Why Endpoint Resilience Matters

Last month, LastPass, a password management firm, made headlines by revealing that one of their DevOps engineers had a personal home computer hacked and implanted with keylogging malware, which subsequently led to the exfiltration of corporate data from the vendor's cloud storage resources. The story shines a rare spotlight on the importance of endpoint resilience. Typically, media coverage of mega breaches (e.g., AT&T, Independent Living Systems, Zoll Medical Data, Latitude Financial Services) focuses on the tail end of the cyber-attack life cycle, namely the exfiltration points rather than how the threat actor got there. However, post-mortem analysis has repeatedly found that the most common source of a hack is compromised credentials that are subsequently used to establish a beachhead on an end user endpoint (e.g., desktop, laptop, or mobile device). This is why in-depth cybersecurity strategies should incorporate endpoint resiliency as an essential component of the overall approach.

Today's Cyberattack Lifecycle

Most of today's cyberattacks are front-ended by credential harvesting campaigns that use social engineering techniques, password sniffers, phishing campaigns, digital scanners, malware attacks, or any combination of these. Cyber criminals also take advantage of millions of stolen credentials being sold on the Dark Web.

Once in possession of stolen, weak, or compromised credentials, attackers are leveraging brute force, credential stuffing, or password spraying campaigns to gain access to their target environment. Increasingly, cyber adversaries take

advantage of the fact that organizations and their workforce are relying on mobile devices, home computers, and laptops to connect to company networks to conduct business. In turn, these endpoint devices become the natural point of entry for many attacks. In fact, a Ponemon Institute survey revealed that 68 percent of organizations suffered a successful endpoint attack within the last 12 months.

As a first step to protect endpoints and minimize their risk exposure, many organizations deploy security tools like data loss prevention; disk and endpoint encryption; endpoint detection and response; anti-virus or anti-malware. However, IT and security practitioners have little visibility into the efficacy of these tools. For example, security applications that go unmonitored on endpoints, can easily degrade and become compromised. Application health can be affected by many things, including lack of updates, software collision, unintentional deletion by end users, and malicious compromise.

A study conducted by Absolute Software on the efficacy of enterprise security controls, found that security tools were typically working effectively on less than 80 percent of devices, and in some cases the number was as low as 35 percent. The lack of efficacy often allows cyber adversaries to move laterally to perform further reconnaissance and identify IT schedules, network traffic flows, and scan the entire IT environment to gain an accurate picture of its resources, privileged accounts, and services. Domain controllers, Active Directory, and servers are prime reconnaissance targets to hunt for additional privileged credentials and privileged access.

Once an attacker has identified where valuable data resides, they typically look for ways to elevate access privileges to exfiltrate the data and conceal their activity to avoid detection. But even the endpoint itself provides a treasure trove for hackers, as more than 76 percent of enterprise devices contain sensitive data, on average.

Boosting Endpoint Resilience

When establishing visibility and security controls across endpoints, security professionals need to understand that each endpoint bears some or all responsibility for its own security. This is different from the traditional network security approach, in which case established security measures apply to the entire network rather than individual devices and servers. Thus, making each endpoint resilient is paramount to implementing a successful defense strategy.

To counteract human error, malicious actions, and decayed, insecure software, Forrester Research recommends taking a pro-active approach to endpoint security and establishing endpoint resilience by:

- Maintaining a trusted connection with endpoints to detect unsafe behaviors or conditions that could put sensitive data at risk. This includes maintaining granular visibility and control over endpoint hardware, operating systems, applications, and data gathered on the device; and self-healing capabilities for the device, mission-critical security controls, and productivity applications.
- Ensuring that endpoint misconfigurations are automatically repaired when possible, as organizations cannot assume that the health of their IT controls or security tools installed on their employees' endpoints will remain stable over time.
- Focusing on the return on investment of the security tools being used. Organizations often use a variety of endpoint security and management tools. Yet, each new tool introduced can serve as both a potential risk and an operational burden. Maintaining continuous endpoint visibility ensures that controls are always working as intended. By doing so, IT security professionals will ensure the ROI of their security investments – both from risk reduction and operational perspectives.

When modernizing endpoint management strategies, organizations should consider resilience as part of their planning process since there’s no guarantee that security controls installed on employee’s devices will not degrade or become compromised over time.

Why Endpoint Resilience Matters