INTRODUCTION

It's an exciting time in the technology industry for enterprise chief information officers (CIOs). The role of the CIO is evolving rapidly as new innovations are constantly being developed and businesses around the globe increasingly rely on technology to power their business. IT departments are assuming new responsibilities across customer acquisition, customer experience, and brand loyalty as digital engagements continue to overtake traditional interactions. In this age of the modern digital business, CIOs are expected to become more proactive and strategic, instead of reactive and static. CIOs have an opportunity to not only define and enable business goals but also lead digital transformations within the enterprise.

There are challenges CIOs face daily though. Security is top of mind for any CIO as the threat landscape continually evolves. The number of users and devices is growing exponentially, thanks to a world of interconnected devices dubbed the Internet of Things (IoT). Mission-critical applications that used to be hosted in datacenters are increasingly being accessed in the cloud, creating a need for higher-bandwidth, lower-latency connections.

As CIOs consider how to prepare for this world, many are increasingly thinking about the need to graduate from silo-based management of disparate resources into a more holistic management that covers multiple integrated domains. The datacenter, campus, cloud, and IoT can no longer be managed separately. Security, applications, and users cannot each have their own siloed management approaches. Doing so creates insecurities and inefficiencies. A multidomain architecture (MDA) that stretches across all of these functional aspects of the modern digital business should be managed cohesively.

This white paper explores the challenges CIOs face daily and how IT leaders think about solving them. It explores the frameworks for multidomain architectures and how organizations have successfully implemented them. While it's an exciting time in the IT industry, it's also a time of transition when CIOs need to consider whether the IT systems in place today are truly meeting the needs of the business, both now and into the future.
CIO Pain Points

CIOs currently face a variety of challenges that are unique to the way modern digital businesses operate. These pain points have evolved significantly over the past few years, driven by the rise and mainstream adoption of technologies such as cloud computing, ubiquitous mobile connectivity, and big data and analytics. Addressing these pain points requires a new way of thinking that allows the IT department to serve the needs of the business for both today and into the future. Some of the challenges are:

- Users, both internal (employees) and external (customers), demand high-quality IT resources. There is an expectation for always-on connectivity, ample bandwidth to serve any application or use case, and instantaneous response times. Users want to access a wide variety of applications and have them customized to their individual needs. If internal users don't get these resources from IT, they will turn to shadow IT. If customers are not delighted by technology, the business risks losing them.

- The enterprise IT environment is broader than ever. IT is no longer centralized to a datacenter; the rise of cloud-based platforms for mission-critical applications has decentralized IT architectures across many different locations and applications. IT resources extend from the datacenter to the campus, out to the branch, into the cloud, and to the edge. Applications that enterprises rely on for mission-critical tasks may be hosted internally in physical, virtual, or containerized infrastructure or externally on public, private, or hosted clouds. CIOs must be able to support all the application and infrastructure needs the business requires to compete and win in this digital-first world.

- Too often, IT systems are managed by manual, ad hoc systems. The lack of standardized operating principles leads to inconsistencies across performance and security and the ability to meet the needs of the business. Disjointed management creates slower, less agile organizations that are not able to respond to the fast-paced changes of a modern digital business.

- Attracting and retaining talent while building innovative teams, both inside IT and across the broader business, has also emerged as a key challenge. Finding highly skilled employees with the talents necessary to execute in today's modern technology environment is difficult. Ensuring they are productive requires that employees are given training that allows for constant learning of new skills, leading to their own advancement and higher levels of job satisfaction. Underpinning all of this is the need for cutting-edge technology that allows workers to be their most productive.

Security in a Complex Threat Environment

Perhaps the most prominent CIO pain point, and priority for the business, is security. Securing a digital enterprise is more complex than ever. As users and applications have become distributed, the attack surface has expanded. Other security-related challenges include:

- Mobile workers connect from anywhere to a wider variety of endpoints, both those located on premises and off premises. This makes perimeter-based security platforms ineffective.
  - Organizations must transition to a multipronged security fabric that includes identity and role-based policies that follow users wherever they go.

- Multicloud usage is standard, with unique challenges and operational concerns for each cloud-based system. CIOs should enable the appropriate use of cloud-based services, but managing the disparate security settings for each one is a complex task.
  - Having a security fabric that is centrally controlled but is able to extend to any endpoint — on premises or off premises — is key to enable secure and efficient use of cloud-based services.
There is a greater need for continuous operations. Modern digital businesses rely on IT resources as the lifeblood of the company. Performance degradations, security breaches, and downtime equate to decreased productivity, lost revenue and, potentially, brand-damaging publicity.

CIOs must consider how to ensure resiliency, with disaster recovery, backup, and always-on operations, no matter what happens. This requires a unified management fabric that is able to continue working even if some aspects of the system go down.

All of these challenges must be addressed during this age of nefarious actors increasingly using automated and sophisticated attack vectors, creating a threat environment that is constantly changing. To help solve these challenges, organizations should not go at it alone: rely on experts in secure monitoring and operations whose sole job is to stay on top of an ever-evolving landscape of threats.

**Embracing Transformation**

While the challenges facing the modern CIO are varied and daunting, there is a significant opportunity if these can be addressed; doing so requires a new way of thinking. Too often, IT has been constructed with a silo-based approach. There are teams that manage the datacenter and others for cloud-based services. Security controls are pervasive but not well integrated into the environment. Newer technologies, such as a range of connected devices, have been patched into this environment with varying degrees of policy controls. That's not to mention the shadow IT resources that are sometimes rampantly used across the business.

The landscape for supporting users, both internal to the business and external, customer facing, has evolved significantly. Users expect always-on IT resources, with elastic scalability, cloud-sized capacity, and frictionless operations – and, most of all, simplicity. New applications pop up every day, most of which are not developed internally, but rather hosted in some cloud. A global sales force and supply chain need to be able to respond to any business opportunity in any corner of the world. IDC survey data reinforces these trends. Figure 1 shows the top goals surveyed organizations are looking for from technology investments.

**FIGURE 1**

---

**Top Business Goals from Technology Investments Over the Next Five Years**

**Q.** What are the top 5 goals for your business over the next five years?

<table>
<thead>
<tr>
<th>Goal</th>
<th>(% of respondents)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Innovate or deliver new products or services</td>
<td>31</td>
</tr>
<tr>
<td>Invest in research and development</td>
<td>25</td>
</tr>
<tr>
<td>Deliver digital products (versus physical products)</td>
<td>24</td>
</tr>
<tr>
<td>Improve marketing of products and services</td>
<td>23</td>
</tr>
<tr>
<td>Expand geographically</td>
<td>23</td>
</tr>
<tr>
<td>Hire quality/talented staff</td>
<td>19</td>
</tr>
<tr>
<td>Compete aggressively to increase market share</td>
<td>19</td>
</tr>
<tr>
<td>Improve products and processes</td>
<td>19</td>
</tr>
</tbody>
</table>

n = 401

Source: IDC's IT Strategy and AI Adoption Survey, February 2019
The Power of Multidomain Architectures

In an interconnected world, there must be an interconnected plan to address the aforementioned CIO challenges. The scale and complexity of operations requires organizations to graduate beyond manual, ad hoc management of resources and toward automated platforms that stretch across multiple domains in an integrated and increasingly automated way. These systems should be aided by machine learning (ML) and artificial intelligence (AI) and provide deep levels of visibility and analytics into everything happening in the IT environment. This multidomain architecture should provide centralized control, no matter where the resources are that are being managed. Instead of IT being a roadblock preventing exciting new business opportunities, CIOs have an opportunity to become an agent of transformation within the enterprise.

There needs to be buy-in for this transformation from all levels of the organization. From executives at the C-level to the teams that manage day-to-day operations. Having a centralized goal of embracing a new way of thinking and architecting the IT system will ensure everyone is on the same page.

One of the paramount challenges to enabling digital transformation (DX) is the inertia of maintaining the status quo. It can be easy to rest on laurels, to solve pointed problems, and be reactionary. To enable an IT system that is transformative and helps the business grow requires CIOs to consider broader solutions that extend beyond individual silos.

How to Execute a Multidomain Architecture

To execute these priorities requires CIOs to consider a holistic approach. There must be alignment between IT and the business and integrations across technology domains. Teams within the IT department must work together rather than in silos. Technology solutions should enable the sharing of valuable data and insights across domains to ensure efficient and secure operations. Four critical areas that CIOs should consider focusing on to enable this transformation are discussed in the sections that follow.

Security

- Take an identity-focused approach. Rather than securing the business at the perimeter of the network, a zero-trust model should be adopted that ensures every user, device, application, or thing is accurately authenticated with consistent policies that stick with that asset no matter where within business it traverses.
- This identity-based approach should be highly integrated across all domains in which IT oversees. Centralized policies should be set once and executed throughout the organization, no matter where the resources are, including the datacenter, the cloud, or any other hosted resource.
- Tools are needed to allow for deep levels of visibility and analytics, powered by machine learning and artificial intelligence algorithms that allow security vulnerabilities to be identified and resolved quickly.

Infrastructure

- Enterprises utilize a variety of infrastructures today, some on premises, some off premises. There are also a variety of physical, virtual, and containerized infrastructure stacks to support. Relying on manual processes for configuring and managing infrastructure at the scale required by digital businesses leads to inefficiencies and a lack of agility. All parts of the infrastructure should be managed through automation software.
- When those automation platforms are enhanced by machine learning and artificial intelligence algorithms, they become powerful platforms that allow for intent-driven infrastructure. Infrastructure operators simply dictate their intent of what they want the infrastructure to do, and the software management platform is intelligent enough to automatically configure it and maintain that policy even as conditions within the environment change.

- The network plays a pivotal role in enabling this functionality. All the technologies that digital businesses rely on, from cloud computing to ubiquitous mobile connectivity, require a robust network connection. The network becomes a centralized platform connecting users and devices to all of the infrastructure and applications they need to access. Automating the operations and management of these connections is critical to ensuring scale and security.

- Automation should be a journey though. Consider first automating mundane manual tasks that free workers to focus on business-enabling tasks rather than "keeping the lights on." Rely on data to ensure processes are automated correctly. And automate with purpose; don't view automation as a way to reduce head count, but rather as a way to make teams more efficient and focus on higher-level tasks.

**Applications**

There is a wide diversity of applications that enterprises rely on to run their daily operations and serve their customers. CIOs have a variety of priorities:

- Monitor application performance to ensure all applications are running smoothly. Performance degradations lead to unhappy users, so they should be identified and resolved using automation techniques as fast as possible. Doing so requires having an interconnected system that allows for the root cause of the problem to be identified quickly, and a fix to be implemented automatically.

- Create an environment where new applications can be developed efficiently, deployed quickly, and scaled dynamically. For applications not developed internally, the job of the IT organization is to allow for secure connections to them, whether they’re hosted in a partner datacenter or the public cloud. When employees do use cloud-based resources, every transaction should be logged and tracked in real time to ensure it meets rigorous standards. IT teams that do not allow their employees to use the applications they need to do their jobs efficiently will find themselves instead dealing with shadow IT.

**Teams**

- While IT operations can increasingly rely on automated systems, the people that make up a business are still any enterprise’s most critical asset. It's the job of the IT organization to ensure connectivity and encourage collaboration between and among employees, customers, and partners. A modern digital business should enable this communication across any medium, in real time.

- Talent should be sought after and deliberate efforts should be made to delight them. On-the-job training and career development are important to attracting and retaining top quality talent.

- IT departments also have an opportunity to remove barriers to innovation and enable agility of the workforce by providing flexible consumption models that empower innovation and rapid development. Having the right tools in the right place, on demand, exactly when they’re needed will allow the next big idea to be created and executed on today rather than budgeted for next year.
The Value of Visibility and Analytics

There are a variety of overarching themes that CIOs should consider as they look to execute on a multidomain architecture. One is to have deep levels of visibility and analytics across the entire IT landscape. This critical information is used for a variety of tasks:

- At a basic level, understanding what is happening within the network is the first step toward ensuring it is performing the way that it should be. Performance degradations should be identified and resolved as quickly as possible. Instead of waiting on a user to report an issue, visibility platforms should be able to automatically recognize problems.
- The next step beyond recognizing the problem is automatically solving it; this is known as a closed-loop system. IT management platforms that are strongly integrated with a visibility platform will be able to quickly determine the root cause of the problem, identify what changed that caused the problem, and automate a fix to resolve the problem, hopefully before any user is impacted. This same logic is applied to security breaches and vulnerabilities.
- At a more advanced level, visibility and analytics insights can be used as foundational information for automating and securing the IT environment, both on premises and off premises. Getting detailed levels of analytics into what's happening across the environment is key toward understanding the history of operations and, specifically, learning what is normal and abnormal behavior.

Enhanced Visibility with Machine Learning and Artificial Intelligence

One of the most exciting advancements in recent years has been the advent of machine learning and artificial intelligence platforms that can be integrated with visibility and analytics platforms. The more data ML/AI platforms have to work with, the better they become at increasing agility of operations. Visibility and analytics platforms create large amounts of data, making this an ideal use case for ML/AI algorithms. When that data is fed into ML/AI systems, the automated platforms learn what "normal" behavior is. Abnormal behavior, or anomalies to that normal behavior, are automatically flagged, investigated and, potentially, automatically resolved. This is a workflow that can be executed across any domain of the IT system.

At the end of the day, it all comes down to having detailed levels of visibility and analytics as the base for enabling ML/AI systems. Visibility becomes a critical, foundational element of a modern IT system: After all, enterprises can't protect, or automate, what they can't see.

Multidomain Architectures

IT management must span across traditional and emerging domains that businesses rely on. Silo-based management of these resources leads to inefficiencies and an environment that's more vulnerable to attacks. CIOs should aim for an IT system that integrates visibility and analytics across all areas of the IT stack, with centralized policy and automated processes. This allows for standardization of operations and improvements in uptime, capacity, and resiliency, and it creates a secure and scalable IT department that's ready to meet the needs of the business both today and into the future. Increased agility fosters innovation and allows businesses to outpace competition.
This multidomain architecture has a handful of key tenets:

▪ Multidomain integrations should extend across all aspects of a modern IT system, from internally controlled resources (datacenter) to external (public cloud), and the growing world of IoT-connected devices.
▪ All types of applications should be supported, both those hosted internally and applications that internal users and external customers may access from cloud-based resources.
▪ Onboarding new users, devices, applications, and things should be a clear, simple process that ensures frictionless operations for users. Once authenticated, the user's identity-based access and control policies should follow them wherever they traverse within the IT system.
▪ A security fabric should extend across all areas of this multidomain architecture and ensure that only authenticated users and traffic enter the environment and are micro-segmented to ensure that if any unwanted activity is detected it can be quarantined and eliminated.
▪ Detailed levels of visibility and analytics should show what is happening across all domains of the system, at a high level for macro views and with the ability to drill down into the individual application, user, or device level to ensure security and high-quality performance.
▪ A management platform should extend across all domains of the architecture, integrated with ML/AI capabilities to automatically resolve issues (performance or security related) before they impact users or cause harm within the environment.

Benefits of Multidomain Architectures

Multidomain architectures create a variety of benefits, not just for the CIO but also for the broader business, users, and customers. There is great variety in how far along organizations are in this journey. Figure 2 represents IDC's survey data showing what percentage of organizations are at various stages of their digital transformation journey. Those that achieve the higher ends of this scale reap significant benefits, including:

▪ Operational experience for users is simplified. Automated systems create agility, allowing workers, both inside IT and across the broader business, to focus on business-enabling tasks rather than mundane, repetitive tasks.
▪ Workers and teams receive high-quality user experiences that are ensured by automated platforms that automatically resolve issues before they impact any user.
▪ IT becomes an enabler of new business opportunities rather than a roadblock. If teams within the organization want to use a new application, deploy a new site, expand to a new geographic location, onboard a new customer, or take up any other task, IT should enable rather than inhibit that task. Doing so requires a centralized system that extends across all aspects of the IT environment.
Customer Case Study

Enterprise customers that have embraced multidomain architectures have yielded significant benefits. One such company is BBVA, a global financial institution headquartered in Spain. About five years ago, the company made a big change: "We launched a major transformation project that aimed to move our technology stack to something completely different," says Ignacio Bernal, Global Head of Architecture and IT Innovation, BBVA. This was no small feat: The company holds $790 billion in assets and has 77 million customers, 125,000 employees, and 7,700 branches, and it operates in 30 countries.

"We were very traditional from an IT perspective," Bernal explains. The company had a mainframe in its headquarters for core banking, but most technology was managed at a local level. This fragmented, silo-based approach created inconsistencies and inefficiencies: Employees across the globe were working off different systems; there were no common operations, and customers got different experiences depending on where they interacted with the bank.

A variety of factors led Bernal and his team to consider a significant transformation of their IT. For one, the bank's chairman and CEO laid out a vision for the bank to expand globally. Bernal wanted to create an efficient process for expanding globally that would scale up with future success while transforming existing operations too. There was a bankwide desire to expand the company's mobile banking app from where it was (initially only available in the headquarter country of Spain) to be available in every country where the bank operates. The bank's existing technology didn't support mobile-first architectures.
everywhere it operated, however. Bernal also wanted to move faster: from an average development time of new app features from six months to one month. "It was a very complex process," he admits.

Bernal began organizing an effort to centralize operations, reorganize teams, and embrace a more agile operational model. One of the biggest keys to success has been to more centrally manage global IT operations. Bernal doesn't think about the bank having multiple IT systems in each of the local regions where it operates: there is one IT system that stretches across the globe. Bank workers can centrally manage, optimize, automate, and monitor the platform.

Another key to success, Bernal says, was choosing a few key technology vendors to work very closely with. Instead of traditional RFP processes for pointed solutions, BBVA chose to work with strategic partnering vendors. By doing so, BBVA IT employees worked side by side with vendor engineers and architects to implement standard practices. Some other success factors are:

- Executive-level support throughout the entirety of the project
- Ambitious but a clear long-term vision with concrete deliverables aligned to KPIs
- Building a platform that will allow BBVA to innovate in the future
- In-sourcing talent while creating partnerships with a handful of key vendors with broad portfolios and the experience and capability to support integration objectives, including Cisco

Since implementing the changes, BBVA has realized significant benefits and has been recognized with numerous awards for its mobile and online banking. The global IT platform is now powering the bank's global operations. Since the project began, the company has tripled the number of transactions it processes while reducing the overall cost of operating the IT resources by about 20%.

**Cisco's Multidomain Architecture**

Cisco's multidomain architecture is a modern playbook for CIOs to reinvent current IT practices so that they better align to the requirements of digital business. The goal of Cisco's MDA is to enable organizations to deliver a set of consistent and frictionless digital experiences that connect users, apps, devices, and networks securely. At the core of Cisco's MDA are cross-domain integrations that are implemented across infrastructure, into the cloud, and with third-party ecosystem solutions. Policy is integrated between these domains, allowing for each domain to function independently and retain its uniqueness while enabling essential consistency and management across those domains. Cisco layers assurance integrations across the domains, allowing IT and business intent to be expressed in one domain and then exchanged, enforced, and monitored across all of them. Cisco's MDA not only represents a strategic road map for IT organizations to remain relevant but also provides a platform for leading digital transformation of the enterprises in the multicloud era.

**Challenges**

Organizations around the globe are at varying stages of their digital transformation journey. One of the biggest inhibitors toward greater levels of transformation is a lack of coordination within the business about goals and objectives of a DX project: It's critical that CIOs are able to marry the needs of the business with any investments in new technologies. Another challenge is the inertia of the status quo. It can be easy to rest on laurels, maintain systems and, generally, focus solely on "keeping the lights on." IDC believes that enterprises that take this approach will be left behind as more enterprises around the globe pursue digital transformation efforts. It's essential that vendors such as Cisco aid organizations through these challenges to focus on business-enabling innovations.
CONCLUSION

Fundamentally, the role of the CIO has changed. CIOs and the IT resources they control don't just have an opportunity, but they have a mandate to become enablers rather than a roadblock. Doing so requires strong alignment between IT systems and the broader business. The scale and complexity of modern digital businesses necessitate that IT systems be centrally controlled across multiple domains. Ensuring that operations, infrastructure, and applications and the teams that create, support, and run these systems are all transformed is an integral part of any transformation project too. IT departments are no longer just a cost center within a business; they have an opportunity to be the engines of digitally transformed enterprises.

It's the task of CIOs to enable this transformation by fostering alignment between the business and technology and by ensuring the necessary resources are in place that allow for integrations. This is the CIO's imperative: Create a technology environment that enables the business to win new customers, attract and retain talent, serve existing customers, and operate in an efficient and secure manner. Bringing resources together under a common multidomain architectural framework will ensure that IT systems are built to serve not just the needs of businesses today but any needs into the future too.
About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data – Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2020 IDC. Reproduction without written permission is completely forbidden.