

# HOPZERO Demonstrates “Data on a Leash” Absolute Security Compliance at TechNet Cyber Conference and D.C. Area Seminars

*Ability Determines Where Data is Going, Who is Trying to Access a Restricted Resource and Where a Compromise May Have Occurred*

AUSTIN, TX, UNITED STATES, May 8, 2019 /EINPresswire.com/ -- HOPZERO Corporation, creator of HopSphere Radius Security, announced that it will be exhibiting at the TechNet Cyber conference at the Baltimore Convention Center from May 14-16, 2019 and also hosting three seminars in the Washington, D.C. area. HOPZERO experts will demonstrate and discuss use of its unique flagship product, HopSphere Radius Security, to establish and enforce limits on how far sensitive data is allowed to travel by utilizing the universal network routing principle of hop count, effectively putting data on a “leash.” Using the same cloud-based solution, HOPZERO can also determine where data is going, who is trying to access a restricted resource and where a compromise might have occurred. Bill Alderson, seminar speaker says "We help executives and technologists see packet travel through powerful sensory visualization"

- [TechNet Cyber 2019 Conference](#) May 14-16, 2019
- Baltimore Convention Center, Baltimore, Maryland
- Booth 2941
  
- Free HOPZERO DC Seminars

“The Hidden Security Secrets of TCP/IP” Seminars take place concurrently in Washington, D.C., Baltimore, Maryland and Arlington, Virginia on May 13, 14 and 15, respectively.

TechNet Cyber is an annual conference sponsored by AFCEA, the member-based, non-profit



The graphic features a blue background with binary code (0s and 1s) and server racks. A cartoon character in a black suit is holding a leash attached to a red line that winds through the network. A white box at the top contains the text "HIDDEN SECURITY SECRETS OF TCP/IP" and "Discover How to Nullify Phishing Attacks". Below this, a date banner shows "MAY 13 14 15" with "DC METRO", "BALTIMORE", and "CRYSTAL CITY" above the respective days. At the bottom, the HOPZERO logo is displayed in large black letters, with a red leash graphic extending from the 'O'. Below the logo, the tagline "sensitive data belongs on a leash" is written in red, followed by the text "HOPZERO Puts Vital Data on a Leash".



We help executives and technologists see packet travel through powerful sensory visualization”

*Bill Alderson, CTO*

association for security professionals that provides highly regarded thought leadership, engagement and networking opportunities. AFCEA focuses on cyber, command, control, communications, computers and intelligence to address national and international security challenges. TechNet Cyber showcases some of the most important security innovations and practices in the world.

The “The Hidden Security Secrets of TCP/IP” seminars are

held outside of the conference led by HOPZERO Co-Founder and Chief Technology Officer, Bill Alderson. There is no cost to attend, but advance registration is encouraged since there is limited space in each venue. Attendees will receive a HOPZERO Portal Account for 30 days to [“See Where Your Data Is Exfiltrating.” Registration Here](#)

HOPZERO has created an intelligent data control system to classify and protect data that should stay inside an organization, out of reach from outside or inside cyber criminals. The system protects information, and prevents data-exfiltration with a virtual perimeter that puts a networking-enforced limit, based on hop count, on how far data can travel. Attempts to breach that perimeter and transport data farther than allowed are blocked and an alert issued indicating precisely where the attack came from and what they were after for rapid remediation.

During the conference, HOPZERO will discuss and demonstrate:

- How hop count can be used to put a “leash” on data and critical resources by limiting how far data can travel or from how far a resource can be accessed; data access and transmission could be limited, for instance, to inside a data center or the internal network of an organization.
- How to determine the user and computing device attempting to access a resource protected by HOPZERO.
- How to locate a computing device that may have been compromised by an external attacker and is being used as a pivot point to conduct an internal attack and data breach.
- How to see where data is going from a particular internal resource.

Conference attendees may drop in to visit HOPZERO experts in booth 2941 or potential clients can make an exclusive appointment to ensure uninterrupted discussion and one-on-one advice using [Calendly.com/billalderson](https://calendly.com/billalderson). Those not attending TechNet Cyber 2019 or not available for the Washington, D.C area seminars can also contact the company for a remote briefing and demonstration.

Ben Merritt  
HOPZERO INC.  
+15129659656

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/484538135>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2021 IPD Group, Inc. All Right Reserved.