Modernizing for the Future of Cybersecurity

How the cloud will enable security effectiveness in the Federal government.

By **James Yeager**
Vice President of Public Sector
CrowdStrike

In 2017, Executive Order 13800 mandated that public sector enterprises must "build and maintain a modern, secure, and more resilient" IT architecture. As adversaries continue to evolve their tactics, techniques and procedures (TTPs), the volume and sophistication of attacks will increase, whether they are from nation-states, criminal actors or hacktivists. The Federal government must be prepared to meet the challenges of today's evolving threat landscape. Implementing these five essential best practices going will go a long way towards securing the Federal domain.

Focus on IT Hygiene

IT hygiene is the foundation of an efficient security posture. Security starts with discovering where you're not protected, so you can close security gaps and be better prepared to face threats. It's imperative that organizations not only understand what software is running in their environments, but also who is leveraging each application. The data that IT hygiene yields is essential to both security and IT teams so they can implement preemptive measures and ensure they are prepared to face today's common and uncommon attacks.

Out-of-date and unpatched applications continue to be a primary attack vector into IT environments. A recent survey notes that 75 percent of organizations cite unpatched and outdated software as their greatest security risk. The ability to discover, patch and update vulnerable applications running in your environment provides a tremendous advantage against attackers. Successfully employing proper IT hygiene measures can also help expose unmanaged assets that pose a considerable risk to the enterprise.

A fully functioning endpoint detection and response (EDR) system should be deployed to record all endpoint activities for deeper inspection, both in real time and after the fact.

Graduate to NGAV

Traditional antivirus (AV) has coasted a long way in the market by touting 97 to 99 percent efficacy rates. However, most security professionals have learned the hard way, that this seemingly small gap of one to three percent provides a huge window of opportunity for adversaries. In addition, legacy AV does not address increasingly sophisticated fileless methods. In fact, studies indicate that many of today's breaches are not caused by malware at all, but rather carried out through social engineering, credential theft or a variety of "living off the land" techniques.

A signature-based approach to security is no longer sufficient enough to keep the enterprise out of harm's way. Next-generation AV (NGAV) goes beyond identifying known signatures to block exploits that leverage vulnerabilities. NGAV needs to fully leverage behavioral analytics and machine learning to identify unknown malicious files, stepping beyond a malware-only focus to look for signs of attack as they occur, rather than after the fact. This approach entails seeking out indicators of attack (IOAs) to identify active attacks, rather than solely relying on indicators of compromise (IOCs), which are only present after an attack has taken place. To effectively achieve this, NGAV solutions must gather enough endpoint activity data throughout the environment to contextualize each IOA with other pieces of information, formulating the most complete picture of the threat.

Put a Premium on Visibility

Mission defenders cannot protect what they cannot see. Regardless of how advanced an organization's defenses are, attacks inevitably slip through, causing a "silent failure." Silent failure happens when existing legacy technologies miss a threat without any alarms going off, allowing attackers to dwell in an environment for days, weeks or months without detection. This is why operators need to have full visibility across all of their assets at all times. A fully functioning endpoint detection and response (EDR) system should be deployed to record all endpoint activities for deeper inspection, both in real time and after the fact.

EDR provides operators with the visibility and capability to proactively hunt through large volumes of data to find malicious patterns of activity that may not have been detected otherwise. Most importantly, EDR tools must offer an easy way to mitigate a breach that is uncovered, including containment of exposed hosts to stop a potential breach in its tracks, allowing remediation to take place before damage occurs.

Hunt for Threats

At the end of the day, attackers are people, and people are adaptive and creative. Defenders are at a major disadvantage if they rely on technology alone to counter every attack. Today's adversaries are committed and resourceful. An effective endpoint security strategy must be bolstered by a team of security experts hunting across the enterprise and proactively looking for threats. An elite hunting team can find things that may have been missed by automated response systems. Threat hunters learn from prior incidents, leveraging telemetry data, analyzing it thoroughly and providing customers with response guidelines when malicious activity is discovered. Managed hunting pits the brainpower of expert human defense teams against the ingenuity of determined adversaries.

Establish a Security Ecosystem

There is no silver bullet in security. However, many tools have been engineered to work well with others. It's important to develop a full-spectrum cybersecurity ecosystem, which functions like an immune system, with each component of your defense strategy working in harmony to form a robust and resilient infrastructure. Endpoint tools must integrate with central and perimeter network appliances, all of which must be able to feed front-end analytics platforms. Invest in tools that are fully open and only engage with solution providers who have an integration strategy that meets your security needs. ■