The game-changing nature **of cyber resiliency**

The latest guidance and evaluation techniques help agencies block, defend and contain adversaries

Todd Helfrich

SentinelOne

The COVID-19 pandemic prompted the largest modernization effort the government has ever seen. However, in addition to the many benefits of that modernization, hybrid work environments have added an ever-growing number of endpoints and created new identity-based vulnerabilities for attackers to exploit.

Agencies can be more strategic in their approach to endpoint security by focusing on cyber resiliency. Although the term has been around for several years, it has been emphasized recently by the National Institute of Standards and Technology (NIST). In response to the White House's executive order on cybersecurity, NIST released Special Publication 800-160 Vol. 2, Rev. 1, titled "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach."

NIST's guidance is helping agencies harden enterprises and develop the ability to rapidly detect adversaries through endpoint behavior analysis, endpoint detection, command line monitoring, exploitation for credential access, forced authentication and event monitoring.

Over the past few years, MITRE Engenuity has performed extensive testing of vendors' endpoint detection and response (EDR) tools. The testing highlights the requirements for monitoring and managing EDR technologies and quickly detecting adversaries. SentinelOne's technology has been top of class for detection and analysis in multiple years of testing.

Identity is the new perimeter

In addition to acknowledging the role that EDR plays in security, many experts are now focusing on identity as the new network perimeter. That's because identity is often at the forefront of attacks. Adversaries can easily harvest and use authenticated identities, whether human or non-human, to maintain persistence and move laterally inside an enterprise without being detected by security systems.

Therefore, it's important to uncover any identity-related cyber hygiene issues, such as cached credentials and over-privileged users, so that agencies can remediate them and shrink the attack surface. Gartner defines identity threat detection and response (ITDR) as the tools and best practices for managing the identity-based attack surface. The importance of ITDR is one of the reasons why SentinelOne partnered with and then acquired Attivo Networks earlier this year.

Furthermore, through MITRE's ATT&CK process, we work with our customers to identify their cyber detection gaps and map adversary attack procedures. We can then use MITRE's D3FEND to help agencies implement countermeasures that prevent adversaries from being successful. In situations where adversaries are already within an enterprise, MITRE's Engage seeks to influence their decision-making and quickly detect the attack procedures they're trying to execute so defenders can block adversaries from advancing.

Those programs augment NIST's Risk Management Framework and cyber resiliency guidance by helping agencies deploy active cyber defense technologies.

Automating endpoint and network security

An official at the Cybersecurity and

Jason Leung

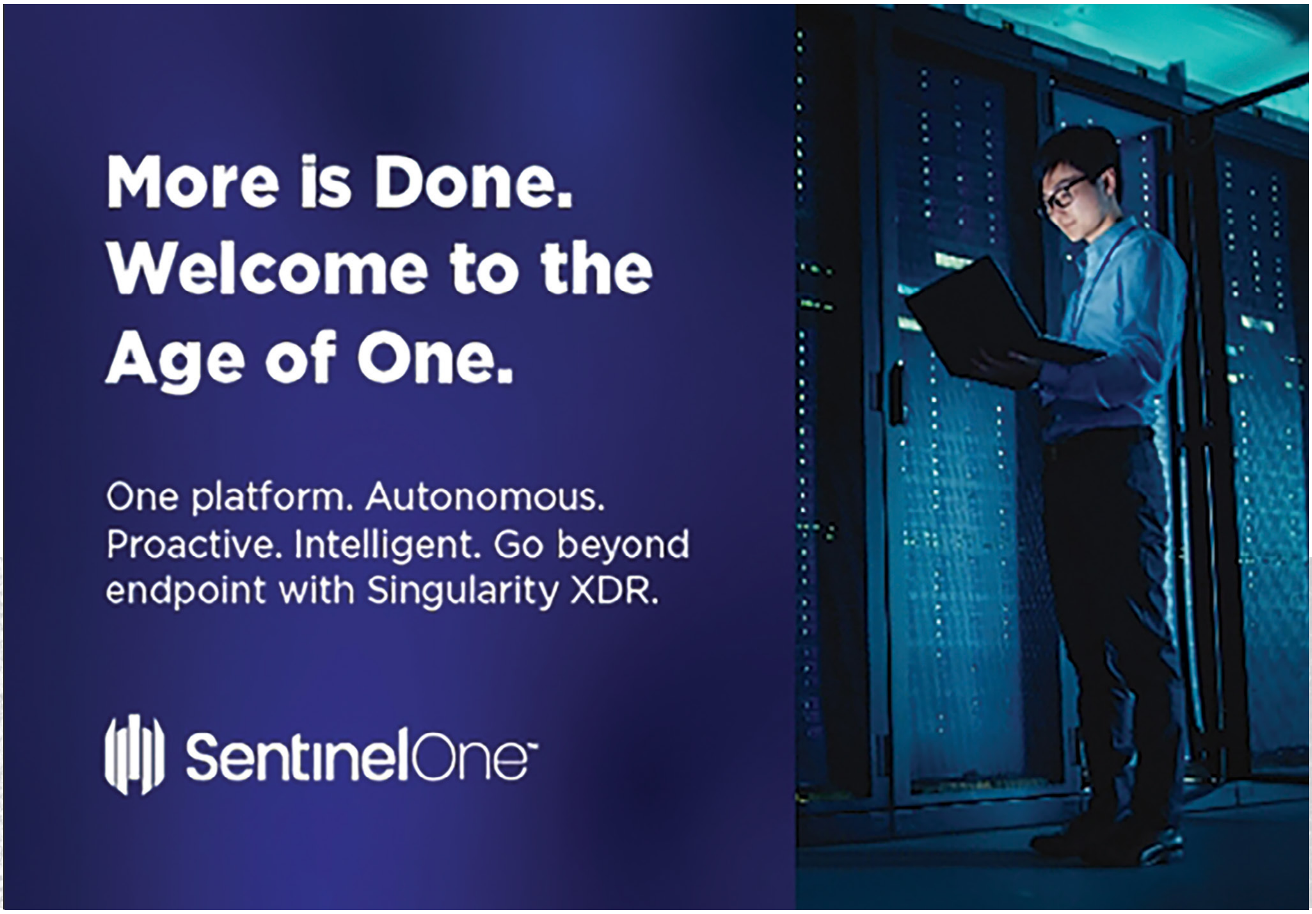
> “Adversaries can easily harvest and use authenticated identities to maintain persistence and move laterally inside an enterprise **without being detected by security systems.”**

Infrastructure Security Agency once told me that if we hired all the people currently studying cybersecurity in undergraduate and graduate programs and put them right into the workforce, we would still be at a 40% deficit.

National Cyber Director Chris Inglis recently announced a cyber workforce strategy that will provide a framework to ensure continued growth in the future. However, in the meantime, the workforce shortage makes automation essential, which is why SentinelOne’s portfolio includes orchestration capabilities that enable us to automate containment and analysis functions. By implementing automation specific to endpoint and network security, agency employees can eliminate routine, manual activities and instead focus on policy, security configurations and cyberthreat hunting to improve their ability to block, defend and contain attackers.

We need to make attacking our networks and systems more costly for the adversary. By implementing cyber resiliency, reducing the identity attack surface and following some industry best practices, we will position our defenders for success. ■

Todd Helfrich is vice president of federal sales at SentinelOne.


More is Done.
Welcome to the
Age of One.
One platform. Autonomous. Proactive. Intelligent. Go beyond endpoint with Singularity XDR.
SentinelOne