Unleashing IT NEXT-GENERATION DATA CENTER EDITION | VOLUME 5, ISSUE 4

Protecting users and data beyond the firewall

Cisco and Intel® partnering in innovation

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

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 the Cisco 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—use 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 born 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 such as 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 [Cisco] 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.

GIVE THEM A TRY

See how easy it is to protect any device, anytime, anywhere by trying Cisco Umbrella for free at cs.co/Umbrella-Demo. And learn how to protect your cloud applications by requesting a Cisco CloudLock demo at cs.co/CloudLock-Demo.

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