Securing Your Distributed Workforce

A Spotlight interview with Tom Kellermann

“Just in the last three months, we’ve seen a 900 percent increase in ransomware attacks.”[1]

TOM KELLERMANN
HEAD OF CYBERSECURITY STRATEGY
VMWARE

Meet Tom Kellermann

Tom Kellermann is the Head of Cybersecurity Strategy for VMware. Tom serves as the Wilson Center’s Global Fellow for Cybersecurity Policy and sits on the Technology Executive Council for CNBC. In 2008, Tom was appointed a commissioner on the Commission on Cyber Security for the 44th President of the United States.

Q: What’s the best way to maintain employee trust and a ‘security first’ corporate culture when everyone is away from each other, and working from home on their own?

A: Make sure employees understand the context they find themselves in, and the role they play inside the organization. A good message to send is: ‘You, as an employee using a corporate device, are being hunted at home by some of the very best cyber criminals and spies in the world because of who you work for. If your device gets compromised or commandeered at home, it will compromise the network in your home. We’re trying to essentially provide an extension of security for you and your family because we used to be able to protect you from inside our corporate facilities. We can no longer do so, unless you actually leverage NGAV and EDR capabilities on your laptop.

The important point to raise is that EDR only triggers an alert when you’re doing things outside of what you would normally do, because it could actually be someone else using your machine besides you. A good analogy for what NGAV and EDR can do in protecting remote workers is that it’s a combination of surveillance cameras that are motion sensitive and a trained attack dog. The dog is only going to react when it’s ordered to do so or when it perceives a threat against you.

Q: How do you convince executives and other VIPs to agree to give up their devices for threat hunting (and what may seem to them like surveillance)? Will most really give up their own devices to rank-and-file employee scrutiny?

A: As you know, remote workers are under attack, and executives even more so. In 2020, the Internet is a truly hostile environment, it’s truly hostile. Just in the last three months, we’ve seen a 900 percent increase in ransomware attacks.[1] Most executives would never want the end of their career to happen because their laptop was used as ground zero for an attack against their entire customer base, causing irreparable brand damage and millions in financial damages. The harsh reality is that a VPN tunnel is no longer sufficient to protect you against today’s threats. We need the equivalent of a bodyguard, an attack dog, and a motion sensitive camera on an executive’s laptop. In this analogy, that is NGAV and EDR to instantly recognize the behavior of someone else using your device, and then shutting this activity down before it can infect anyone else.

[1] Security Week. “Defending Against the Latest Ransomware Surge”. Torsten George. July 15, 2020.

LEARN MORE

THE FUTURE OF REMOTE WORK: SECURING A DISTRIBUTED WORKFORCE EBOOK

Check out our one-stop-shop eBook for everything you need to know about workforce security, so your users (and you) stay safe while working remotely. After all, the easier you make it for employees to do the right thing, the better the outcome. *carbonblack.com/resources/the-future-of-remote-work-securing-a-distributed-workforce*

Q: How do enterprises balance remote worker privacy concerns with the need to monitor activity to detect and respond to endpoint attacks? For example, now that there are no boundaries between work and home life, how do we ensure that we're respecting employee privacy when monitoring the security of their devices, which they often own?

A: Privacy does not exist in the absence of cybersecurity, and the great hope for data privacy - encryption - is not bulletproof, and remains insufficient for privacy protection. To maintain your own safety and privacy, it is imperative that you implement the latest cybersecurity technologies such as EDR and NGAV. The worst-case scenario in today's world is no longer the theft of your personal data or corporate data. Today's nightmare is that your home, your infrastructure, your IP address space, your brand and your identity are being used to attack everyone who trusts you.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 **vmware.com**