INTEGRATING INNOVATIVE TECHNOLOGIES FOR SUCCESSFUL DIGITAL TRANSFORMATION
Transforming Infrastructure, Workforce and Security to Thrive in a Digital World

We are in the midst of a technology revolution. Whether an organization was born in the digital age or is remaking itself in it, digital transformation persists as innovation continues to disrupt the market.

Digital transformation is the transition of an organization’s technology, culture and processes to take advantage of a digital world. Innovation plays a role in building or accelerating digital transformations. With the underlying architecture in place, optimizations leveraging collective data and computing allow organizations to move with the market.

Cloud adoption is paving the way for emerging technologies such as blockchain and artificial intelligence (AI), in particular machine learning, to reinvent policies, practices and experiences. Integrating technologies that build and accelerate digital infrastructure, workforce and security transformations will enable secure digital engagements that allow organizations to thrive in a digital world.

Building Secure Digital Engagements

Digital initiatives connect customers, partners, employees and things in a new borderless IT ecosystem. But as organizations rapidly adopt digital capabilities, the cyberattack surface expands. The ability to secure digital engagements—person-to-person, person-to-machine and machine-to-machine—is fundamental in a dynamic online environment.

When organizations build a platform to drive digital business initiatives, security cannot be an afterthought. Cloud technology provides an adaptable infrastructure that accommodates innovation. It also delivers anytime, anywhere access, enabling a multitude of devices and users to connect to critical enterprise data and assets.

The previously accepted notion that systems and traffic within a data center are safe is not realistic in the cloud. Static privileges are insufficient in a digital environment where access must be modified based on changing roles, devices or locations. A new approach to cybersecurity that never assumes trust is required to address ever-evolving threats.

Infrastructure Transformation

Moving to the Cloud

The platform to support digital transformation resides in the cloud. Cloud technology supports the components of digital business—strategy, culture, processes and engagement—and enables them to succeed.

Successful migration to cloud infrastructure, applications and services is essential to the digital transformation journey. Not only do organizations immediately tap into resource elasticity, but they also gain access to an API-flush ecosystem that allows digital business interactions.

Once data and applications are in the cloud, ubiquitous interconnectivity is possible between businesses, people, places and devices. The shift from local desktop office suites to cloud-based productivity tools adds collaborative file sharing with enterprise social networking capabilities. Easily constructed workflows with embedded security governance support operations, rather than inhibit them.

Workplace Transformation

Enabling Anytime, Anywhere Access

The workplace is transforming in the cloud, with work that is no longer tethered to a desk in the office. The workforce is out in the field recording measurements on tablets, taking conference calls in route to a client or handing off projects across time zones.

The bring your own device (BYOD) phenomenon—which includes phones, tablets and laptops—has taken hold in the workplace. A survey from Unisys and research agency Loudhouse on the importance of digital capabilities in the workplace found that devices are the biggest pain point for workers, with 45 percent of them complaining that they are held back by outdated technology.

While BYOD increases worker satisfaction, it decreases visibility into security posture for organizations—ceding that responsibility to employees, who don’t have as much at risk in the event of a breach. Supporting digital workplace initiatives such as BYOD requires the hardware, software and security to protect data, wherever it goes.

Security Transformation

Implementing Zero Trust

Traditional security approaches that rely on an overly trusting static perimeter will not adequately control risk in a dynamic digital environment. A Zero Trust model assumes the network is already compromised, trusting no user or device until its identity is verified. According to a Forrester study commissioned by Unisys, 84 percent of security decision makers report that they have already adopted, plan to adopt or have interest in adopting aspects of this model.

A Zero Trust approach accommodates innovation while protecting critical resources and assets from cyberattacks. Taking Zero Trust from concept to implementation demands an architecture that is designed to grow with the business and is monitored and managed to be resilient. It requires complete visibility into the network, devices and users to map security controls with precision as well as the ability to quickly and easily adjust privileges.

With identity-based microsegmentation, only authorized users—regardless of device or location—are provided access to assets on a least-privilege basis. In the event of a breach, microsegmentation minimizes damage by preventing a threat from moving laterally in an organization. Isolating critical assets creates trusted enclaves that provide secure engagements between employees, customers and partners. Zero Trust weaves security into the fabric of digital business.
Establishing an Incorruptible Record

An emerging technology that has the power to establish more secure digital transactions is distributed ledger technology, commonly known as blockchain. While not a security solution itself, blockchain establishes transparency, a key tenet of security, since all transactions are recorded and visible to all parties with access to the information.

Blockchain creates an incorruptible transactional ledger where information can be added, but any attempt to modify previously-stored data is immediately evident to all participants. It promotes reliable data due to the distributed nature of the technology and encryption used—information is recorded in multiple nodes that must reach consensus to commit data in the chain using cryptographic algorithms—complexity that is difficult for a threat exploit.

In industries with a high level of regulation, blockchain provides a single source of truth to comply with an audit at any time. In addition, organizations with supply chains where products change hands frequently have full transparency into any deviations from the process or where a problem originated, so that corrective measures can be taken to minimize damage and prevent recurrences. For example, if a raw material vendor is violating the ethical and environmental standards for production, that violation is transparent to all participants in the blockchain so they can take action.

Increasing Pharmaceutical Supply Chain Transparency

The average medicine can be transferred between as many as 10 vendors from the time it leaves the manufacturer to when it reaches the pharmacy. The Pharmaceutical Security Institute (PSI), a not-for-profit organization that has collected data on counterfeiting, illegal diversion and theft incidents for over 15 years, reports that pharmaceutical crime incidents continue to rise.

Unisys created a solution that leverages blockchain to capture electronic product code information services (EPCIS) chain of custody transactions in a distributed ledger. This data is stored and tracked for all the vendors in the supply chain, including manufacturing and shipping, to access and view. By connecting all of the points in the supply chain, blockchain enhances transparency throughout the ecosystem and protects product safety.

Accelerating Digital Outcomes

Once the digital architecture is built, innovation further accelerates digital outcomes. Automation, advanced analytics and machine learning leverage the data processing power, distributed management and storage capabilities of the cloud. When used together, these technologies transform automation from simple to sophisticated.

Robotic process automation powers repetitive tasks—by inserting machine learning techniques, a feedback loop is created that learns from data, reduces human error, processes information more quickly and reveals insights through previously unknown patterns. When AI is applied to a process, intelligent automation transpires—continually improving results as more data is consumed.

In a survey for IDG’s 2018 State of Digital Business Transformation report, nearly two-thirds (64 percent) of IT leaders said they expect their enterprises to improve process efficiency through automation. From scaling infrastructure, to doing more with fewer resources, to staying ahead of security threats, intelligent automation enhances productivity in the digital age.

Infrastructure Transformation

Utilizing Cloud More Effectively

Cloud automation allows organizations to provision, manage and scale compute power to meet the fluctuating needs of the digital economy. Using analytic insights to constantly assess and improve operations, successful organizations orchestrate and automate data center and cloud services for optimal performance.

Cloud automation provides just enough infrastructure capacity to avoid idle resources. The orchestration platforms are able to marshal resources in the form of virtual machine (VM) systems, containers and microservices to serve even the most erratic demands, such as surges in traffic from viral social media on an ecommerce website.

Automation of cloud-based IT infrastructure also improves productivity by streamlining recurring workflow approvals as well as reducing production and development time. With automation, IT tasks that take people weeks or even months to perform can be done in just minutes. If there’s a need for additional resources to support new product testing, pre-configured VMs or containers of microservices are available via self-service and automatically deployed with all approvals, notifications and security requirements embedded, enabling businesses to move faster.
Workforce Transformation
Empowering the Workforce

Automation is often viewed as a threat to the human workforce, however, it can have the opposite effect in digital transformation. In a Wall Street Journal commentary, Ken Goldberg, director of the People and Robots Initiative and professor of engineering at the University of California, Berkeley, describes people and machines working together to solve problems as multiplicity. “Multiplicity is collaborative instead of combative,” says Goldberg. “Rather than discourage the human workers of the world, this new frontier has the potential to empower them.”

When humans work side by side with robots, the collaboration frees people to solve more sophisticated, and rewarding, challenges. By leveraging automation, expert resources are maximized, rather than spending time on routine matters that can be handled through virtual and self-help options. Service agents across all industries will require new, higher-level skills, including the ability to train, manage and configure support automation.

For example, IT is at the center of digital workplace transformation—integrating innovative technology with legacy infrastructure, retraining staff on new tools, adding digital capabilities and defining BYOD policies. To succeed in an environment of constant change, and meet user expectations for uninterrupted productivity, automation is a necessity. An IT service desk bolstered with automation empowers end users to access help in the most efficient manner possible.

Making Faster, More Accurate Decisions

Manual systems and limited personnel across industries—financial services, manufacturing, travel and transportation—can no longer keep up with the growing volume of transactions and data processing required to make timely, informed decisions. AI-driven analytics sift through data quickly to spot patterns and anomalies, scaling beyond the capabilities of legacy rule-based analytical models.

Increased transaction volumes, higher data availability, greater processing power and advanced algorithms are fueling innovation in analytics. More transactions and data provide the inputs required for more accurate results. Greater processing power from cluster computing, distributed data management and cloud storage enables this data to be collected and utilized. And advanced algorithms in AI and machine learning examine data fast and update frequently, continually improving results.

The application of machine learning is enabling the next generation of analytics modeling using intelligent automation, supporting faster, more accurate decision-making. According to Gartner predictions, “By 2020, more than 40 percent of data science tasks will be automated, resulting in increased productivity.”

Detecting Mortgage Risk Earlier with Machine Learning

Banks and financial institutions look at the likelihood of loan default to provide the appropriate customer intervention. But lenders lack important insights that can guide strategies to modify customer behavior and lower financial risk at the individual level.

Unisys analyzed live customer mortgage data to anticipate default by predicting arrears—the ability of a customer to make a payment at each pay period. By segmenting the customer base, applying machine learning models and identifying risk behavior, Unisys predicts customer arrears for 30-, 60- and 90-day periods. When measuring predictions against actuals, Unisys achieves more than 90 percent accuracy—helping mortgage companies make data-driven lending decisions to lower operational costs and risk, while improving customer relationships and experiences.
Security Transformation
Promoting Early Detection and Isolation of Threats
AI and machine learning also increase the speed and effectiveness of security solutions. A security threat is identified sooner, sometimes even predicted before a cyberattack actually takes place, using advanced analytics and automatic detection—containing a breach with intelligence-based action.

When a threat is detected, organizations have a difficult time responding quickly. The security operations center (SOC) contacts multiple teams to identify the problem and then determine how to contain it—an inefficient process that can consume days or weeks before remediation. By automating anomalous behavior detection, security policy enforcement and dynamic isolation of a suspicious user or device, threats are immediately quarantined to minimize damage without human bottlenecks.

Alleviating reactive cybersecurity tasks fosters a more proactive approach to security—addressing complex threats, securing existing assets and training the workforce on security hygiene—promoting the adoption of a security-first culture. In addition to protecting intellectual property, personally identifiable information and payment card details, a stronger security posture safeguards the critical applications and systems that deliver vital access to energy, transportation, financial services and healthcare as well as national security and defense.

Improving Risk Management Using Advanced Analytics
International tourist arrivals increased 6 percent to 1.4 billion in 2018, according to the World Tourism Organization. Governments need tools to prevent entry of illicit drug shipments, people traffickers, weapon smugglers, counterfeit goods, biosecurity threats and terrorists. Legacy screening systems have high levels of false positives as they depend heavily on rule-based pattern matching to identify risk.

To keep up with rapidly changing threat patterns, avoid gaps or contradictions between the rules and ensure that security resources are not distracted with false alarms, AI objectively identifies anomalies. Unisys advanced analytics solutions combine rule-based and predictive algorithm models to focus on border movement with potential security risk, allowing low-risk clearances with minimal interference. A continuous feedback loop to learn about high-risk behaviors improves targeting accuracy.

Transformation That Works
While disruptive technologies including cloud, blockchain, and AI and machine learning promise to increase efficiency and offer a competitive advantage, each transformation journey is unique. For digital transformation to work, it must be well planned, instilled culturally and inherently secure.

Digital transformations are successful when organizations leverage an innovative, trusted partner—one with the expertise required to integrate disparate services, systems and platforms with security built in from the start. Unisys provides the infrastructure, workforce and security transformation solutions and services to support commercial and government organizations at every stage of their digital transformation initiatives. In the age of everything digital, transformation that works, lasts.

Visit us at unisys.com/business-drivers/digital-transformation

For more information visit www.unisys.com
© 2019 Unisys Corporation. All rights reserved.
Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.