BROADCOM

Adopting a highly adaptive defensive posture

By unifying threat prevention, detection and remediation, agencies can become more proactive in responding to risks and breaches

Justin Falck
Broadcom

Government networks face ever-evolving threats, and bad actors are constantly looking for ways to improve the effectiveness of their attacks. The latest top-tier threats involve stealing legitimate users' credentials, gaining access to an unmanaged device and then moving laterally across a network, and exploiting a vulnerability in a third-party supplier's system to reach a government network. Adversaries are also taking advantage of endpoint-related blind spots more than ever.

The most effective attacks blend in with users' behavior patterns and tap into the network's existing tools. These "living off the land" attacks are low and slow and can evade traditional detection methods.

Defenders can counter all those threats by adopting a zero trust architecture, integrated security platforms, and intelligence-driven threat prevention and detection.

Achieving real-time visibility across the entire network

The key to success is to become more proactive in preventing threats and reducing security risks. Agencies can start by achieving real-time visibility across the entire network, including endpoints and data. That visibility is a crucial first step in the shift to threat-informed prioritization of risks.

Agencies need to understand their current exposure so they can model likely attack paths. Sophisticated threat actors exist and should be part of an agency's threat model, but it is far more likely that an agency will be hit by a ransomware or phishing attack or infiltrated by someone who wants to use its infrastructure to mine cryptocurrency. Security teams need to focus their efforts on preventing and stopping those kinds of attacks.

The best defensive posture is highly adaptive and can be achieved by investing in solutions that integrate threat prevention, detection and response and that learn from every incident. Such tools prioritize threats based on ease of exploitability and potential impact. That kind of insight helps agencies focus on what really matters. And they should continuously validate their security controls via red team exercises.

Incorporating data protection into threat prevention

Data protection should also be incorporated into threat prevention efforts because those activities are two sides of the same coin. Although attackers may have different end goals, most of them will exfiltrate sensitive data at some point during an attack. So a threat that starts on an endpoint, for example, quickly leads to data loss if the attacker is not stopped.

By combining data protection with threat prevention, detection and response, defenders will receive better detection signals and can more easily prioritize the way they respond to potential attacks that target critical data. In addition, when defenders reduce the possibility of losing sensitive data, they improve their ability stay in compliance with government security policies.

Threat detection and response are core requirements of the Federal Information Security Modernization Act, various security standards issued by the National Institute of Standards and Technology, and multiple executive orders that seek to prevent data access and exfiltration by bad actors. Those directives also have audit and documentation requirements, and they emphasize the need to ensure the availability and integrity of data.

Without a strong ability to detect breaches and respond accordingly, agencies will not be able to stop unauthorized access to data. Furthermore, they will not know if attackers have corrupted or modified their data. However, a highly adaptive defensive posture means that when a breach happens, agencies know exactly what the attacker did, how to stop the attack and what to do to keep such an incident from happening again. ■

Justin Falck *is head of product for endpoint security at Broadcom.*

“ALTHOUGH ATTACKERS MAY HAVE DIFFERENT END GOALS, MOST OF THEM WILL EXFILTRATE SENSITIVE DATA AT SOME POINT DURING AN ATTACK.”

ADOBE STOCK// ALI