IDC TECHNOLOGY SPOTLIGHT

Key Considerations for Securing Privilege on the Endpoint

December 2016

Adapted from *Security Survey Analysis: Growing Interest in Data Security, Endpoint Security, and Network Security Products*, by Robert Westervelt, Robert Ayoub, Sean Pike, Pete Lindstrom, IDC # *US41694116*

Sponsored by CyberArk

The constant litany of corporate data breaches continues despite the fact that many companies have adopted modern security solutions designed to detect malware and the activity of attackers. Security solutions designed to detect targeted attacks and so-called advanced threats on endpoints play an important role, but far too often enterprise CISOs may be overlooking the underlying issues that can result in costly data exposure or theft. This Technology Spotlight explores how enterprises can significantly reduce the attack surface and drive up the cost of carrying out an attack by removing local administrator privileges and adopting a modern application control solution. It explains why simply adopting modern endpoint anti-malware products without additional controls leaves gaps that significantly reduce the value of the investment. It also describes the role that CyberArk plays in addressing malware and non-malware-based threats with its privileged account security solution for endpoints.

Threat Landscape: Local Admin Rights Fuel Costly Data Breaches

The endpoint continues to be the front line where attackers gain initial entry into the corporate network. Security controls are critical in detecting and containing attacks at the earliest stages, before real damage is done. This has become increasingly difficult because criminal groups have become highly organized and sophisticated in their approach. They frequently conduct reconnaissance of their targets to identify key users. Social engineering attacks have become extremely convincing, making it increasingly difficult for end users to identify valid messages from those containing malware and malicious links. As a result, attackers are getting into corporate networks at an alarming rate. The best defense is an internal security strategy that stops the advancement of attacks once inside and one that reduces risks posed by insiders.

Countless data breach investigations have uncovered the threats that pose the biggest risks to organizations including:

- *Exploiting Local Admin Rights:* Attackers take control of endpoint systems that have local admin rights because it gives them the tools they need to pivot to the sensitive data they are targeting**.** The best practice is to harden the endpoint by removing local administrator rights from business users. This reduces the attack surface and prevents attacks from establishing a foothold. However, many organizations refuse to remove local admin rights since the trade-off between security, usability and supportability is too painful.
- *Account Credential Theft*: An attacker that has evaded existing perimeter and endpoint security controls will try and steal credentials to elevate privileges and move through the network looking

for sensitive information. It is substantially more challenging to steal Windows credentials if the attacker does not have local admin rights but it is a trivial task to access the credentials saved by web browsers such as Chrome. Even if an endpoint is hardened with application control, a determined attacker could use process injection techniques to evade a stringent default deny application control policy.

- *Insider Threats:* This accounts for both insiders with malicious intent and unintentional employee errors. There are countless reports of malicious and disgruntled employees being a primary cause of IT sabotage. The U.S. Computer Emergency Response Team reports that an overwhelming majority of saboteurs are long-term employees that grow frustrated with a lack of career progression. Trusted insiders can become possessive over privileged access or control over data or systems. These malicious insiders can use their own credentials to steal information or obtain the credentials of all users with local access rights or simply steal a browser's password file. The rights granted to them gives them the ability to establish backdoor accounts or deploy remote access tools to disable and bypass security controls. Proactive monitoring and regular audits of access logs could identify suspicious activity but this could be too late to prevent the information theft
- *Ransomware:* One of the more insidious threats, ransomware has been the fastest growing threat in recent years targeting both consumers and businesses. The extortion scheme often has organizations reassessing their data governance strategy. A recent IDC survey found a renewed focus on modern endpoint security solutions and products designed to increase visibility and control over sensitive data. This is driven in part by the precipitous increase in ransomware infections.

When an attacker gains access to a local administrator account, the chances of success grows dramatically because they gain the ability to use remote access tools and functionality that should be reserved for IT personnel. The massive data breach at retail giant Target in 2013 is an example of how anti-malware alone often fails to recognize the use of legitimate system tools and gives attackers the ability to execute malicious files on endpoint systems that could have benefited with additional security best practices.

After using a variety of techniques to gain remote access to Target’s point-of-sale systems, attackers had the ability to use IT administrative tools and run custom malware on the payment system terminals, effectively scraping sensitive credit card data. The combination of removing local administrator rights and implementing application whitelisting may have deterred or at least delayed attackers long enough for other security defenses to detect suspicious activity.

In addition to removing local administrator privileges, organizations should consider better management over user access rights, and adding real-time monitoring to quickly spot suspicious activity. The 2012 data breach at the South Carolina Department of Revenue demonstrated what could go wrong if a system is compromised and an attacker gets the “keys to the IT kingdom.”

Forensics investigators concluded that the attacker used at least four valid user accounts during the attack. The attacker remotely logged into a user workstation at the state agency and leveraged the access rights to penetrate the agency’s revenue systems and databases. A backdoor was installed on an endpoint to maintain a stealthy presence for more than two months, using malware and standard administrator utilities to compromise 43 other systems. After gaining the encryption key, the attacker stole the personal data of millions of residents before law enforcement detected the leak.

Most Endpoint Security Solutions Are Reactive

Enterprises have shifted a significant amount of attention to protecting endpoint devices because laptops and workstations are the most frequently targeted attack vector used by cybercriminals to gain initial access to the corporate network. Enterprise endpoint devices are a favorite target of attackers because they typically contain the most vulnerable software and enterprises often give end users the ability to download and install just about any kind of application.

This capability gives cybercriminals a broad array of software to exploit. If successful, most modern attacks result in complete control of the endpoint PC without the victim’s knowledge. Combined with poor password management and other inadequate controls to enforce security policies, attackers have demonstrated that most organizations leave a low-barrier for them to gain an initial foothold into the corporate network.

Traditional enterprise antivirus is no longer keeping up with the pace of new malware variants used by cybercriminals, with some estimates indicating more than 400,000 new threats surfacing daily. A recent study conducted by IDC found that most enterprises considered replacing traditional endpoint antivirus with modern endpoint and network products to prevent targeted attacks and other threats to critical corporate assets. According to the study, mitigating laptop and workstation risks was the biggest challenge to enterprise client networks, based on surveying more than 350 security consultants, systems integrators, and resellers.

Stronger threat detection alone doesn't solve underlying issues. Modern endpoint security solutions have flooded the market with novel threat detection approaches, but they continue to focus on detecting malware rather than preventing the underlying causes of most breaches. Significant gaps remain. These solutions are mainly reactive in nature and prevention capabilities are often not enabled by default to avoid false positives and end user disruption. Organizations also find they require managed and professional services to get the full value out of forensics data, investigation, and remediation tools.

These modern endpoint security solutions don’t rely solely on signatures to identify threats. They examine system and user behaviors, monitor memory and applications for abnormal activity, and can alert and sometimes prevent malware from executing. However, IDC interviews with early adopters of these solutions found that, while these products generally provide better security, they are certainly no silver bullet. Many enterprises fall short by failing to apply endpoint security best practices thereby leaving significant gaps in protection.

Effective Endpoint Security: A Comprehensive Approach

IDC interviews with enterprise CISOs across a variety of industries found an overwhelming number of IT security teams taking steps to increase their security posture in a bid to harden endpoints against targeted attacks. The logical first step is to remove local administrator rights because studies have shown that it can reduce the attack surface by 25% or more. But studies frequently find that many organizations (60% or more) often skip this step because their management solutions lacked the ability to alleviate potential end-user dissatisfaction and increased help desk calls. Other areas of focus when securing the endpoint include disabling operating system and application functionality that isn't required by most end users, establishing stronger patch management practices and identifying and addressing high risk configuration weaknesses.

Removing Local Administrator Rights

For far too long, IT teams, fearful that removing local administrator privileges would result in countless helpdesk calls from frustrated end users, wouldn't take steps to restrict users from privileges they rarely, if ever need. Granting administrator privileges to users increases risk significantly because users gain much more authority than simply the ability to download and install any application they desire. Users gain unfettered access and control over every file, folder and object on their machine. It gives them and any cybercriminal who gains access to their system, complete control of their environment. Users are granted full rights to functions typically granted to administrators, such as debugging programs and the ability to manipulate underlying operating system functions.

Countless data breaches begin with an attacker leveraging local administrator privileges. These cybercriminals have gotten much more creative in socially engineering end users into installing phony antivirus or software updates or tricking them into clicking on a malicious link or a file attachment with embedded malware. Users also take actions that open up their systems to many of these threats such as removing patches that appear to cause system instability, turning off security controls, or simply turning off operating system updates altogether.

In some ways, IT teams were hand-tied. Older operating systems and applications required users to run as local administrators. Removing local administrator rights resulted in immediate pushback from frustrated users who couldn't perform simple changes to their systems and applications crashed. But much has changed. Further, even if local administrator rights are disabled, without application control, users can still install many programs.

There are solutions to manage removal of local administrator rights and combine it with modern application control so that only trusted applications can run without severely impairing user productivity. These security solutions provide mechanisms to detect untrusted applications and prevent them from executing.

Removing local administrator rights is a surefire way to bolster defenses against “pass-the-hash” attacks that start by stealing credentials. The lack of administrator rights blocks access to credential stores and increases the level of sophistication required of criminals to carry out this attack. It forces the attacker to escalate user privileges by exploiting a system vulnerability. The additional step gives security solutions that are focused on monitoring behaviors indicative of this type of attack more time to detect malicious activity.

Other recommended key elements that serve as the foundation of a comprehensive endpoint security strategy include:

- *Patch Management:* Establish a formal patch management program to support a regular patching cycle for endpoint systems. Address vulnerabilities in browsers and browser components, productivity applications, custom software, and operating system vulnerabilities.
- *Password Management:* Forensics investigators tell IDC that the vast majority of the breaches they document involved weak, default, or stolen passwords. Password management is a significant challenge at many enterprises and one of the most basic elements of a comprehensive security program. Implement strict password and account management policies and enforcement mechanisms.
- *Real Time Monitoring:* Continuous monitoring solutions ensure that system resources and applications are performing normally and can spot and block anomalous activity. Consider solutions that can log, monitor, and audit end user actions.

Considering CyberArk

CyberArk Endpoint Privilege Manager provides Windows privilege management and application control to harden the endpoint from malware-based attacks and insider threats. Using analysis of application and user activity, suspected attempts at stealing credentials can be quickly identified and blocked. The product enables organizations to remove local administrator privileges for business users, granularly controlling IT administrator privileges on Windows Servers based on role, and elevating privileges for trusted applications when necessary and authorized. Malicious applications can be immediately blocked, and unknown applications can be “greylisted” and allowed to run in a restricted mode, pending further analysis.

The product enables organizations of all sizes to conduct proactive protection with effective privilege management, application control features, as well as detection, blocking and containment of in-progress attacks in an on-premises or SaaS-based offering. Features include:

- *Trusted Sources***:** allows system administrators to automatically create application control and privilege elevation policies based on trusted sources such as System Center Configuration Manager (SCCM), software distributors, updaters, and more. Trusted sources can be used to automate the creation of privilege policies for more than 99 percent of applications within the organization.
- *Greylisting:* This is an innovative approach that reduces the end user pain perceived with traditional application whitelisting solutions by allowing greylisted applications to run in a restricted mode without Internet connectivity or access to network shares and selected folders. The containment limits the damage a malicious application could cause.
- *Credential Theft Monitoring and Blocking***:** CyberArk Endpoint Privilege Manager monitors user and application behavior to prevent credential theft and contain attacks before they progress beyond the endpoint. In addition, behavioral analytics applied to users and applications identifies and blocks unauthorized access to credential stores.
- *Application Intelligence:* Provides support for application forensic and investigation processes; an aggregated historical timeline is compiled for each application with details such as first seen in the organization, where installed, original source and full family tree.

The CyberArk Privileged Account Security Solution is a unified policy-based offering that secures privileged account credentials and provides an audit trail of their use. It also isolates critical assets from malware, controls privileged access, records command-level details on every privileged session, and provides analytics capabilities to identify malicious privileged user behavior. Built on a common platform, the CyberArk solution offers the ability to protect privileged accounts in major public, private, hybrid cloud, and SaaS environments.

Challenges

CyberArk acquired Viewfinity in 2015, adding granular-level control of Windows end user permissions and application control to its portfolio Viewfinity is newly integrated into the CyberArk portfolio. Viewfinity is offered as an on-premises solution and a SaaS-delivered solution, which may appeal as an entry level offering for some businesses. Support for Mac endpoints is not yet available. The CyberArk least privilege solution for Unix is sold separately.

Conclusion

The endpoint continues to be the focal point where criminals clash with IT defenders on a daily basis. Unfortunately, most organizations continue to invest in sophisticated malware detection technology without addressing endpoint security best practices. This leaves significant gaps that enable attackers to evade detection.

Hardening endpoint systems requires a three-pronged approach beginning with the mastery of endpoint security best practices, adoption of modern endpoint security products, and effective communication of security policies and mechanisms to enforce them. Combined, these steps support a comprehensive endpoint security strategy designed to reduce the attack surface and drive up attacker costs. The following recommendations can have a positive impact on the organization’s overall security strategy:

- *Remove local administrator functionality*: One of the best ways to protect against today's malware and non-malware-based threats is to remove local administrator rights from users on their endpoints. Unfortunately, it is often difficult to do so because certain applications and/or functions require the rights, but effective solutions, such as those from CyberArk, leverage modern application control and limit end user frustration. In addition, consider supporting two-factor authentication to protect users at high risk of being targeted by attackers. Assess the state of privileged credentials throughout the environment.

- *Identify ways to unify siloed security solutions for collective visibility and optimize the endpoint risk management strategy leveraging existing security investments*: Conduct an assessment of endpoint security controls before rationalizing the purchase of emerging technologies. IDC believes the market for some emerging security technologies is grossly overvalued. Some technology areas may not be sustainable, so features and capabilities will be consumed into mature security areas.
- *Conduct an inventory of all endpoints*: Combine threat and vulnerability information with external intelligence to prioritize risk mitigation efforts at the endpoint. Block command-and-control channels for malware calling home from the endpoint.
- *Develop a program that identifies and remediates endpoint vulnerabilities and configuration issues that are at high risk of being targeted by criminals*: Review log and event management systems and identify tools that help incident responders prioritize alerts and efficiently address threats.

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

For more information on IDC visit www.idc.com. For more information on IDC Custom Solutions visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com