NEXT-GENERATION DATA CENTER EDITION

Unleashing IT

VOLUME 5 / ISSUE 4

EVOLUTION OF THE DATA CENTER

How next-generation data centers have become frontline drivers of business transformation, orchestration, and success. PAGE 3

IN COLLABORATION WITH INTEL®

Unleashing IT

VOLUME 5 / ISSUE 4

EVERYTHING, EVERYWHERE

In today's day and age, what enterprise activity can be accomplished without the assistance of a data center? Beyond face-to-face conversations, not much. And certainly not the business transformation many are seeking.

This edition of *Unleashing IT* explains why the data center is more important than ever before (page 3), facilitating virtually all business activities, wherever those activities take place.

But that's not all. Next-generation data centers offer widespread protection for an enterprise, its users, and its data (pages 12 and 14). They drive business efficiency, velocity, and growth (page 16). They bring visibility (page 5) and optimization (page 8) to activities and resources that are increasingly dispersed across a hybrid IT environment. And they are doing it all with an application-centric, software-defined policy model (page 10), built on the Intel® Xeon® processor-based Cisco Unified Computing System™ (Cisco UCS®).

Agility, efficiency, and transformation are essential elements of business success. And they can't be achieved without a next-generation data center.

For more information, follow the links inside or contact Cisco at 1-866-428-9596. We welcome your feedback on the articles in this publication at www.UnleashingIT.com.

Sincerely,

Dhritiman Dasgupta
Vice President
Cisco Systems, Inc.

Lisa Spelman
Vice President
Intel Corporation

STRATEGIES & SOLUTIONS

EXPERIENCES

Unleashing IT is published by Cisco Systems, Inc. To receive future editions of *Unleashing IT*, visit UnleashingIT.com.

WHY DATA CENTERS ARE MORE IMPORTANT THAN EVER

With analytics, simplification, automation, and protection—all connected through a common policy model—next-generation data centers are driving business transformation.

As cloud solutions and services continue their rapid ascent in the enterprise world, becoming mainstays of business agility and efficiency, it's fair to question the impact on traditional data centers and those who manage them. Are on-premises systems and specialists losing a measure of relevance?

Not remotely. In fact, it's quite the opposite.

"There has been an explosion of applications, devices, and endpoints that need to be secured and managed. Organizations must optimize the utilization of on-premises, private, and public cloud infrastructure; after all, hybrid is the new black. And countless companies are digitizing their operations," says Dhritiman Dasgupta, vice president of data center marketing at Cisco. "All of that starts with a next-generation data center."

The roots of data center modernization, he adds, were sprouted in the cloud.

"The cloud is not a place, it's a paradigm," Dasgupta notes. "It opened up everyone's eyes about the possibilities for greater agility, automation, efficiency, and simplicity. And those attributes have been pulled into the data center."

What used to be a fortified castle safeguarding an organization's crown jewels has become a hub of business activity, an orchestration engine that connects and protects a company in a dynamic, global marketplace.

"Data centers still possess the crown jewels, but they have become more open and connected," says Lisa Spelman, vice president and general manager of Intel Xeon products and data center marketing at Intel. "They are no longer operating behind the scenes as a support mechanism, but rather as a frontline driver of business productivity and transformation."

As modern data centers facilitate diverse and dispersed business activities, seamless orchestration, stout security, and consistent governance are essential.

"You need analytics, simplification, automation, and protection—what we call the ASAP data center," says Dasgupta. "Cisco is the only vendor that can deliver all of these attributes through a common, consistent policy model."

THE IMPORTANCE OF POLICY

With so many environments, components, systems, and languages, a common thread is needed throughout them. That thread is application policy, which acts as a Rosetta Stone for managing a heterogeneous, distributed infrastructure spanning multiple data center and cloud locations.

"Policy is the single source of truth across all environments and elements," Dasgupta explains. "It reflects the intent of the business, controls applications, and automates the delivery of hybrid infrastructure."

Cisco and Intel have worked together for years to develop, integrate, and optimize foundational technologies that enable business flexibility and efficiency without compromising IT performance, security, or governance. The combination of the Intel® Xeon® processor-based Cisco Unified Computing System™ (Cisco UCS®) and Cisco Application Centric Infrastructure (Cisco ACI™), in particular, provides the underpinnings of a policy-based, next-generation data center. One that delivers the agility and simplicity of the public cloud with the security and control of on-premises systems. One that is more important—and more attainable—than ever.

"The time is now," says Spelman. "There has never been a better opportunity to move up the value chain and transition from a service department to a strategic driver of business success. The longer you are stuck in 'analysis paralysis' mode, the harder it will be to catch up."

TRANSFORM YOUR OPERATIONS, ASAP

To learn more about the ASAP data center and to engage with Cisco, visit **cisco.com/go/datacenter**.

A DVR FOR YOUR DATA CENTER

In mapping and recording a distributed IT environment, Cisco Tetration Analytics provides full visibility of application dependencies and unmatched forensic capabilities if something goes wrong.

"You can't manage what you can't see," says Zeus Kerravala, founder and principal analyst at ZK Research. "You can't secure it either."

With three-quarters of application performance problems being identified by end users and not technology specialists[1], it's safe to assume most IT teams have blind spots. And who can blame them? Modern enterprises rely on hundreds if not thousands of applications, which are increasingly distributed across multiple environments, from physical machines and virtual infrastructure to private and public clouds.

"Traditional monitoring solutions were built for monolithic, static applications, not distributed apps that are continually evolving," says Yogesh Kaushik, senior director of product management for Cisco Tetration Analytics. "If you can't see where your apps are and what they are touching, how can you secure them? How can you patch everything?"

Companies use around 20 monitoring tools on average, he explains, which all provide a different—and limited—picture of what is happening. If something goes wrong, it can take months to determine the source and scope of the problem.

"Most tools focus on each element individually, not how those elements are interacting with each other or how they relate to what the user is experiencing," say Kerravala. "And many only show one slice of time or averages over time, so they miss a lot."

What's needed is a holistic mapping and analytics platform that provides visibility and telemetry data across every application and infrastructure component—all at once.

VISIBILITY AND FORENSICS

Cisco Tetration Analytics is a new platform that provides unprecedented visibility and fine-grained forensics across everything in an IT environment, in real time. It creates a topology map that shows all applications, their connections, and their dependencies.

"Mapping is very important, more important than people realize," Kerravala claims. "You need to see what is touching what, and the dependencies between applications and systems. Everyone has a story of turning a server or some other infrastructure off and having something else unexpectedly go down with it because they didn't know the two were connected."

One of the biggest security risks in modern IT environments is open connections between systems—many of which are unknown or forgotten. With Tetration, every connection is revealed. And all of the data flowing through those connections is recorded.

"Tetration captures every packet and every flow at every speed," says Kaushik. "It's like a DVR for your entire data center."

The platform provides unmatched forensic capabilities to better understand anomalies, performance dips, breaches, and other issues. IT specialists can easily see everything that happened before, during, and after an event.

"Investigations that used to take months can be done in minutes or hours," Kaushik explains. "You can zoom in and see exactly what happened at any moment in time, in extremely granular detail. You can see what machine was compromised, what it talked to, and what those machines talked to. It's like stepping into the scene of a crime as it happens instead of trying to piece it together with limited information after it has occurred."

MACHINE LEARNING

With better visibility comes better security, anomaly detection, and forensics. But capturing every packet and flow at every speed creates its own challenges.

"Everyone loves data," says Kerravala, "but big data requires big analytics. And that's hard to do."

For Cisco IT, which is already using the Tetration platform, this means processing and filtering millions of events every second—one billion packets every day. That's why Tetration includes a robust machine learning and analytics engine that helps filter out the noise and draw attention to data worthy of investigation.

"Machines are good at processing data, and humans are good at making decisions," says Kaushik. "Tetration processes huge volumes of data in real time and serves it up to humans in ways that make sense. Instead of searching for needles in a massive haystack, users get a focused and actionable decision tree."

The resulting time savings are significant. According to an IDC Business Value Brief, Cisco IT expects to avoid 3,650 hours of IT staff time per 100 applications in application dependency mapping and establishing zero-trust operations—a 70 percent reduction—by using the combination of Tetration and Cisco Application Centric Infrastructure (Cisco ACI™).[2]

"Manual processes are too slow for an increasingly digital world, and companies need to rethink their entire IT strategy," says Kerravala. "The siloed, bottom-up approach of systems management and security isn't sustainable. You need full visibility of all elements, all applications, and all data—and you need automation and analytics to interpret and act on that data."

With an application dependency map and DVR-like recording and playback, there's never been a better way to manage and secure a distributed IT environment.

1 ZK Research, "Network Purchase Intention Study," 2016

[2] IDC Business Value Brief, "Cisco Tetration Analytics: Cisco Datacenters Get Pervasive Visibility and Reduced Security Risk with 70% Less Time and Cost, sponsored by Cisco," June 2016

WATCH THE VIDEO

To see how Cisco Tetration captures every packet and every flow at line rate, watch the video at **UnleashingIT.com/analytics**.

FINDING THE RIGHT HOME FOR YOUR APPLICATIONS

Infrastructure-agnostic modeling tools improve application placement, management, and portability.

It wasn't long ago that software and hardware were indelibly tied. Applications were forced to conform to the specific nuances of the various infrastructure environments on which they would operate. Servers and networks were manually configured to host each application. And the pairings were built to last.

But they haven't.

"The explosion of applications and the diversification of infrastructure have changed everything," says David Cope, senior director of cloud market development at Cisco. "Large enterprises now support more than 5000 applications on average, which are dispersed among physical and virtual data center systems as well as private and public clouds."

With a staggering array of software and a growing number of infrastructure options, how do companies know which environment is best suited for each application? And as those applications evolve—from development to staging to production and beyond—how can IT organizations effectively port them to the environment best suited for each stage of the lifecycle?

INFRASTRUCTURE-AGNOSTIC APPLICATION MODELING

"Companies should be taking a fresh look at their application portfolio and doing some rightsizing analysis on a quarterly basis," recommends Dave Bartoletti, principal analyst at Forrester. "You're looking for the best fit for each application, whether that is keeping it in the data center, pushing it to the cloud, or replacing it with a SaaS-based solution."

Application modeling is the first step, describing the application's characteristics and policy requirements in a way that is abstracted from underlying systems. Cisco® CloudCenter, for example, creates an infrastructure-agnostic profile or blueprint of each application, including its topology and dependencies. Formerly known as CliQr CloudCenter, the solution uses the profile to benchmark the application on available environments.

"You need to put the right workload in the right environment, and that comes down to utility economics," says Cope. "Price versus performance is key, and the relationship between them isn't always linear. You can see a 50x difference in application performance depending on the environment. Infrastructure matters."

Data sovereignty, compliance requirements, service-level agreements, and the fluctuating priority of the application also matter. Cisco CloudCenter evaluates a number of variables to help find the best home for each application. And as those variables change, so too might the optimum venue.

APPLICATION PORTABILITY AND OPTIMIZATION

Cisco CloudCenter helps model, deploy, and manage applications in the environment best suited to their unique policy requirements. But just because an application is placed in—or moved to—an ideal environment doesn't mean it should stay there forever. Priorities and requirements change over time, and modeling and management provide the flexibility to continually evaluate and optimize an application portfolio.

"The more you tie applications to the underlying infrastructure—even with public cloud APIs—the harder it will be to migrate them in the future," Bartoletti warns. "You need to consider optimization and portability up front, before you need them."

It all boils down to the needs of each application.

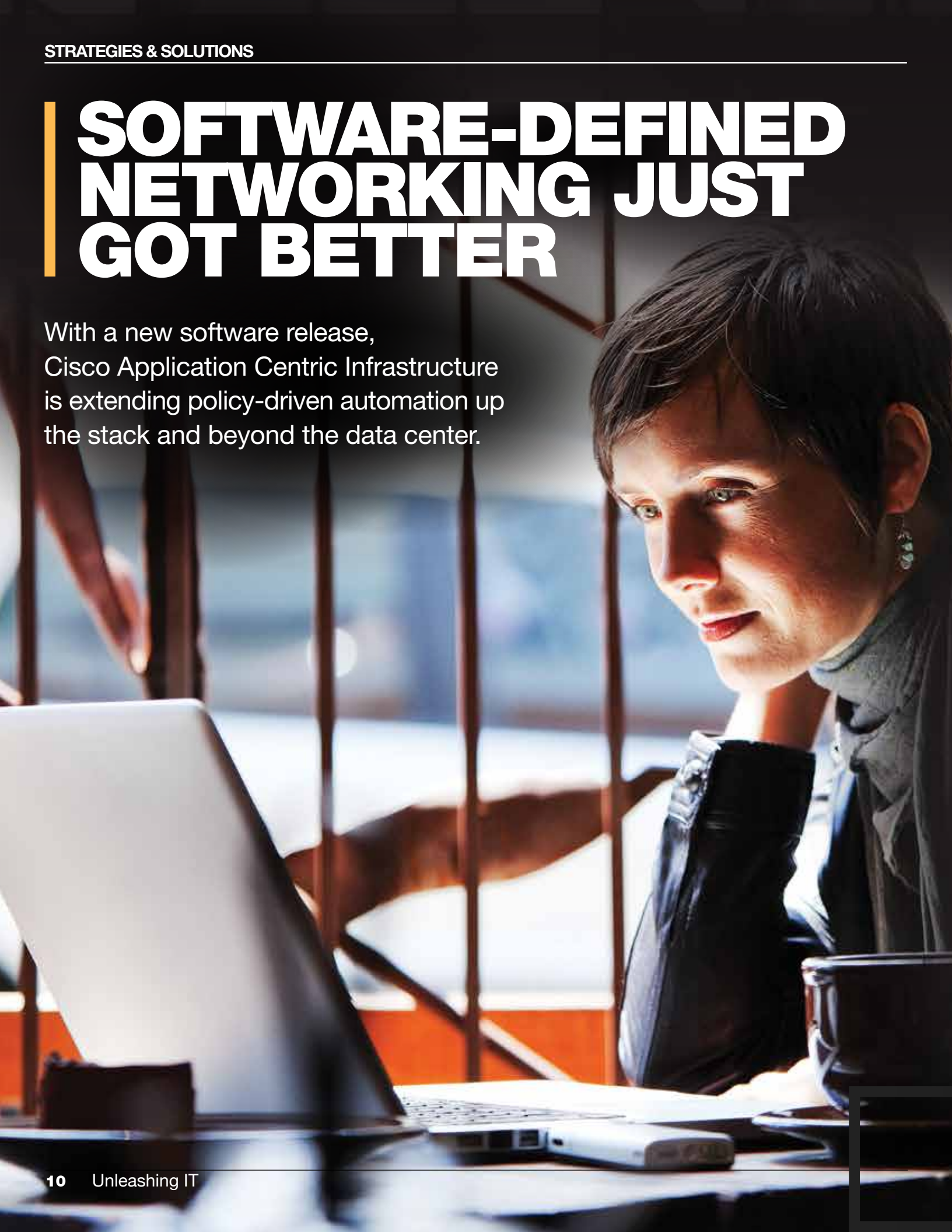
"In the past, applications had to conform to the infrastructure. Today, it's the opposite," says Cope. "But there are so many infrastructure choices, and all of them are becoming more specialized. You need to make decisions on a case-by-case basis, and you need to revisit those decisions as priorities evolve."

REQUEST A DEMO

See how easy application-centric cloud management can be by scheduling a demo at **UnleashingIT.com/CloudCenter**.

SOFTWARE-DEFINED NETWORKING JUST GOT BETTER

With a new software release, Cisco Application Centric Infrastructure is extending policy-driven automation up the stack and beyond the data center.



Software-defined networking (SDN) is no longer a trendy concept or technological curiosity. With more than 2700 customers and counting, Cisco® Application Centric Infrastructure (Cisco ACI™)—the industry's leading SDN solution—has become a popular engine for automating, managing, and securing distributed IT resources and applications.

And it just got better.

The recent ACI 2.0 software release extends policy-driven automation up the stack and beyond the data center, simplifying IT operations and delivering better security and more granular control.

"The first wave of ACI was focused squarely on the network," says Carlos Pereira, distinguished systems engineer at Cisco. "Our latest software release expands on that goodness in layers four through seven and across multiple locations."

EXTENDING THE BENEFITS OF SDN

Instead of micromanaging every piece of an infrastructure individually, Cisco ACI allows everything to be centrally managed with application policies that are easy to define and replicate. As a result, manual, repetitious processes—to set up network connections, enforce security rules, make changes, etcetera—are reduced by an order of magnitude.

"ACI is the lynchpin that pulls everything together in a single pane of glass," says Harry Petty, director of data center and cloud marketing at Cisco. "It uses a declarative policy model based on intent, describing applications in ways that everyone understands and automating the configuration of the infrastructure accordingly. Not just box-by-box configurations of network ports, but service levels for applications based on all their interconnections."

The open architecture can accommodate any L4-7 service, he explains, including third-party access control, firewall, intrusion detection, and load balancing solutions. And those services can all be configured and managed with a common policy model.

ACI is also inherently secure. No connections are established without explicit, policy-based instruction, and ACI 2.0 includes more granular segmentation and control that can be extended across multiple environments and hypervisors.

"ACI is a groundbreaking technology that can be the catalyst for an entirely new IT operational model, or it can become a valuable piece of an existing network construct," says Pereira. "It's incredibly flexible and scalable, allowing organizations to start small with certain applications, workloads, and policies. And once they try it out, they invariably want to use it elsewhere."

LEARN MORE

To learn more about Cisco ACI, the industry's leading SDN solution, visit **cisco.com/go/aci**.

CISCO ACI APP CENTER TAKES SHAPE

Openness and programmability have always been hallmarks of Cisco® Application Centric Infrastructure (Cisco ACI™). And never before has that been more evident.

The Cisco ACI App Center was recently announced, providing a new marketplace for developers and customers utilizing the industry's leading software-defined networking (SDN) solution.

"The ACI community is active and growing," says Salman Asadullah, CTO of the Americas Partner Organization (APO) and distinguished engineer at Cisco. "We wanted to make it easier for everyone to develop, share, consume, and monetize new ACI tools and functionality."

Five technology leaders have already developed new tools and contributed to the ACI App Center, which will be available in early 2017:

1. Dimension Data—GIT integration for ACI
2. GDT—Application profile browser
3. Kovarus—Security reporter
4. Netnuvem—ACI App testing and validation
5. World Wide Technology—Automated security management

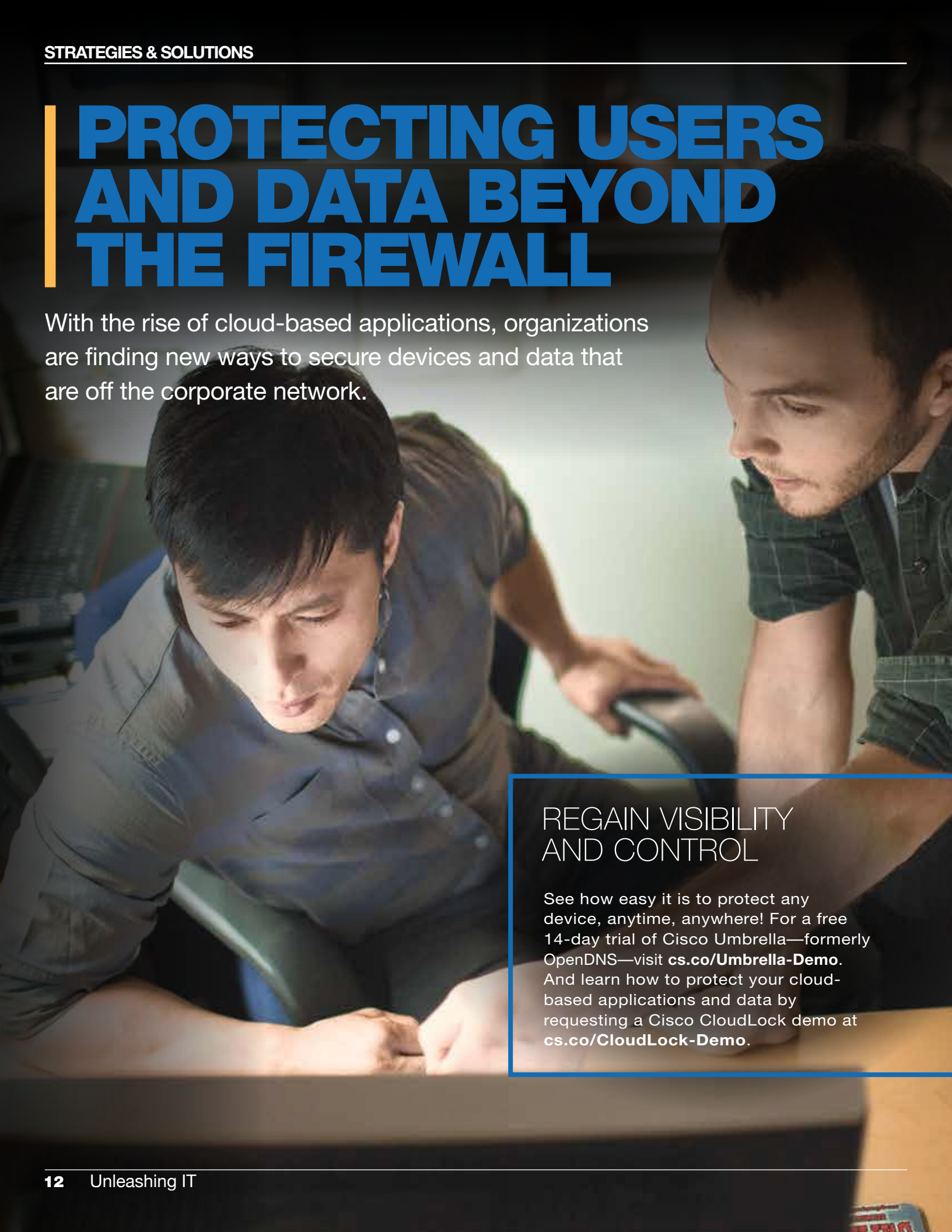
Cisco ACI software development kits and APIs are available free of charge, streamlining the development of new features and functionality. Network administrators will be able to install the apps on the Cisco Application Policy Infrastructure Controller (APIC), which ensures reliable, secure app performance as part of the ACI Fabric.

"Custom apps can help simplify, enhance, and better visualize the ACI experience," says Shelly Blackburn, director of systems engineering for Cisco APO. "We're excited to see more contributions and innovation from our partners and the development community."

For more information and to get involved, please reach out to the Cisco ACI App Center team at **appcenter@cisco.com**.

PROTECTING USERS AND DATA BEYOND THE FIREWALL

With the rise of cloud-based applications, organizations are finding new ways to secure devices and data that are off the corporate network.



REGAIN VISIBILITY AND CONTROL

See how easy it is to protect any device, anytime, anywhere! For a free 14-day trial of Cisco Umbrella—formerly OpenDNS—visit **cs.co/Umbrella-Demo**. And learn how to protect your cloud-based applications and data by requesting a Cisco CloudLock demo at **cs.co/CloudLock-Demo**.

Users and applications have escaped the "four walls" of the data center, and that creates a risk/reward scenario for all enterprises.

"Every organization is trying to get their arms around this," says Scott Harrell, vice president of Cisco's Security Business Group. "They want to leverage the cloud to drive business efficiency and productivity, but without losing visibility and control of their applications and data."

According to Gartner, a whopping 25 percent of corporate data traffic will bypass perimeter security and flow directly from mobile devices to the cloud by 2018[1]. With the meteoric rise of cloud-based applications and services—and with countless employees using work computers for personal Internet browsing—how can companies protect users and data when they are outside the corporate network? And how can they keep potential threats from getting in?

As Harrell mentions, it comes down to visibility and control. Without the former, IT teams cannot attain the latter.

KEEPING DEVICES CLEAN

Broadcom, a global semiconductor leader for more than 50 years, was an early cloud adopter. Today, every one of its employees—spanning 30-plus countries and 100-plus locations—utilize cloud-based applications to collaborate with each other and their customers.

"We have employees and customers all around the world," says Andy Nallappan, vice president and CIO of Broadcom, "and we rely heavily on the cloud to be fast, efficient, and productive."

Broadcom protects its users and data in multiple ways, one of which is making sure devices don't get infected when they are off the corporate network. The company uses Cisco® Umbrella—formerly OpenDNS—to see who is accessing what on the Internet. The solution analyzes domain requests to determine if the destination is potentially malicious, and if so, that domain is blocked.

"We were worried about Internet browsing, and signature-based antivirus solutions aren't enough," Nallappan says. "Cisco Umbrella makes sure devices are clean before they come back on our network, and provides user and domain visibility if something does get infected. It has helped us strike a balance between empowerment and protection as we continue to expand our cloud usage."

SECURING DATA IN THE CLOUD

Security incidents aren't just borne from threats. In many cases, they are the result of accidental user behavior. The innocent task of sending an email or saving a spreadsheet in a cloud environment can have serious implications—especially in regulated industries like healthcare, finance, and education.

"It's all about the data," says Joel Rosenblatt, director of computer and network security at Columbia University. "If you can secure the data, it doesn't matter where it is."

Columbia University uses Cisco CloudLock to monitor user behavior and confidential data in cloud applications.

"We have millions of documents and hundreds of terabytes of data in the cloud, and sensitive data is fine as long as it's encrypted," Rosenblatt explains. "We use CloudLock to continually scan for social security numbers, credit card numbers, and other personally identifiable information. If that data isn't protected, the system automatically locks down the sharing of the document and sends a note to the user with encryption instructions."

It's a proactive step that helps detect and protect confidential information that is accidentally uploaded or shared—before malicious actors can find it.

"We find files and emails that should have encryption on a daily basis," says Rosenblatt. "People make mistakes, but we can find and fix those mistakes before they cause damage."

PROTECTION WITHOUT RESTRICTION

There is no panacea for protecting users and data beyond the firewall, but there are tools that provide visibility of the activity occurring outside the network and inside cloud applications. And there are solutions that provide exceptional levels of access control to minimize the impact of security incidents—both intentional and unintentional.

Regardless of the technologies being used, both Nallappan and Rosenblatt say a comprehensive security strategy that doesn't restrict cloud usage is key.

"You can't tell people not to browse or not to use the cloud. It won't happen," says Nallappan. "But you can put a virtual cop on the road to slow people down, and you can make sure devices are clean before they get back onto your network."

"We protect our data by protecting users and their behavior," Rosenblatt adds. "It's all about authenticated user access and steadfast data encryption."

And that starts with visibility and control.

[1] twitter.com/gartner_inc/status/481528221054169088

EASIER, BETTER SECURITY WITH MICRO-SEGMENTATION

How group-based policy automation simplifies and fortifies security throughout a data center and beyond.

Firewall access control lists can have millions of rules. Just for one data center. Anyone who has been manually building, managing, updating, or auditing these highly complex lists knows the process is no longer sustainable.

Something has to give.

“It’s becoming impossible to define and manage each device and user individually, and manually configure the network for every application and IP address,” says Kevin Regan, product manager for Cisco TrustSec®, a segmentation technology that is embedded in more than 40 Cisco switches, routers, and wireless devices. “It can take a month just to set up the security and access policies for one new application.”

With the proliferation of users and devices and the constant evolution of business-critical applications, a new approach is necessary. One that is automated instead of manual. One that facilitates the management and protection of groups instead of each and every “thing” that needs access to the network.

“It’s easier to classify and manage things in groups,” Regan explains. “That could be a user group, like doctors and nurses who need access to sensitive patient data. It could be a group of devices, like point of sale systems that must remain PCI compliant. Or it could be a group of endpoints, like bare metal server workloads, virtual machines, or containers.”

Group-based policy management—and the micro-segmentation it provides—is an increasingly important security measure. Especially as applications, devices, and users become more distributed and as threats become more sophisticated and debilitating.

“Once you map logical groups together, you can establish security policies for those groups,” says Regan, “and enforce them everywhere.”

END-TO-END SEGMENTATION

Group-based management and policy automation are core capabilities of Cisco® Application Centric Infrastructure (Cisco ACI™), and their reach has been extended. What was once limited to the network has been pushed up and down the stack and beyond the data center.

“ACI has been tightly integrated with TrustSec and Cisco Identity Services Engine (ISE), extending group management to campus, branch, and virtual private networks,” Regan explains. “IT teams can define group-based policies with ACI, which automatically configures the data center network infrastructure based on those policies. And then the same groups are used by TrustSec to apply policy to devices and users outside the data center.”

The result is end-to-end segmentation and policy enforcement that is easy to configure and manage.

"It simplifies firewall rules and web security policies across the network because you can set up group-based policies once and use them again and again," says Regan. "That's a huge difference compared to manually configuring the network for every new application, device, and user."

What used to take weeks or months can now be done in minutes, with better coverage and control.

BETTER MALWARE CONTAINMENT

Attackers have historically breached corporate networks with the intent of pulling valuable data out, but their strategies have evolved. Many hackers are now looking to get in with the intent of usurping control of enterprise systems, or shutting them down altogether. Ransomware, for example, which hijacks enterprise systems and data until a payment is made, is becoming an increasingly popular form of malware.

"Most networks are flat. Once something gets in, it can infect everything," says Kerry Armistead, senior product manager for Cisco Stealthwatch, which works in tandem with Cisco ACI and Cisco TrustSec to provide advanced network visibility, analytics, and protection. "That's why gates and security measures at the perimeter are no longer enough. You need them everywhere, from the data center to branch offices to remote users to IoT devices."

Instead of a single castle wall that protects an open courtyard, micro-segmentation provides fortified walls around each and every group, no matter where they are. In doing so, it dramatically reduces the attack surface and automatically contains network breaches.

"Cisco is the only company that can provide end-to-end segmentation, from applications and microservices in the data center to remote devices and branch offices," says Scott Harrell, vice president of product management for Cisco's Security Business Group. "Segmentation is crucial to limiting the potential impact of modern threats and for securely adopting new technologies."

GET THE WHITE PAPER

For a complimentary white paper on policy-driven microsegmentation, visit **UnleashingIT.com/segmentation**.

HYPERCONVERGED INFRASTRUCTURE, HYPER EFFICIENT OPERATIONS

BluePearl Veterinary Partners has standardized on a Cisco HyperFlex System to boost the efficiency of its IT staff—and its business.

Despite the ongoing convergence of IT infrastructure, many organizations still find themselves managing compute, storage, and networking systems as independent silos. Such was the case for BluePearl Veterinary Partners, which runs 57 animal hospitals in 18 states.

The company's shared infrastructure platform "worked fine for our current hub-and-spoke architecture, but couldn't support our long-term goal of moving to a centralized data center," says Derek DePasture, senior network engineer at BluePearl. "There was no modular scalability, and each platform was a management silo."

After two years of growth that saw BluePearl's business double in size, DePasture and his small team were having trouble keeping up.

"We faced a choice," he recalls. "We either needed to hire more IT staff or make our environment easier to manage."

BluePearl chose the latter, seeking a hyperconverged infrastructure platform that could deliver scalability and end-to-end management efficiency.

"We wanted an all-in-one solution that would be data center ready without spawning new islands of infrastructure," says DePasture. "Our goal was to eliminate silos, not create them."

DEPLOYING IN A DAY

BluePearl recently standardized on Cisco HyperFlex™, which combines software-defined networking and computing with a next-generation data platform. Engineered on the Intel® Xeon® processor-based Cisco Unified Computing System™ (Cisco UCS®), it unlocks the full potential of hyperconvergence and brings new levels of operational efficiency and adaptability to a data center.

"Cisco HyperFlex was the perfect fit for us. We can invest once and scale up as high as we need," DePasture explains. "It's a better solution from a technical perspective and it makes a lot more financial sense. And we have Cisco support behind us, which gives us a lot of confidence."

The platform has also delivered tremendous efficiency—for BluePearl's IT staff and its business.

"Cisco HyperFlex took 80 percent less time to deploy than our previous solution, and speed equals efficiency," says DePasture, noting the solution was unboxed and configured in a single business day. "When you run as lean as we do, every minute is valuable."

With single-pane-of-glass management, the platform has enabled BluePearl to keep IT headcount flat despite rapid growth and avoid hiring three senior-level engineers. Instead of being consumed by infrastructure management, the IT team is now focusing on growth and providing excellent user experiences.

"With Cisco HyperFlex, we don't have to worry because everything is designed to work together, and there are multiple redundancies in place," says DePasture. "As we grow, we can onboard new sites faster and find new ways to help our veterinarians deliver the best care possible. Where HyperFlex has been deployed, reports from users have been stellar."

To see what 451 Research is saying about the next phase of hyperconverged infrastructure, download the report at **UnleashingIT.com/hyperconvergence**.

THE EVOLUTION OF DATA CENTER CONVERGENCE

The simplicity, economics, and scalability of cloud computing have prompted many IT professionals to ask: "Why can't we bring those attributes into our own data center?"

With the evolution and maturation of hyperconverged infrastructure systems, now they can.

The latest generation of hyperconverged systems, like Cisco HyperFlex™, have completely amalgamated not just compute and storage, but also networking infrastructure. Engineered as a single system, they make good on the promise and potential of a fully converged and virtualized data center.

"It's like a cloud in a box," explains Kaustubh Das, vice president of product management at Cisco. "And the network is included, so you don't have to configure anything or set up any VLANs. Just plug it in and it's ready to go."

SINGLE POOL OF RESOURCES, SINGLE MANAGEMENT INTERFACE

Built on the Intel® Xeon® processor-based Cisco Unified Computing System™ (Cisco UCS®), Cisco HyperFlex allows compute, storage, and networking components to be managed as a single pool of resources. Better yet, they can be scaled independently.

"If you need more compute, you can add more blades or racks. If you need more storage, you can add more drives. If you need more everything, you can add more HyperFlex nodes," says Das. "But it remains a single, unified system and fabric with a single management interface."

Because the network is pre-configured and pre-installed, Cisco HyperFlex also acts as a traffic cop that ensures optimum quality of service (QoS) and performance from Day One. Different levels of bandwidth, latency, and performance can be reserved for management, storage, replication, and other traffic types.

"With hyperconverged systems like HyperFlex, everything becomes faster, more predictable, and easier to manage," says Das. "Because it's one unified system and fabric, it coexists seamlessly with your existing environment and is easy to scale. Start with a new workload like VDI, virtual infrastructure, or test/dev, and then expand over time. You'll never look back."

BUILDING A "FIELD OF DREAMS"

With a powerful data center platform that delivers end-to-end automation and orchestration, Hutchinson Networks is creating new services and reaching new markets.

"We can't wait for customers to commit and then build the platform," says Stephen Hampton, CTO of Hutchinson Networks. "We must have faith that if we build it, the customers will come."

Hutchinson used to focus squarely on systems design, implementation, and integration. It is a master of corporate and wireless networks, and a wizard with firewalls and load balancers. But the Edinburgh, Scotland-based service provider is now taking a "field of dreams" approach to IT delivery and innovation.

"With systems integration, there are a lot of peaks and valleys. We wanted more predictable, annuity-based revenue," Hampton explains. "And I've always been keenly interested in delivering services from a data center. Even before the cloud was such a thing."

The sweeping adoption of that "thing" threatened Hutchinson's core business and its ability to retain its cache of clients. But Hampton saw opportunity amidst the peril.

"There are no Cisco Powered™ service providers in Scotland," he says. "We saw an opportunity to build a world-class cloud platform, stay in front of the market, and become experts in DevOps and orchestration."

DEVOPS AS A SERVICE

Hutchinson recently assembled a powerful cloud platform using a combination of Intel® Xeon® processor-based Cisco Unified Computing System™ (Cisco UCS®), Cisco Application Centric Infrastructure (Cisco ACI™), F5 Big-IP for Cisco Application Policy Infrastructure Controller (APIC), and Nimble Storage. Known as Fabrix, the platform offers everything but the application, providing network connectivity, security, load balancing, storage, and virtual servers, allowing Hutchinson's clients to focus on that which they care about most—the application.

"The platform enables unprecedented automation and orchestration," Hampton says. "With UCS Director and ACI, we can define workflows and tasks, and then automate the deployment of secure, multitenant containers and complex network fabrics. What used to take four to six months can be done in five minutes."

The solution is also inherently open and programmable, he adds, with the northbound API of Cisco APIC enabling integration with external tools like OpenStack. All of this is allowing Hutchinson to advance its DevOps, coding, and orchestration capabilities.

"The platform has helped us transition from a network integrator to a DevOps facilitator," Hampton claims. "At first, DevOps was viewed as an internal capability. But we now think it can be a new professional service that we take to market."

His company doesn't just intend to deliver new market services, it aims to enter new markets altogether. With a powerful cloud platform that facilitates DevOps, automation, and orchestration, Hutchinson is becoming increasingly attractive to agile startups and Software-as-a-Service providers.

To learn more about Hutchinson Networks' business transformation and use of Cisco ACI, download the case study at **UnleashingIT.com/Hutchinson**.