NEXT-GENERATION DATA CENTER EDITION

Unleashing IT

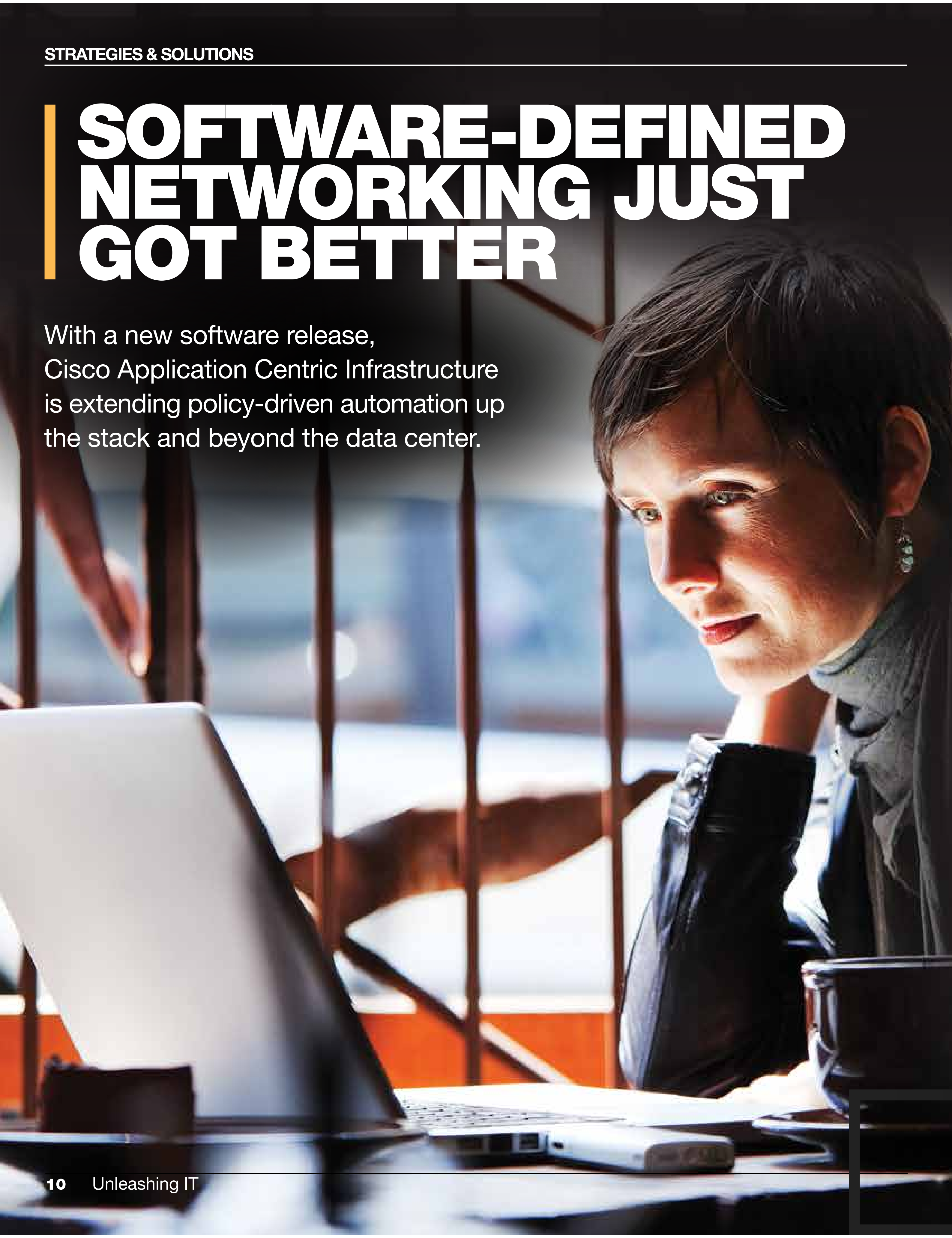
VOLUME 5 / ISSUE 4

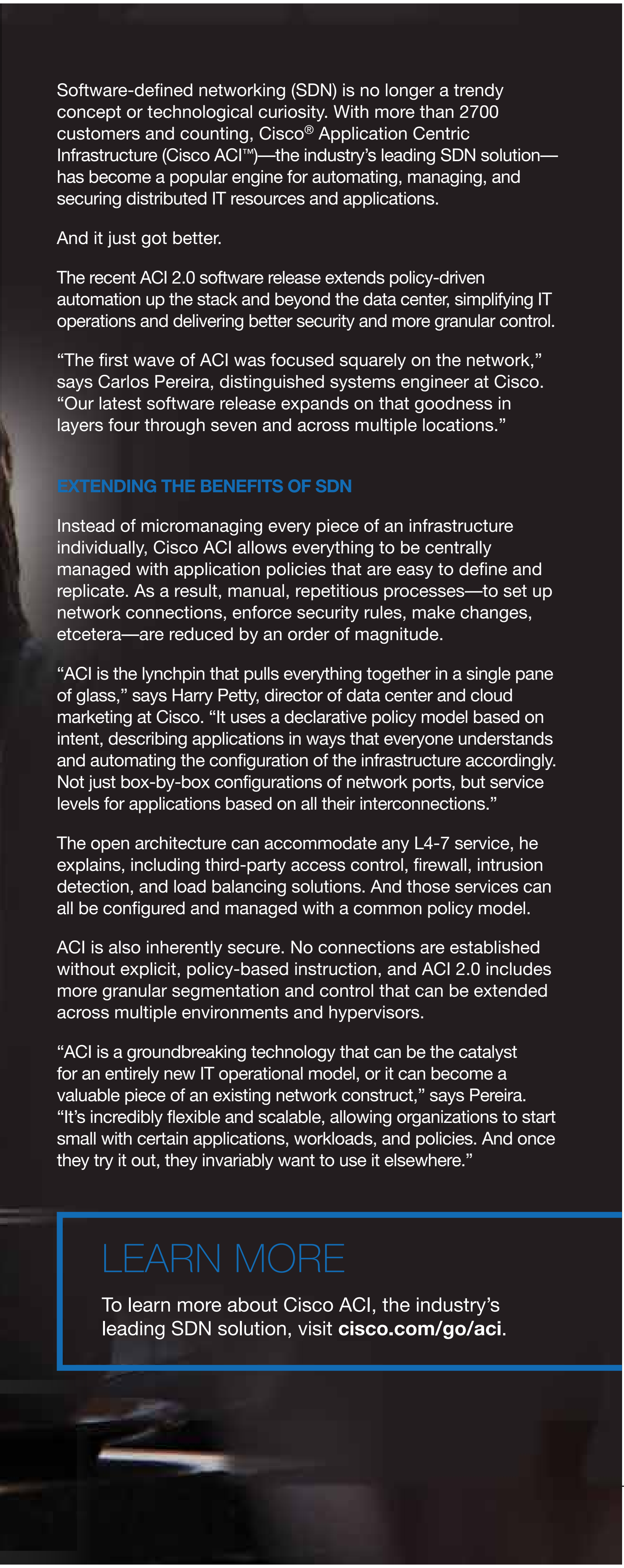
EVOLUTION OF THE DATA CENTER

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

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."

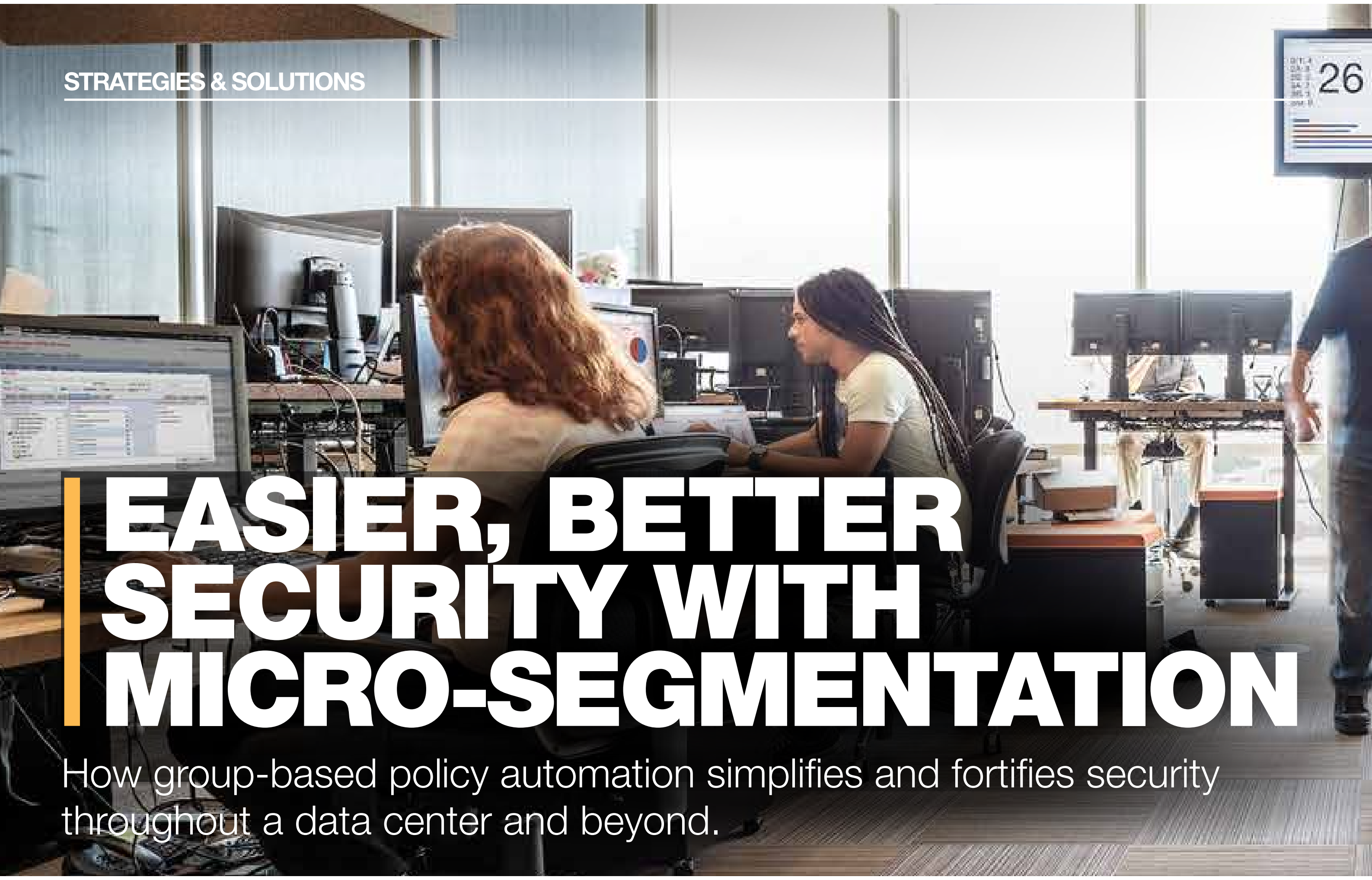
Five technology leaders have already developed new tools and contributed to the ACI App Center, which will be available in early 2017:

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**.



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.”

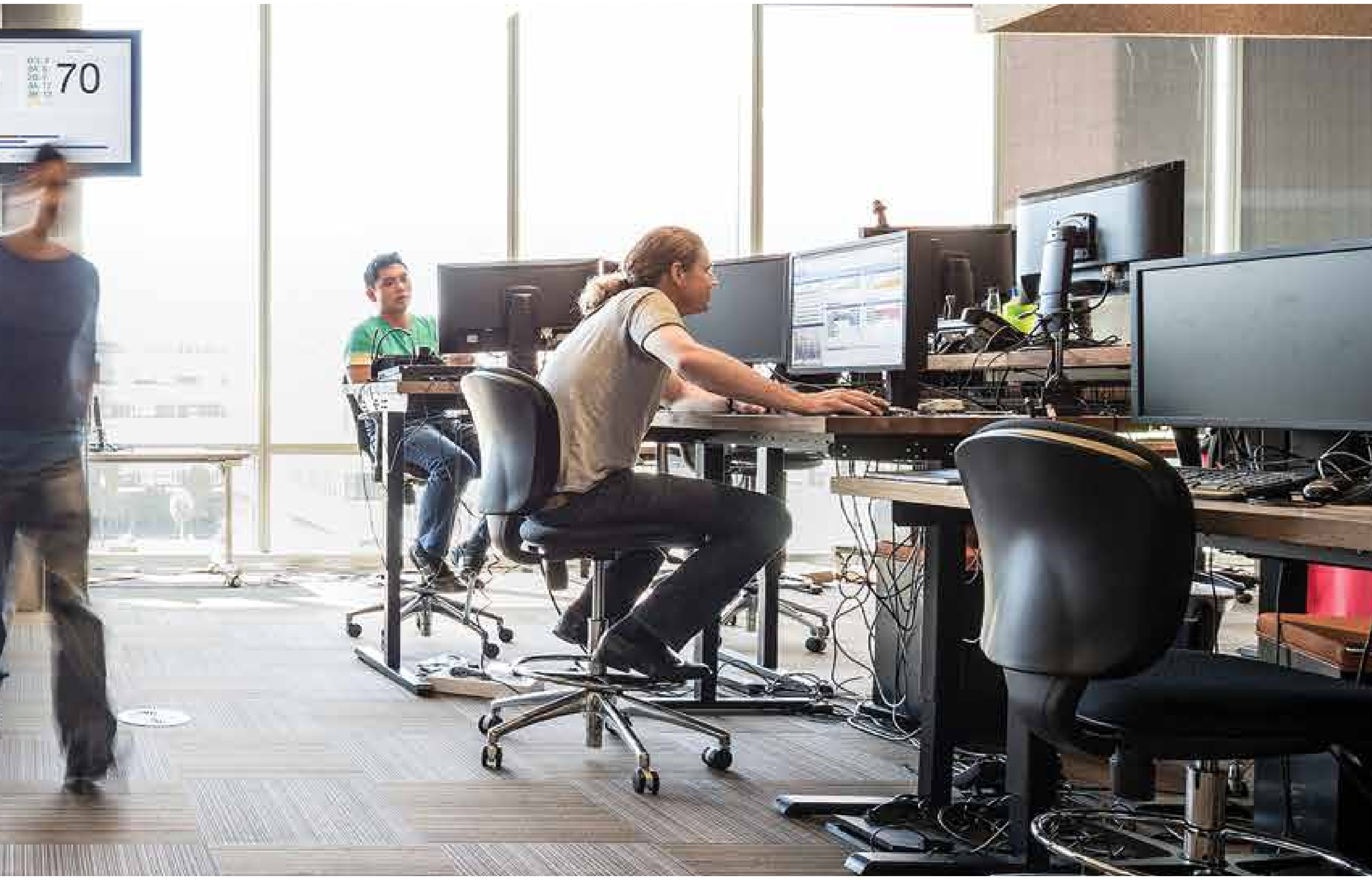
Group-based policy management—and the micro-segmentation it provides—is an increasingly important security measure. Especially as applications, devices, and users become more distributed and as threats become more sophisticated and debilitating.

“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**.

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.

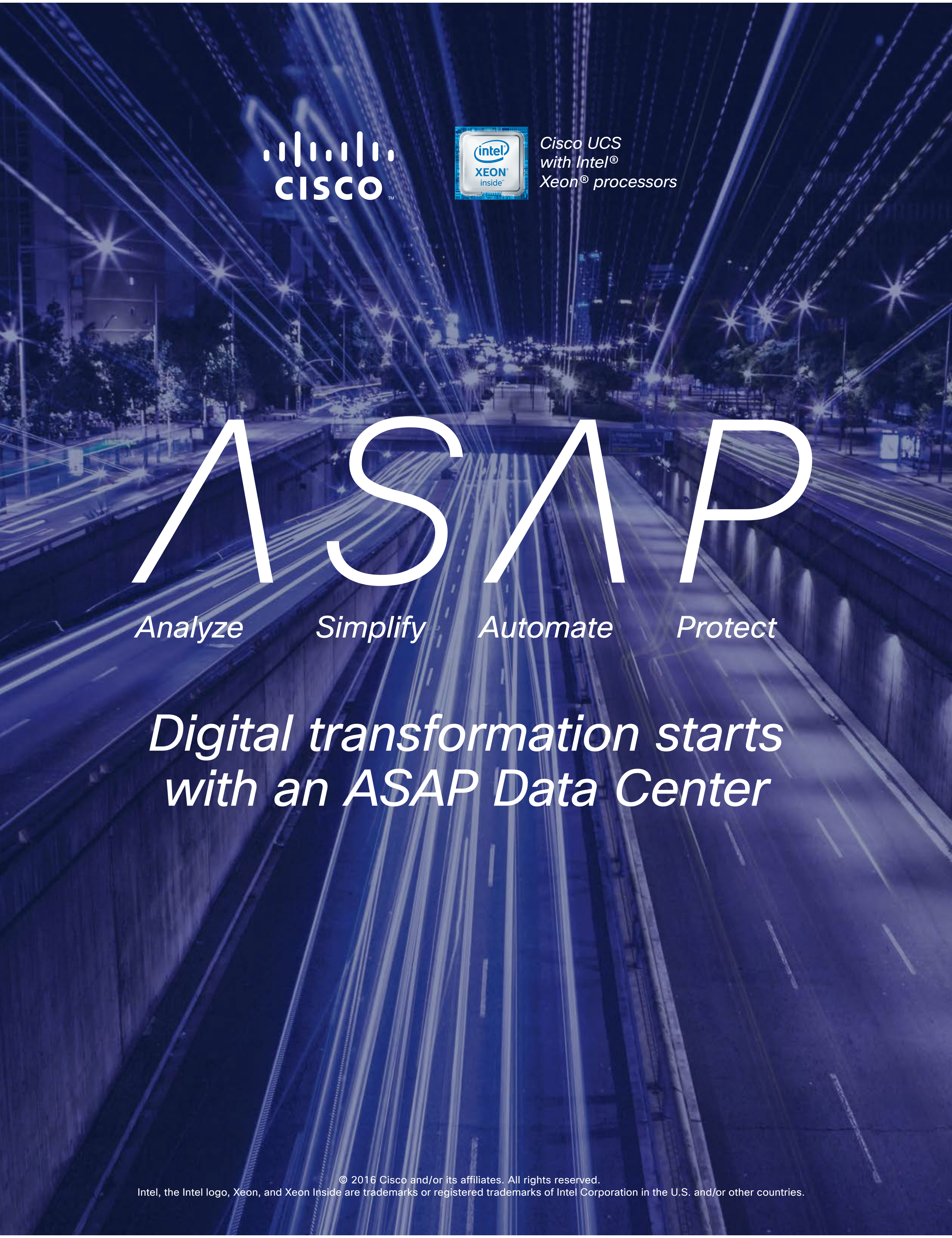
“The platform enables unprecedented automation and orchestration,” Hampton says. “With UCS Director and ACI, we can define workflows and tasks, and then automate the deployment of secure, multitenant containers and complex network fabrics. What used to take four to six months can be done in five minutes.”

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**.



Cisco UCS
with Intel®
Xeon® processors

ASAP

Analyze *Simplify* *Automate* *Protect*

Digital transformation starts with an ASAP Data Center