EINPRESSWIRE

FCI Layers Zero Trust Across Four Critical Areas for Greater Compliance

Creating More Secure Networks, Software, Endpoints and Users

BLOOMFIELD, NJ, USA, July 26, 2022 /EINPresswire.com/ -- FCI has mapped the four critical areas of Zero Trust including: Users, Endpoints, Software, and Networks that are required for true compliance and overall cybersecurity. Clarifying the definition of Zero Trust has become important with everyone posturing themselves as a Zero Trust solution. The simplified version of Zero Trust is that you trust “no one” and “nothing” until verified. FCI’s recent [infographic on Zero Trust](#) outlines who originally coined the term, John Kindervag of Forrester back in 2010. Today’s interpretation of Zero Trust is nicely described by [Deloitte](#) as, “It’s not one solution, but a set of controls and design principles guiding decision-making in security architecture.”

> “
> To clarify market confusion about the term Zero Trust, all four areas including networks, software, endpoints and users must be protected. Having Zero Trust in one area only isn’t complete Zero Trust.”
>
> *Brian Edelman, FCI CEO & Cybersecurity Expert*

Global events have elevated the importance of cybersecurity across all industries, boards of directors and leadership teams. Over a few years, employees went remote during the pandemic, geopolitical tensions increased and so did the sophistication and frequency of attacks. Everyone went on high alert and Zero Trust came to the forefront as a key concept to reinforce.

FCI is unique in its cybersecurity offering. From standalone components to a complete Zero Trust ecosystem solution, FCI analyzes current environments and works with clients to fill Zero Trust gaps. FCI Zero Trust services follow a NIST Framework and ties in regulatory requirements from multiple regulations like SEC, FINRA, and NYDFS, to ensure increased security and compliance. FCI takes clients to Zero Trust in the following areas:

- Software: Hardening software and validating user and endpoint compliance at the time of login to systems of private data.
- Users: Verifying that only authorized users can access private data, endpoints, software, and networks.
- Endpoints: Automating the enforcement of cybersecurity settings and endpoint protection.
- Networks: Enforcing secure and encrypted communication inside and outside corporate

networks.

Wrapped around this Zero Trust Ecosystem are FCI's Security Operation Center (SOC) Services that provides 24x7 cybersecurity monitoring and incident response support.

Brian Edelman, FCI's Founder and CEO comments, "There's confusion in the market today about the term Zero Trust. You have some vendors covering one functionality and others covering a different area - this is "partial" Zero Trust. Everyone now uses the term in messaging, confusing security professionals that need all areas protected, not just one. Having Zero Trust in one area only, isn't complete Zero Trust."

About FCI Cyber
FCI is a NIST-Based Managed Security Service Provider (MSSP) offering Cybersecurity Compliance Enablement Technologies & Services to CISOs and security personnel of Financial Services organizations with prescriptive cybersecurity regulatory requirements. FCI blends best-of-breed technologies, cybersecurity best practices, expertise, and innovation to perform Security Assessments and deliver cloud-based Managed Endpoint and Network Protection. www.fcicyber.com

Michelle Campione
FCI
mcampione@fcicyber.com
Visit us on social media:
Facebook
Twitter
LinkedIn
Other

This press release can be viewed online at: https://www.einpresswire.com/article/582003496