Case Study

# UMBC Securing Friction-Free Endpoint Protection Using OnSystem Defender

University of Maryland, Baltimore County (UMBC), one of the country's most innovative universities (US News), is the first to recognize and act upon OnSystem Logic's vision for delivering a best of breed defense against both malware and attacks via application flaws that routinely bypass existing endpoint defenses to deliver ransomware, supply chain, and other attacks.

OnSystemLogic™

Across higher education data breaches are increasing rapidly, successful ransomware attacks and monetary demands are multiplying, the FBI is warning institutions that they are becoming the focus of many cybercriminals; and yet, like organizations everywhere, colleges and universities are struggling to protect their environments from cybercrime.

**CAN WE DEFEND OUR ENVIRONMENTS?** Higher education institutions face a long, steep hill to climb before effectively safeguarding data and resources; and institutional leaders are beginning to look and ask for innovative solutions and not simply more of what they already have. Given current infrastructures, networks, third-party products and systems, and the growing backlog of known vulnerabilities in Microsoft and other leading vendor products, innovative institutional leaders are looking for a different vision for resolution of the problem.

**WE CAN**. One such institution, the University of Maryland, Baltimore County ("UMBC"), has traveled up that hill because of its willingness to listen, consider, test and adopt the product vision and solution brought to them by the team at OnSystem Logic (OSL).

**OSL's VISION FOR UMBC AND OTHERS PROMISES TO RENDER MALWARE BENIGN**. OSL was started by senior cybersecurity veterans who refused to accept an environment within which malware was successfully bypassing existing cyber defenses by hiding inside applications -- where those defenses were non-existent and/or ineffective, and always bypassable by attackers. OSL's vision was to have a product that would run on ANY operating system and ANY form factor, to use crowdsourcing and other means to learn and to enforce the legitimate runtime code paths for accessing rare but critical resources (e.g. code generated on the fly by applications inside themselves or others', known as dynamic code, just in time code, code injection, etc.) within EVERY application.

 | (443) 494-9398 | info@onsystemlogic.com | onsystemlogic.com

Case Study

# *"OnSystem Defender provides a new level of assurance that no level of external or traditional protections can provide."*

**PARTNERING WITH UMBC**. OSL discussed the problem and its vision of the solution with the UMBC senior information management team in 2019. UMBC's team immediately recognized the problem and the value of this new class of solution.

**TESTING & ROLLOUT.** The UMBC team decided to rollout the beta version of the product on a small number of Windows systems in 2019, during which they found the effort to be transparent to their end users, while placing no additional burden on their IT staff. The ease of deployment, coupled with the performance they experienced led the UMBC team to the decision to deploy more widely after OSL met the requirements of the Higher Education Community Vendor Assessment Toolkit (HECVAT) for UMBC. The large rollout of the product started in 2021 and continues.

**OUTCOMES AND LESSONS LEARNED.** The efficacy of the product has been proven at UMBC, other customer sites and in the OSL labs. Fortunately for UMBC, OSL has detected no attacks on their systems. However, attacks have been observed and stopped on other OSL customer systems, including some with never seen before attack techniques based on flaws in one of the Microsoft products, a flaw since addressed by Microsoft after OSL reported it to them.

According to Jack Suess, VP of IT at UMBC, "our work with OnSystem Logic over the last two years has allowed us to watch the product mature and develop into a truly impressive tool for preventing malware from gaining a foothold into a system. We first deployed the tool within our own division, one of the more complex and difficult groups on campus due to the large and diverse set of applications we utilize. After that, we began the process of rolling out the software to our higher-risk departments across campus that work with financial or student data."

Mr. Suess believes "***OnSystem Defender provides a new level of assurance that no level of external or traditional protections can provide***. Most other tools securing our endpoints focus on reactive measures, all of which can be either bypassed or disabled by new zero-day malware. The in-depth understanding of the applications and their behavior within OnSystem Defender provides a new level of assurance that no level of external or traditional protections can provide."

 | (443) 494-9398 | info@onsystemlogic.com | onsystemlogic.com