INTERVIEW TRANSCRIPT

Connecting Users to Apps

'It's Just Different,' Says iboss CEO Paul Martini

Paul Martini

Paul Martini is the CEO, co-founder and chief architect of iboss. Prior to founding iboss, he was key architect for a wide variety of complex security and technology solutions for clients such as Phogenix, the U.S. Navy and Hewlett-Packard. He was also a key contributor at Copper Mountain Networks, which was a pioneer in introducing broadband networks used by telcos to build the cloud. His work at Science Applications International Corp. involved building distributed real-time network systems for companies such as Rolls Royce.

The new world of "work from anywhere" is all about connecting users to applications. "It's just different," says iboss CEO **Paul Martini**. Yet, many enterprises still approach this new dynamic with the wrong security mindset. Martini outlines what they're missing.

In this video interview with Tom Field of Information Security Media Group, Martini discusses:

- The true enterprise impact of "work from anywhere";
- If not the VPN, then what?
- The new mindset of security at the edge.

The User Is the New Office

TOM FIELD: Since the advent of "work from anywhere," it has been all about connecting users securely to applications. From your perspective, where are enterprises getting it wrong?

PAUL MARTINI: It's critical that enterprises change the mindset to a model in which the user is the new office. The user connects to applications directly without going through a location such as an office or a data center. Previously, users connected through VPNs and through network security appliances in order to get secure connectivity to the applications they needed. Security was mainly focused on protecting the buildings where employees worked.

> "The user connects to applications directly without going through a location such as an office or a data center. The user is the new office."

Now, where the user is actually working from is not relevant, but enterprises take technology that's designed to protect a physical building and try to adapt it to apply to an individual. They end up overloading their VPNs, forcing traffic through an office. That makes productivity and the end-user experience go down. It makes employees call the help desk to complain about not being able to use their video and meeting apps.

The Future of VPN

FIELD: A year ago when the COVID-19 pandemic started, it was all about the VPN. If that's no longer true, then what are we talking about – a VIP VPN?

MARTINI: The concept of a virtual private network implies security, but the reality is that a VPN securely connects you to an office. It does not provide security within the data itself. At iboss, we don't think you should replace your VPN with any other technology or get a different variation of a virtual private network. The goal should be to either eliminate the VPN altogether or offload all the traffic from it as much as possible.

As applications move from the office to the cloud, private applications are no longer sitting in your building and within your office. Cloud transformation is making the cloud applications that you access private. The future of VPN is having technology that allows you to shut the front door of those cloud applications so that no one can access them unless they're going through a secure connectivity service.

The New Security Mindset

FIELD: In this future, what new mindset are we asking security leaders to adopt?

MARTINI: It starts with acknowledging that the way you connect things and people together is going to be completely different. Then you acknowledge that, without fast and secure connections between users and the applications they need, your cloud transformation is not possible because, without moving data, there is no cloud. Then you think about moving your network security and connectivity functions – such as CASB, malware defense and data loss prevention – from traditional appliances that sit in your data center to a cloud service.

Once those functions sit in the cloud and users connect to those applications, they are connecting through a cloud security service that performs the same functions it did in your data center or offices. You just connect through a service that runs natively in the cloud globally, and you get the same functions. It's much more agile, faster and more efficient versus racking and stacking gear. You can just connect new users through a service that's near them, and they'll be under the same compliance, policy and security that all the others users have.

The Need for SASE

FIELD: What does that mean for new tooling? Are we talking about SASE here?

MARTINI: It is SASE, but there are other terms for it: Zero Trust, or Google calls it BeyondCorp. A lot of vendors are using the terms SASE and ZTNA, or Zero Trust Network Access. Some vendors that traditionally started with appliances are putting those appliances into a cloud like Google or AWS and calling that a cloud service.

“Operating a SASE platform costs less. You get so much savings in core infrastructure and labor related to that infrastructure. And SASE gives you agility.”

But we use SaaS, or software as a service, to deliver our SASE services. It allows you to connect users automatically and to follow users wherever they go. By using SaaS, we ensure that the security and network capabilities that you use today are still possible within the new service.

A true SASE, at least to iboss, is a security edge that people connect through to access virtually anything they need from wherever they sit. But that edge needs to be able to provide the same capabilities that you're used to with traditional network security appliances, like proxies, just without the gear and at scale and at speed.

At iboss, we think containerization is really important. We use it through the platform because it allows us to isolate the traffic as it goes to the service for every organization. That's important, because we believe that delivering SASE services in a containerized or an isolated way is the only way to deliver firewall and proxy functions.

Benefits of the SASE Model

FIELD: As organizations make this transition, what business and security benefits can their security leaders expect to see?

MARTINI: Operating a SASE platform costs less. You get so much savings in core infrastructure and labor related to that infrastructure. You don't have to deal with the gear, the project management of installing the gear or worrying about offices as much. And your resources will be more efficient. When you open a new office, you can connect your remote workforce through a service very quickly without doing the huge project management tasks of moving, shipping and installing gear. And SASE gives you agility. When you don't have to spend six months getting a group of remote workers up and running at a new company you've just acquired, you can spend that time working on other projects.

The iboss Approach

FIELD: What is iboss doing to help its customers to make this transition?

MARTINI: At iboss, we provide a Zero Trust, SASE edge that allows you to virtually connect anything to anything else. By using SASE in a connectivity model, we can ensure that a user, wherever they sit, or a device, whether it's IoT or a smart device, can connect to whatever it needs to through a secure SASE edge. And we include all of the policies and security – CASB, malware events, data loss prevention, filtering, compliance and log visibility – into that service, so you can get them at scale and instantly without having to send data through a VPN.

The cloud transformations that we've accomplished with our customers have been pretty dramatic. We're doing over 100 billion transactions a day through the service. We have 4 billion threats going through every day – malicious source, botnet, C&C callback, infected computers, phishing links. Many organizations do over 1 billion transactions every day through the service. In some cases, we've retired over 340 network security appliances. And that was before COVID-19 hit. Customers told us that without our service, after the pandemic started, they would not have been able to refresh their gear or get people out to the countries where the gear was located. So the transformation prevented a very difficult situation for them. ■

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io