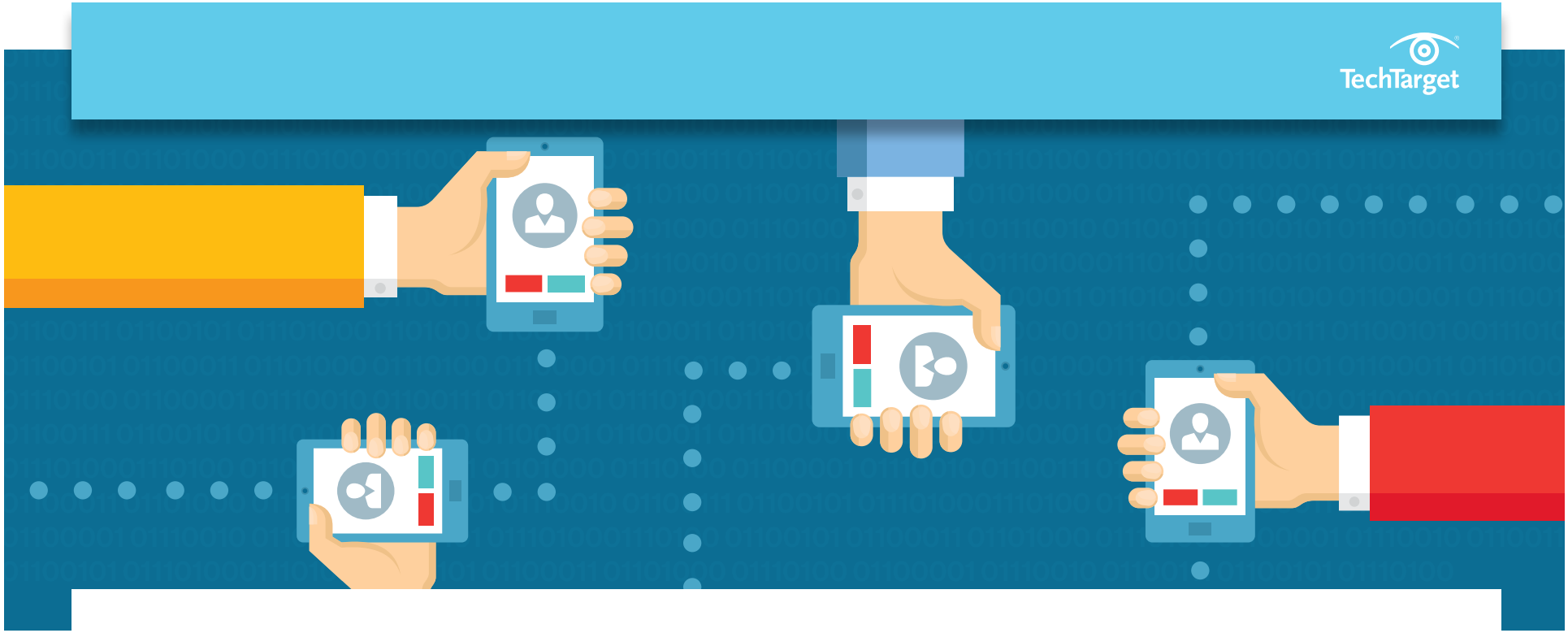

Is It Time to 'Software-Define' Your Network Security?

From mobile to micro to 'no-touch': Learn the latest ways to apply software-defined networking to your network security management.

Three Ways SDN Can Work for You Now

One may debate whether software-defined networking, or SDN, can be applied to everything, but it definitely applies to security. SDN makes possible the deployment and automation of a variety of security controls—like network segmentation, identity and access management and data loss prevention—by implementing them at the software (rather than hardware) level.

In this three-part technical guide, we look at other ways in which security professionals can now use SDN to improve enterprise security. Our first contributor, Craig Mathias, considers mobile security and how to use SDN to lock down those pesky mobile endpoints. He draws the conclusion that SDN might just become the only viable mobile security strategy in the not-too-distant future. Next, Kevin Beaver discusses how SDN enables the security-enhancing process of network microsegmentation. Finally, Keith Townsend looks at an emerging application of SDN to security, a technique he terms 'no-touch' network administration.

Software-defined networking is not really a new idea, but discussions of it can often feel nebulous. This guide aims to solidify the notion of SDN by looking at three specific ways IT professionals can implement it to improve network security. Our hope is that infosec pros will come away with both a deeper knowledge of SDN in general but also a specific collection of new tactics to apply to their network's security.

When will SDE—software-defined everything—arrive? Hard to say. But it's clearly time to apply SDN to security. ■

Brenda L. Horrigan, Ph.D.
Managing Editor
Security Media Group

SDN's Key Role in Mobile Network Security

MOBILITY ARRIVED AT the center of IT strategy, technology, planning and operations about a decade ago, and continues to drive IT spending and evolution in almost every organization today. Key activities include implementing mobile operating policies; monitoring network (particularly Wi-Fi) capacity; and managing devices, applications, content and remote access.

But no IT requirement is more important than security—without security, we never have a valid IT approach. In an era of hackers, breaches, data theft and an increasingly demanding regulatory environment (corporate governance, Sarbanes-Oxley, PCI DSS and HIPAA, just to name a few), we need to extend the security capabilities implemented within networks and their management systems to mobile-centric organizations. Why? Because endpoint security alone, the traditional focus of mobile network security, is proving insufficient at best.

THE NETWORK'S ROLE

Even with today's evolved mobility-management tools, endpoint security remains difficult due to the diversity of devices, users, applications and networks—and is inadequate, given the requirements for end-to-end security needs. The network itself must therefore play a key role in mobile security.

Core mobile network security requirements include policy enforcement, authentication

Even with today's tools, endpoint security remains difficult to manage due to the diversity of devices, users, applications and networks.

(identity management, the successor to AAA, for both the device and the network) and encryption of sensitive data (whether on a device, on a server or in transit). Organizations must also secure device updates, protect against malware, and maintain overall network and service integrity. Mobility introduces another complication: the use of third-party networks from cellular to guest-access Wi-Fi.

Fortunately, today's organizational networks can address many of these issues, with centralized authentication, VPNs and mobile network security policy enforcement capabilities. But a major challenge remains: Security threats are not static—they change and evolve with frightening regularity. So, traditional network-centric security is going to have to evolve to meet these new challenges.

AN SDN FRAMEWORK

Again fortunately, though, we have at least a conceptual framework for the future of mobile network security: software-defined networking (SDN). SDN's most visible appeal is that it extends the traditional mix-and-match interoperability that has defined networking to date with a degree of programmability and adaptability that brings new cost, management and operational benefits. Key among these is the introduction of new security methodologies that fit perfectly with today's mobile-centric IT strategies. SDN can adapt to changing conditions, including fluid and unpredictable security threats.

What's more, SDN is becoming a major factor in the evolution of networking as a service, moving key networking functionality, including security, into the cloud—the same cloud that is also central to mobility. In fact, SDN-based network functions virtualization (NFV) will likely form the backbone of a very large number of organizational networking initiatives going forward. Want to check for malware, look for traffic patterns that might represent an attack or dynamically re-configure the network to repel or at least counter a security threat in a mobile-centric world? Think SDN, NFV and cloud. Oh, yes—all of this also works for the wired portions of the network.

The bottom line? First, SDN is the key direction for networking today, and, while the

benefits of SDN extend far beyond security alone, security needs may very well provide the key justification for its implementation. Policy-based SDN is an ideal vehicle for implementing—and updating as new threats are identified—security across the entire network, right to the mobile edge. Virtualization enables the transparent and universal implementation of key security functionality. Ultimately, there is no easier or more effective strategy for mobile security—and security overall.

PROCEED WITH CARE

A cautionary note: The programmability that is essential to SDN requires its own security; the viability of SDN itself is called into question if, for example, an SDN controller is hacked. But, again, when it comes to security, no one is ever "done," and the likelihood that good solutions to the infrastructure integrity challenge will become common is high.

SDN will reshape the nature of mobile security and could even become the only—not just dominant—security strategy.

SDN's fundamental adaptability will play a central role in the future of mobile network security, whether in-house, in the cloud or in a hybrid setting. SDN will, in fact, reshape the very nature of mobile security, and may even become the only—not just dominant—security strategy going forward. —*Craig Mathias*

Smarter Security Through Microsegmentation

IT AND SECURITY professionals are increasingly looking for ways to better address the security challenges of virtualization. Network segmentation has been in the spotlight lately largely due to the stringent requirements of the Payment Card Industry Data Security Standard.

Network virtualization technology from vendors such as VMware, Palo Alto Networks and Cisco Systems promises to help address virtualization issues through a process called *microsegmentation*.

The microsegmentation approach to network segmentation is said to improve usability and security by establishing "zero trust" zones where more granular access controls can be enforced. The resulting efforts essentially create isolated virtual networks that run parallel to one another. Effectively, creating zero trust zones with microsegmentation offers a technique to use software-defined networking (SDN) to meet the unique challenges of securing today's data centers. The microsegmentation approach to network segmentation is similar to the way mobile device management products keep business data separate from personal data in a bring your own device setting.

Although microsegmentation and zero trust zones are not new concepts, the benefits appear to be driving deployment momentum in the enterprise.

Before jumping on the bandwagon, however, there are a number of pros and cons for this type of network virtualization for large and small organizations to consider.

PROS OF MICROSEGMENTATION

- More granular control over traditional network choke points, including ingress/egress and cardholder data environments. Such granular control would be more difficult to

implement using traditional network security controls such as firewalls and routers.

- Custom security controls for each virtualized environment persist even when those environments are reconfigured and repositioned around the data center.

- When properly implemented, microsegmentation can simplify incident response and forensics in the event of breaches and other network events that must be investigated.

CONS OF MICROSEGMENTATION

- More granular controls offered by zero trust configurations can translate into more network complexity in areas such as identity management and system monitoring/alerting, and they may also require that more people be involved in the design and administration, including (but not limited to) network architects, security administrators, developers and data owners.

- The process of implementing microsegmentation will inevitably create new demands on budgets and personnel, for initial deployment and for ongoing management.

- As a niche technology, justifying network microsegmentation to management may prove difficult, especially since most enterprises still struggle to get their arms around information security fundamentals.

KEY QUESTIONS

- Do unique access controls exist for sensitive areas of the data center?

- Would this technology help to better enforce existing security policies?

- What gaps currently exist that microsegmentation could address?

- If visibility is minimal, is there a need for more specific information to help manage the threats and vulnerabilities unique to specific network and application environments?

- Is there a business case for keeping specific

traffic and data away from certain areas of the network, including specific systems and devices?

Customer privacy, government snooping and related issues may also be of concern, especially if systems that would fall under the umbrella of these controls are located in the cloud.

Much of this goes beyond specific network and security requirements and depends on an organization's culture and approach to security. Emerging security concepts and technologies, such as zero trust virtualization, need to be on the radar so the risks don't enable exploits.

The absolute last thing anyone responsible for network security needs is to be blind-sided by something that wasn't expected, yet could have been prevented nonetheless.

—Kevin Beaver

Extending SDN with a 'No-Touch' Approach

Software-defined networking, or SDN, is a bit of a loose term, to say the least. SDN means different things to different people. One of the original definitions skewed toward flow control. Network virtualization and NFV are commonly considered SDN. Another conception of SDN focuses on device management and configuration. Using SDN to provide software-defined network security is just as fluid of a topic. VMware's NSX has gained plenty of attention for its ability to protect data in virtualized workloads. Kevin Beaver (IT consultant and contributor to this guide) provided significant details around leveraging the concept of zero trust and network segmentation using network virtualization. In this chapter, I'll take a look at how software-defined network security is possible by extending SDN's role beyond enhanced network capability. I'll examine how SDN requires a new approach to securing the administration of SDN.

CURRENT STATE OF NETWORK MANAGEMENT SECURITY

Before we even start talking about data packets, let's discuss a practical consideration—management security. In today's data center where network automation isn't a commonality, management security hasn't changed in almost 20 years. Today, network managers employ traditional identity and access management (IAM) tools to control and log access to network equipment. In a device-central model, this isn't overly complicated

In the device-central model, security administrators apply device-level rights via TACACS+, which may tie back to LDAP. Advanced environments may deploy role-based security for different layers of access to network functions. A challenge is this approach doesn't account for intent. It takes a deal of effort to tie device-level rights with what ability specific administrators requires. For

example, a junior administrator has the rights to create VLANs to support a general-purpose application. However, the junior administrators shouldn't have rights to create routes from non-secure areas to the PCI zone on the same switch.

SOFTWARE-DEFINED NETWORKING SECURITY

One way to eliminate this security issue noted above is using a "no-touch" design to network changes. Obviously, Web-scale companies such as Facebook and Google have moved away from having engineer logging into individual network devices to make changes. The technology is filtering down to the enterprise-scale data center. I spoke with Matt Oswalt, who is leading an open source project called Testing on Demand Driven (ToDD). ToDD enables network engineers to test network configuration changes. Oswalt views ToDD as a cog in the machine that becomes SDN-enabled automation.

In the future, SDN controllers and supporting applications and tools support a touchless configuration policy. Template-based configuration displaces device-based rules and configuration. Validation of configuration happens via centralized management and security audit tools. Instead of configuring devices via a command-line interface (CLI), administrators would make changes via a centralized orchestration tool. The tools validate that proposed changes are compliant with enterprise data-security policies.

There's a significant amount of work needed prior to reaching a future in which no-touch technology is in wide use and software-defined network security is common. Besides the technology challenge, there needs to be a change in the mindset of existing network managers and engineers. Organizations will need to tear down their conceptions of network change management and security to fully support not just automation but the higher standard for security in today's business climate. —*Keith Townsend*

KEVIN BEAVER *is a consultant with Principle Logic LLC based in Atlanta. He has 26 years of experience in the industry, and performs independent security vulnerability assessments and penetration tests of network systems, among other subjects. He's written 12 books on information security including the best-selling Hacking For Dummies. Reach Beaver through his website and follow him on Twitter at: @kevinbeaver.*

CRAIG MATHIAS *is a principal with Farpoint Group, a wireless and mobile advisory firm. It works with manufacturers, network operators, enterprises and the financial community on technology assessment and analysis, strategy development and the integration of emerging technologies into business.*

KEITH TOWNSEND *is the principal of The CTO Advisor LLC and founder of TheCTOAdvisor.com. His areas of expertise include virtualization, networking and storage solutions for Fortune 500 organizations. Follow him on Twitter: @ctoadvisor.*

TechTarget

Is It Time to 'Software-Define' Your Network Security? is a SearchSecurity.com e-publication.

Robert Richardson | *Editorial Director*

Kara Gattine | *Executive Managing Editor*

Brenda L. Horrigan | *Managing Editor*

Robert Wright | *Site Editor*

Peter Loshin | *Site Editor*

Linda Koury | *Director of Online Design*

Jacquelyn Howard | *Senior Director, Editorial Production*

Joe Hebert | *Managing Editor, E-Products*

Doug Olender | *Senior Vice President/Group Publisher*
dolender@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com