productivity and security with BYOD is through research into "Continuous Authentication." Our team is developing algorithms and leveraging machine learning to create technology for devices to authenticate a user based on a range of characteristics that are particular to that person. For instance, a machine will learn to recognize patterns in the way a user types, swipes, and interacts with it. Each person has characteristic pressures, rhythms, and gestures that a machine can use to determine, on a continuous basis, whether the

current user is the original owner of the device or someone who is not authorized to complete the requested actions. Ultimately, this research could lead to the elimination of the use of passwords.

These enhancements will pave the way for a workforce that's increasingly mobile, increasingly participatory in BYOD programs, and increasingly productive at work and home, all the while with greater security.

4. By 2016, an explosion of internet-connected devices will create new challenges and opportunities.

The Internet of Things will bring new connectivity, more sophisticated management.

Anyone who doesn't have a green thumb knows how difficult it can be to successfully grow a plant. It requires a delicate balancing act that's made more difficult by the fact that the subject can't communicate with its caretaker...until now.

The Internet of Things (IoT) has already begun to disrupt the agriculture industry on a large scale, helping farmers monitor everything from soil nutrients to cows' fertility levels. Other industries are showing signs of disruption as well, from city services' use of smart garbage cans that ensure garbage services only attend to bins that need emptying, to the aviation industry's use of smart engines that not only maintain their own ideal RPMs and temperature, but communicate service needs before landing, so the appropriate crew can be assembled and ready.

In the more immediate future, smart devices will disrupt a wide range of industries. For example, the SyFy channel is already experimenting with "light shows" that continuously adjust viewers' Internet-connected home lighting systems to enhance what's happening on their TV programs.

There are a few market factors driving this transition:

- **CPU cost is dropping dramatically, while CPU capability is increasing:** Today, it costs less than one dollar (e.g. Kinetis KL03 from Freescale) to put a 32-bit ARM processor with 2KB of SRAM and 32KB of flash into an object smaller than a dimple on a golf ball. Meanwhile, major advances in processing and storage capability enable us to store and analyze the enormous amounts of data being generated by this proliferation of smart devices.
- **Network connectivity is getting cheaper:** Cellular and Wi-Fi competition is driving less expensive networking for consumers and enterprises, making it feasible for more people to use more internet-connected devices.

- **IoT provides an avenue for product differentiation and success:** Industries that have deployed IoT devices, such as agriculture, architecture, manufacturing, and utilities, are showing better performance and business results, leading more companies to consider IoT. In addition, early entrants into the field stand to benefit from novelty and product differentiation, driving new IoT innovation.

Dell Research believes the capabilities of several of today's enterprise IT products may need to improve as much as 100 fold in order to meet the demands of IOT in 5 years.

However, we are still facing three substantial inhibitors that need to be addressed before IoT can proliferate:

1. **Security and privacy issues:** By inviting Internet-connected devices into our homes and workplaces, we're giving up a certain degree of privacy. Consumers may feel squeamish about the level of personal information utility companies, entertainment providers, and a wide range of other companies can access. In addition, while a programmable thermostat offers a great deal of convenience and potential cost savings, it also runs on open operating systems like many traditional Internet-connected devices, offering a new attack vector into the home.



- 2. Lack of standards:** Right now there are no standard protocols for Internet-connected devices. There are many different protocols in use, making it more difficult to integrate these devices with each other and protect them.
- 3. Skills and staffing:** The companies that make appliances are typically not equipped with programming engineers. This lack of extant IT staff is a hurdle for many companies that will eventually enter the IoT space.

Dell Research believes the capabilities of several of today's enterprise IT products may need to improve as much as 100 fold in order to meet the demands of IOT in 5 years. For example, current end-point device management products capable of managing 20,000 devices will need to be redesigned or enhanced to be able to manage many millions of IoT devices. As a case in point, utility company PG&E has a need to manage many millions of smart meters across California.²

A second example is one involving self-driving cars. If the 13,000 taxicabs in NYC were all self-driving, at 1 Gbit/sec per self-driving car, 13 Tbits per second or 26 Exabytes of data per year would be generated.³ Current storage and data analytics solutions will need to be significantly enhanced to support the requirements of an application like this. At the same time, it will be necessary to create new architectures that process more of the data nearer to the IoT device and eliminate the need to send all the data to the cloud. Furthermore, current networking and security products will similarly need to be enhanced to tackle IoT.

Dell, too, must rise to the challenge by scaling its current management, security, networking, data storage, and data analytics technologies to IoT levels. These are the challenges that Dell Research is tackling.

5. By 2018, user interfaces will evolve to understand more about user intent.

Personal devices will get smarter and more sensitive.

Devices are becoming more and more sensor-rich, and more capable of understanding the context of the user's environment. For example, before mobile phones included GPS receivers, users had to enter locational information when searching for area restaurants or other recommendations. With the addition of GPS, smartphones now automatically infer the user's intent from the context of their current location to find restaurants in the immediate area and display recommendations accordingly.

Dell Research predicts a new wave of technologies will arise to divine user intent by 2018, making the connection between the personal device and the user more fluid and natural. In particular, we predict it will become possible to learn more about the emotional state of a user, measuring and responding to user levels of attentiveness, stress, happiness or interest.

Dell Research is experimenting with technologies to determine a user's emotional state using voice tone, signals from consumer-grade brain-computer interface (BCI) devices, and cameras.

The results of this research will have important implications for the workplace, such as safety and productivity. If a chauffeur or taxi driver's vehicle senses the driver has begun to doze or lose concentration, it can potentially alert the dispatcher and have the driver's next fare reassigned. If a worker is deep in concentration, the system could suppress incoming emails, instant messages, and phone calls that might break the user's focus.

Dell Research predicts a new wave of technologies will arise to divine user intent by 2018, making the connection between the personal device and the user more fluid and natural.

There are recreational and educational implications as well. If a game recognizes that a player is growing bored, it can ratchet up the challenge level. Similarly, a teacher would be able to tell how well he or she is keeping the class engaged, and then experiment accordingly with different teaching methods.

In collaboration with partners, Dell Research and Dell Client Solutions demonstrated some of the possibilities of emotional state detection at TEDx Amsterdam 2014. Visit dell.com/TEDx to see the resulting "emotional track" for each TEDx talk, showing attention levels, attentiveness, and audience demographic information.



6. By 2020, analytics will evolve from descriptive to predictive to prescriptive faster than anticipated.



Analytics will become central to decision making.

As a society, we're gathering a great deal of information about ourselves: how our projects are performing, who our customers are, how many people are visiting our websites, which customers like our social media posts, how many steps we take, even how we're sleeping. We've become adept at creating graphical representations that boil this data down into easily digestible facts that describe what's going on.

However, using analytics in this way is only the first stage of three we expect to unfold as the data revolution continues to move from descriptive (tell me what is going on in my business) to predictive (tell me what will happen next in my business) to prescriptive (tell me what to do about it) analytics.

Dell Research believes that the compounded effect of faster hardware, cheaper storage, and greater amounts of data available to be analyzed, combined with improved machine learning algorithms for analytics, will cause exponential improvements in analytics capabilities.

There are three factors driving this evolution:

1. Improved server performance and cheaper storage capacity are enabling increasingly complex data to be stored, analyzed and delivered in real time.
2. Analytics and machine learning algorithms are being continually improved and applied to new business domains against ever increasing amounts of data.
3. Enterprises are recognizing the competitive imperative to not only gather data but harness it to improve operations, strategy and customer experience.

Dell Research believes that the compounded effect of faster hardware, cheaper storage, and greater amounts of data available to be analyzed, combined with improved machine learning algorithms for analytics, will cause exponential improvements in analytics capabilities. This will drive the industry toward greater use of advanced analytics faster than most people predict.

These advanced analytics will certainly have monumental implications for the corporate world, but also for doctors and lawyers, where predictive and prescriptive analytics can reduce human error and/or lead to much greater efficiency and efficacy in practice.

Dell Research is currently working on projects that apply predictive and prescriptive analytics to healthcare. With our partners in Dell Information Management, we are building a **Healthcare Computational Lab** with a HIPAA-compliant data sandbox, along with a set of healthcare research tools that serve as models for prediction and mitigation of hospital 30-day readmission risk, and for medical image analytics.

7. By 2020, the majority of real-time data analytics will be seamlessly integrated into business processes.

Analytics will become democratized, instantly applicable and easy to consume.

Many companies rely on an analytics department to pull data, analyze it and give feedback on its implications. These analysts might operate inside marketing, sales or operations, but they are usually specialized and distinct from other business personnel.

Leading companies are integrating analytics into their business processes and applications, making reporting more accessible to personnel directly affected by the data being produced. An

increasing amount of analytics capabilities will be embedded within applications, making it possible for users to have the information they need to make smarter choices at the time of transaction.

Going one step further, Dell Research believes the majority of systems in 2020 will incorporate data analysis recommendations into business processes, without the need



for human oversight. This closing of the loop between analysis and action will give companies the opportunity to become more effective and efficient on a daily basis. Furthermore, as analytics prove to be trustworthy over time, decision making will become a much quicker and more streamlined process.

Just as Dell is focused on democratizing technology to improve people’s lives, Dell Research wants to ensure that easily consumable analytics is available to businesses of all sizes, not just the data scientists and large corporations of the world. However, we understand that even when easy-to-use predictive and prescriptive analytics are available, some businesses – especially small businesses - might not generate enough data to yield conclusive results. To provide every business with “big data” business opportunities, Dell Research is exploring possible research projects that could use a cloud-based service to anonymously pool data from multiple small businesses in order to provide to each small business the same level of analytics that larger corporations are able to achieve.

Dell Research believes the majority of systems in 2020 will incorporate data analysis recommendations into business processes, without the need of human oversight.

Real-time analytics integrated into business processes

Capability	Descriptive <ul style="list-style-type: none"> Describe what occurred Hindsight 	Predictive <ul style="list-style-type: none"> Predict what will occur Foresight 	Prescriptive <ul style="list-style-type: none"> Advise future action Control
Latency	Slow	Fast	Real time
App integration	Standalone Separate system	Inline Analysis integrated as advisory	Infused Analysis embedded in workflow

8. By 2018, security will shift from reactive to predictive and become context aware.



Enterprises will be able to predict, and possibly prevent, both external and insider attacks before they happen.

If we think of network security the same way we think of home security, it breaks down into three levels of preparedness: reactive, proactive and predictive.

- 1. Reactive:** We can think of enterprises that rely on reactive security procedures as analogous to the person who changes the locks after his or her house is burgled. Today, many enterprises only know they should modify their firewall settings after they’ve been breached, helping to stave off future attacks but remaining helpless to deal with the one that’s just occurred.
- 2. Proactive:** Proactive security could be likened to a person who changes the locks after a neighbor’s house is burgled. In

the near future, enterprises will be able to more proactively monitor their firewalls across the infrastructure, and adjust settings as needed. If suspicious activity begins to occur within firewalls in a specific region or country, the company can change their firewall settings across the enterprise. Dell security products such as SonicWALL and SecureWorks already provide some forms of proactive security.

- 3. Predictive:** If a person could predict that a burglary was imminent, they could change the locks preemptively. Alternatively, if a person can detect the attack as it is happening, like hearing the clicking sounds of someone trying to pick your lock, they could prevent the attack by denying the access. In the future, predictive security will



Dell Research foresees a shift to predictive security by 2018, and also believes that security systems will leverage awareness of user context and user intent by then.

enable enterprises to detect and respond to threats before attacks or insider breaches occur. Predictive security systems will use algorithms to predict an imminent external attack by recognizing unusual, irregular or suspicious access patterns of employees, such as an access from Russia by an employee who lives in California. This would allow an organization to deny the access.

Dell Research foresees a shift to predictive security by 2018, and also believes that security systems will leverage awareness of user context and user intent by then.

9. By 2019, cloud security will be strengthened by homomorphic encryption.

Operations will be completed against encrypted data.

Although adoption of cloud computing continues to advance, security remains a primary concern and barrier to adoption. Today, even though the cloud is used to store a wide range of data, organizations typically have reservations about sending their most sensitive information into the cloud.

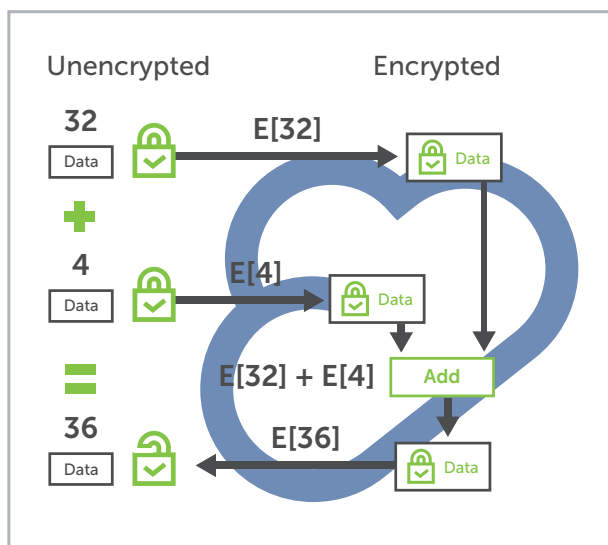
Encryption can be used to protect sensitive data, but systems running in the cloud must decipher the data in order to make use of it. The keys for decryption will exist in the cloud, making even the stored data vulnerable. Furthermore, demonstrations have shown exploits capable of reading deciphered data in server memory.

Homomorphic Encryption (HE) has emerged as a technology that has the potential to solve this cloud security problem, as it enables enciphered data to be used for calculations without requiring decryption or a key.

Dell Research believes that Homomorphic Encryption could become practical by 2019 through improved algorithms, faster processors, and hardware accelerators.

For example, many consumers rely on cloud-based tax preparation services each year. Today, the user is forced to provide sensitive personal information, such as salary and Social Security Number, which is encrypted before being sent to the tax preparer. Then it is decrypted in the cloud when calculations are performed, exposing the data. Homomorphic Encryption will enable the tax service provider to run calculations without ever decrypting, exposing, or even knowing this sensitive information. The tax service will never have the decryption key. Once the calculations are complete, the encrypted results will be sent back to the consumer, where they will be decrypted using the original key.

The first fully homomorphic encryption scheme was developed in 2009. Since then, the methods have been continually improved. This is still not practical today because the computations take far too long. However, over a period of five years, HE speed has improved by a factor of nine million. (See the paper by Lianlinag Xiao, Osbert Bastani and I-Ling Yen "An efficient Homomorphic Encryption Protocol for Multi-User Systems"⁴). Dell Research believes that HE could become practical by 2019 through improved algorithms, faster processors, and hardware accelerators.



Using data in cloud without a decryption key



10. By 2017, there will be a paradigm shift in Data Loss Prevention (DLP) to self-protecting data.

Policy and enforcement travel with the data.

Even within the most transparent organizations, sensitive data exists that should not reach the public eye. Whether it is credit card information or trade secrets, proprietary data is typically protected in two ways:

- **Software:** Many organizations use firewalls and Data Loss Prevention (DLP) software to recognize sensitive information and keep it from leaving the company.
- **Policies:** Ultimately, much of the responsibility for preventing data leakage falls on employees, who are required to maintain caution and propriety when sending files to outside parties.

Dell Research predicts a significant shift in the DLP paradigm to self-protecting data, where the policy, enforcement, and encryption mechanisms will be tightly bound to the data. By 2017, data that has left the enterprise will still be able to be controlled and protected. If it lands in the inbox of an unauthorized user, a policy code that exists within the file will instruct the file to remain closed to everyone except authorized users. Ex-partners or ex-employees who possess data protected in this way can be retroactively de-authorized. Data enciphered

with weak or compromised keys can be dynamically re-encrypted in the field.

This shift toward self-protecting data will reduce reliance on limited functionality DLP software and policies without enforcement mechanisms.

Dell Research predicts a significant shift in the DLP paradigm to self-protecting data, where the policy, enforcement, and encryption mechanisms will be tightly bound to the data.



Predictions in Motion: A Day in Healthcare 2020

Imagine the year is 2020. A once-emerging healthcare provider has become a major global player, in part thanks to a popular health-tracking device it pioneered.

This provider operates a large, cloud-optimized data center where the company stores and processes data about their customers. In its earlier years, circa 2015, this data center ran on standard servers, storage devices and networking boxes, each of which were managed using software. However in 2020, the provider uses only servers, with storage and networking provided as software functions on servers. These servers feature a new generation of non-volatile memory (NVM) that enables the health-tracking device to access and reliably store data in real time.

The health tracking device reads a number of bio-indicators for its wearer, including blood pressure, pulse, temperature, activity and even stress, as detected in the wearer's movements and voice. Device owners can monitor these health signs using simple and approachable graphic representations.

Occasionally, the device sends the wearer's data, using homomorphic encryption for anonymity, to a cloud-based app so that it can compare the data to other data sets from the larger population. Should the app detect a rise in complaints of flu-like symptoms, for instance, it will correlate that with other external data sources such as the Centers for Disease Control database and publish an alert to users to be on the lookout for the specific symptoms.

Given that the device is aware of each user's personal health indicators, the app can go a step further and notify users in whom it detects those same symptoms. At that point, the data center will also analyze users' allergies, current medications, congenital issues, genetic profile and medical history to develop personalized treatment programs for each, complete with prescriptions and dosage. A simultaneous business process orders the medicine the device has prescribed and ships it to the users with tracked delivery.

Conclusion

The next five years promise exciting times in human history, holding the potential to usher in new technologies that will make us smarter, more productive, and possibly healthier. At the same time, these technologies will free up more time for us to focus on the aspects of our lives that we find truly meaningful.

As Dell Research and the entire Dell community stride forward into this extraordinary new era, we look forward to continuing to work with our partners, customers and contemporaries to reach new achievements in innovation at the intersection between what is possible and what is practical.



About Dell Research

Dell Research was formally established in 2013 to focus on organic, long-range, disruptive innovation across the company to complement and expand upon the development taking place within Dell business units. Led by Chief Research Officer Jai Menon, the team is charged with identifying and examining industry trends, and deciding which to pursue based on Dell's customer imperatives of transform, connect, inform and protect.

More specifically, Dell Research invests in projects that have the potential to impact Dell, its customers, partners and/or the industry at large in one of four ways:

1. Make an existing solution better
2. Develop a new solution
3. Create a new line of business for Dell
4. Advance and participate in the development of industry standards

For many organizations, research is considered successful when it leads to a published paper. For Dell, a research project is considered a success only when it becomes a solution that meets customers' needs. Menon's goal for the team is for 60-75 percent of Dell Research projects to successfully lead to products for the Dell line. Any fewer, and the team would need to reexamine its approach, but any more, according to Menon, would indicate a lack of imagination and risk-taking in their project selection.

The Dell Research Collaborative Approach

Dell works closely with customers to learn about their changing needs to determine how technologies might provide

solutions. Believing that collaboration leads to better ideas and information, Dell Research actively invites participation and input from passionate team members throughout the Dell organization. Dell Research also augments its organic research with an extended external community, including alliances with universities such as University of Southern California and University of Houston, to leverage their deep technical expertise and wealth of knowledge for the benefit of Dell customers.

Practical Innovation

Dell has always been a listening company. Part of our innovation story includes ongoing, direct conversations with customers on a daily basis, through account execs, support services, or active social media outreach programs. We continuously receive feedback on the needs of our customers. Dell uses knowledge of our customers to drive products and solutions. Dell Research relies on customer knowledge to direct our research for new product innovation. The reward is that customers get a lot more value from Dell's investment dollars because our innovation focus is relevant and practical.

To learn more about Dell Research, visit dell.com/dellresearch

¹ <http://www.dell.com/learn/us/en/555/dcm/storage-iscsi-san>

² http://www.pge.com/about/newsroom/newsreleases/20120515/pgampe_reaches_major_milestone_installing_9_millionth_smartmeter.shtml

³ <http://www.kurzweilai.net/googles-self-driving-car-gathers-nearly-1-gbsec>

⁴ <http://eprint.iacr.org/2012/193.pdf>

This white paper is for informational purposes only, and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

