

Editorial Contact

Noah Garrett, NGC Communications, on behalf of MCNC: (252) 423.1277 or press@mcnc.org

MCNC introduces next-level cybersecurity for North Carolina

RTP nonprofit launches cybersecurity practice called Vital Cyber; rolls out new Managed Endpoint Protection Service in a coordinated effort to provide protected connectivity on school and health care networks throughout North Carolina

RESEARCH TRIANGLE PARK, N.C. (Sept. 28, 2021) – Cyber threats are becoming more sophisticated and relentless – forcing organizations to implement advanced cybersecurity services and digital health checks no matter their size. In response, [MCNC](#) today has announced the creation of [Vital Cyber](#) to ensure all of North Carolina’s important community anchor institutions can access affordable and reliable cybersecurity solutions.

As the non-profit operator of the North Carolina Research and Education Network (NCREN), MCNC is an established and trusted technology partner offering a robust portfolio of cybersecurity tools, services, and personnel to help solve today's most pressing networking challenges. Through NCREN, MCNC provides Internet connectivity to every K-12 public school in North Carolina as well as all community colleges, and UNC System institutions. MCNC’s new Vital Cyber protects those in the education community in addition to other sectors such as health care and research organizations with a steadfast commitment to the operational health of their networks.

"We have more than 40 years of experience helping North Carolina institutions with their toughest technology and security challenges," said MCNC President and CEO Tracy Doaks. "Vital Cyber is uniquely qualified to provide world-class cybersecurity services and expertise to protect networks, technology, proprietary information, students, employees, patients, and clients."

MCNC Vital Cyber also announced today that it is partnering with CrowdStrike, a leader in cloud-delivered endpoint and workload protection, to provide its new Managed Endpoint Protection Service to help MCNC clients better defend endpoints – such as desktops, laptops, and mobile devices – from malicious activity. CrowdStrike’s Falcon platform provides AI and ML powered endpoint protection with continuous, comprehensive visibility to endpoint activity to ensure nothing is missed; providing important information for MCNC clients into what is happening on their systems and how to protect users from modern cyber threats.

"MCNC continues to partner with top-tier solution providers to deliver world-class cyber protections for our community," said MCNC Chief Information Security Officer Chris Beal. "An endpoint protection strategy is essential for protecting against today’s complex cyber threats like ransomware. Every endpoint can be an entry point for attackers, and the number of endpoint devices is only increasing with the shift to remote learning, work, and health care. We are pleased to work with CrowdStrike to provide the very best Endpoint Protection Service available today to our clients."

Editorial Contact

Noah Garrett, NGC Communications, on behalf of MCNC: (252) 423.1277 or press@mcnc.org

"Organizations want fast and continuous detection, prevention and response," added James Yeager, vice president of Public Sector and Healthcare at CrowdStrike. "That requires comprehensive visibility across all endpoints and the ability to prevent sophisticated attacks in real-time by blocking persistent attackers from compromising their environments and stealing data. We are excited to work with MCNC to bring the power of the CrowdStrike Falcon platform to academic institutions in North Carolina, establishing fortified defenses for our highly connected students and teachers."

Since 2007, all 115 North Carolina Local Education Agencies (LEAs) have been connected to MCNC's network through the N.C. School Connectivity Initiative (SCI). Educational institutions, specifically public K-12 schools, provide the "soft targets" sought by hackers and cyber criminals. A natural evolution through the SCI is a proactive approach to shoring up technology defenses by prioritizing cybersecurity on school networks.

"As cyber threats continue to evolve, it will be the organizations that address security from both a technology and behavior level that will be the strongest and most successful," explained Beal. "MCNC Vital Cyber is ready to assist and protect against today's sophisticated cyber threats and prepare your organization for what's next."

Vital Cyber supports MCNC's five-year goal to support digital equity and inclusion throughout North Carolina, aiming to ensure equitable access to affordable and protected connectivity for all community anchor institutions throughout the state. MCNC and other collaborative partners continue to build-out a robust suite of customized and accessible cybersecurity tools and services, with two new services in the pipeline for release in June 2022.

MCNC Vital Cyber and the new Managed Endpoint Protection Service powered by CrowdStrike, along with other critical cybersecurity and cyber hygiene best practices, will be a point of emphasis at this year's MCNC Community Day on Nov. 9 at the Durham Convention Center. [Registration](#) is now open for the event (both virtual and in-person options are available).

###

About MCNC

MCNC is a 501(c)(3) non-profit client-focused technology organization. Founded in 1980, MCNC owns and operates the North Carolina Research and Education Network (NCREN), one of America's longest-running regional research and education networks. With over 40 years of innovation, MCNC provides high-performance services for education, research, libraries, healthcare, public safety, and other community anchor institutions throughout North Carolina. NCREN is the fundamental broadband infrastructure for over 850 of these institutions including all public K-20 education in North Carolina. As one of the nation's premier middle-mile fiber backbone networks, MCNC leverages NCREN to customize protected Internet, cybersecurity services, and related applications for each client while supporting private service providers in bringing cost-efficient connectivity to rural and underserved communities in North Carolina.

Visit www.mcnc.org. MCNC Social: [Facebook](#), [Twitter](#), [YouTube](#), [LinkedIn](#).

Editorial Contact

Noah Garrett, NGC Communications, on behalf of MCNC: (252) 423.1277 or press@mcnc.org

Acceptable Use Policy & Forward-Looking Statements

MCNC respects the intellectual property rights of others. MCNC® and other MCNC product and service names may be registered trademarks in the USA. Whenever your document or writing uses any name, material, or information that is a registered trademark or service mark of, or is copyrighted by, MCNC, you are requested to obtain prior written permission from MCNC for such use. All requests for permission to use MCNC or NCREN trademarks, service marks, or copyrighted materials, along with a copy of any materials you wish to use and a description or copy of the document you are writing and a description of where it will be published and/or distributed, should be sent to an MCNC communications representative. In addition, certain statements made herein are considered forward looking, reflecting MCNC's current and future intent, belief, or expectation; however, MCNC undertakes no obligation to publicly update any forward-looking statements herein whether as a result of new information, future events, or otherwise. For additional questions or clarity regarding acceptable use, contact MCNC's communications office.

Keywords & Tags

MCNC, NCREN, CrowdStrike, Cybersecurity, Vital Cyber, Endpoint Protection, Ransomware, Broadband, Education, Telehealth, Networking, North Carolina