EBOOK

ENDPOINT SECURITY REVIEW
A DEFENSE-IN-DEPTH PERSPECTIVE ON RANSOMWARE

INTRODUCTION: REVISITING THE ENDPOINT

The cloud has eroded the once well-defined network perimeter, exposing your business to increasingly sophisticated and damaging cyber-attacks. Inadequately protected desktops, laptops and servers all provide entry points for attackers to steal data and wreak havoc. This is exacerbated by end-users being spread out across multiple (home) offices and geographies and the variety of devices and cloud applications required to do their jobs.

Ransomware attacks are ever evolving and more prevalent than before – directly disrupting business and causing reputational repercussions by making the headlines. Combined with the costs of lawsuits and fines, endpoint attacks cost large enterprises over $9 million. In a CyberArk survey of 1,000 IT security decision makers, 59 percent included ransomware on their list of greatest security risks[2].

Defense-In-Depth

It's time to revisit the endpoint and take a defense-in-depth approach to endpoint security, instituting an assortment of security controls to protect against ransomware. Originally conceived by the U.S. National Security Agency, a defense-in-depth approach employs multiple layers of security to eliminate gaps, reduce attack surfaces and contain risk.

This eBook reviews the five essential elements of a comprehensive endpoint security strategy. A multi-layered endpoint security plan can help you shore up vulnerabilities, improve your security posture and mitigate risk.

The average economic loss from an endpoint attack exceeds $9 million[1]

[1] 2019 State of Endpoint Security Risk, Ponemon Institute
[2] CyberArk Global Advanced Threat Landscape Report

A Defense-In-Depth Approach to Ransomware Protection

Five Essential Endpoint Security Strategy Elements

- Endpoint Detection & Response (EDR)
- Anti-Virus and NGAV
- Privilege Management
- CDR - Email Security
- Application & OS Patching

ELEMENT ONE

ENDPOINT DETECTION & RESPONSE (EDR)

EDR tools let you proactively identify and investigate suspicious activity on endpoints. Originated as an additional security layer back in 2013, EDR solutions continuously monitor, record and analyze endpoint activities, helping IT and security professionals efficiently uncover and mitigate advanced threats.

Many EDR solutions use advanced analytics, analyzing endpoint events to detect malicious activities that might otherwise go unnoticed. EDR tools provide visibility into suspicious endpoint behavior in real-time, helping you to stop threats before they take root and spread across the business.

Extended Detection & Response (XDR)

To uncover more threats and provide more context to their analyses, tools are evolving to include networks, clouds and endpoints with more advanced analytics and automation.

ENDPOINT DETECTION & RESPONSE

Detect and respond to advanced active attacks on endpoints

ANTIVIRUS/NGAV

Prevent malware infection using a variety of techniques

ELEMENT TWO

ANTI-VIRUS AND NGAV

Anti-virus (AV) and next-generation antivirus (NGAV) protection tools help you to detect and remove various forms of malware. Traditional AV solutions identify and block malicious programs by inspecting files and looking for the signature patterns of known viruses. While effective when they were first introduced, these tools don't detect newer types of threats like file-less malware and zero-day exploits. In fact, in a Ponemon Institute survey, 62 percent of respondents said their traditional antivirus solutions mitigates only 50 percent or fewer of attacks[3].

NGAV tools use predictive analytics, artificial intelligence (AI) and machine learning (ML) to defend against contemporary attacks such as ransomware and advanced phishing, which can evade conventional antivirus programs. Unlike traditional AV solutions that scan files looking for known patterns, NGAV solutions take a holistic approach, examining every process running on an endpoint and using AI and ML to intelligently detect and proactively block previously unknown forms of malware.

[3] 2018 State of Endpoint Security Risk, Ponemon Institute

ELEMENT THREE

PRIVILEGE MANAGEMENT

Privilege management solutions help you contain risks associated with privileged accounts such as Windows or Mac administrator accounts. Privileged accounts are used to control files, directories, services and user access rights. In the wrong hands, they can be used to steal data or disrupt systems.

Attackers often try to gain unauthorized access to privileged accounts via malware or phishing attacks at the endpoint. Once they gain a foothold, they can traverse the network looking for high-value targets and use elevated privileges to steal confidential information or disrupt critical applications. Forrester estimates that at least 80 percent of data breaches have a connection to compromised privileged credentials[5].

Solutions help to reduce exposure by removing local administrative rights and tightly controlling user and application permissions based on policy. By enforcing the principle of least privilege – granting users the minimum set of privileges required to perform their jobs – you can prevent lateral movement and improve your security posture, without impairing user productivity or impacting business performance.

Ransomware Protection with Privilege at Its Core

By instituting application controls, some solutions allow you to prevent known malicious applications from running and restrict the operation of unsanctioned applications. This significantly reduces risk and uncertainty. Extended capabilities include the ability to detect ransomware in apps not (yet) covered through policies, the blocking of attempted credential theft and the proactive shutting down of in-progress attacks through privilege deception components, such as local admin deceptive accounts or fake passwords lure.

[5] The Forrester Wave™: Privileged Identity Management, Q4 2018

CDR - Email Security

Protect email accounts against unauthorized access, loss or compromise

ELEMENT FOUR

CDR - EMAIL SECURITY

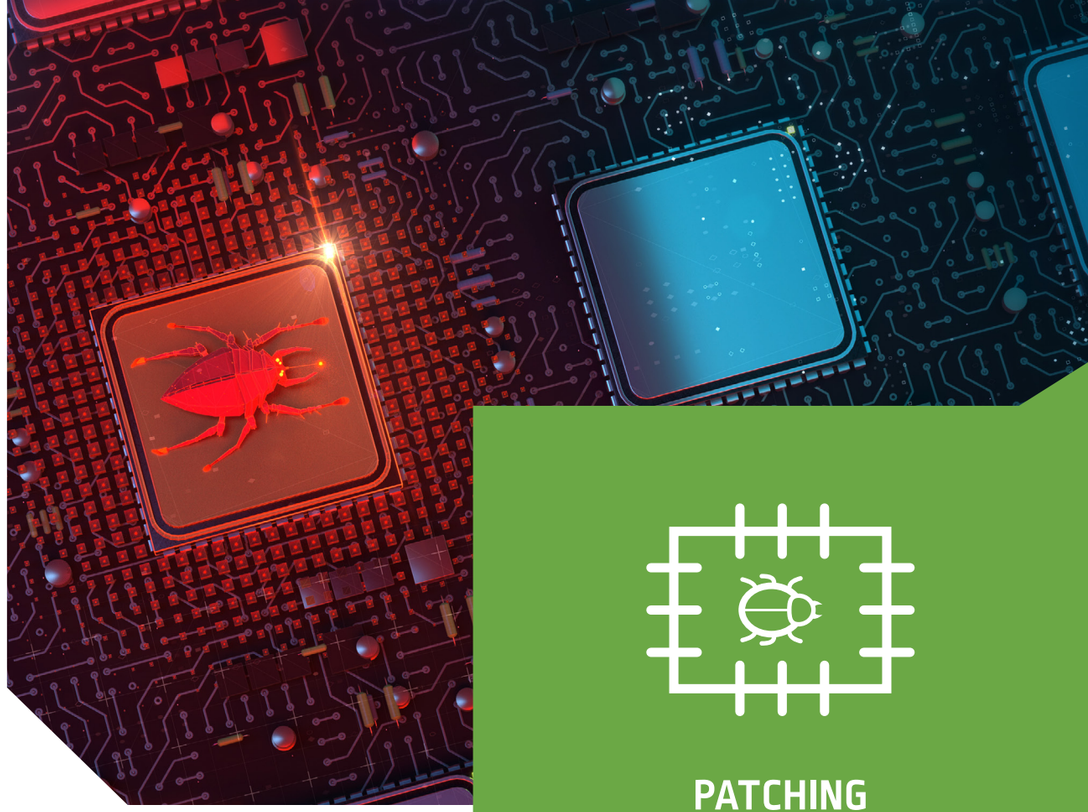
94% of all malware is delivered through email and phishing accounts for more than 80% of reported social engineering incidents[4]. Whilst end-user awareness training plays an important role in addressing these issues, CDR (Content Disarm & Reconstruction) tools offer an additional layer of protection. Traditionally, CDR, unlike EDR, does not detect malicious files but rather allows you to remove components that are not approved through set rules and policies across a variety of sources including email.

Email security capabilities include spam protection, URL analysis, attachment sandboxing, dynamic content filtering, encryption – in addition to archiving and back-up. Some solutions are evolving to leverage AI and real-time end-user intelligence to identify and remove malicious emails. Admin consoles allow you to set policies for users, domains and domain groups, use allow/ deny lists and customize Data Loss Prevention (DLP) rules.

[4] 2019 Data Breach Investigations Report, Verizon

ELEMENT FIVE

PATCHING TOOLS



Patching tools help you efficiently track and implement endpoint software updates to strengthen your security posture. Savvy attackers and cybercriminals constantly seek application and operating system security vulnerabilities to exploit. Software vendors continuously issue patches to address known vulnerabilities[6]. In this ongoing game of cat and mouse, applications and operating systems must stay current to keep one step ahead of the bad guys.

Application Patching

Managing application updates is a challenge for many organizations. According to one study, it takes the typical IT organization an average of 34 days to patch high-severity vulnerabilities . Application patching solutions help you eliminate manually intensive, error-prone and time-consuming patch management processes and improve cyber readiness.

Most application patching solutions provide:

- Inventory scanners to discover all the applications scattered across the business
- Status dashboards and reports to identify patched and vulnerable applications
- Tools to automate patch approval, distribution and the installation processes.

PATCHING

Apply updates to address security issues and bug fixes

[6] Security Report for In-Production Web Applications, tCell by Rapid7

ELEMENT FIVE

OS Patching

Just like application updates, you need to be vigilant with endpoint OS updates. You can reduce security vulnerabilities by instituting automatic OS updates or by implementing other systems and practices to ensure all corporate desktops, laptops and servers run the latest releases.

Each vendor has its own approach to issuing OS patches and must be considered individually. Microsoft releases **security updates** for Windows server and Windows desktop on the second Tuesday of each month. You can install these patches automatically using Windows Update. If you want to test out updates before you deploy them in production, you can use Windows Server Update Services (WSUS) or a third-party application patching tool to distribute and implement OS updates on your own schedule.

Apple releases macOS software periodically (which can include security updates). You can **configure a Mac** to install macOS updates manually or automatically.

SUMMARY

Endpoints pose significant security risks. Savvy attackers can exploit endpoint vulnerabilities to steal confidential information or disrupt IT services, resulting in revenue loss and costly regulatory fines and legal settlements. By taking a defense-in-depth approach to ransomware —instituting a wide range of endpoint security controls—you can strengthen your security posture and reduce exposure.

Privileged management is a critical, and often overlooked, component of an effective endpoint security strategy. Malicious insiders or external attackers exploit endpoint administrator accounts to gain a foothold in a network, and then move laterally to penetrate or disrupt higher-value targets.

Privileged management solutions restrict privileged access and enforce application control, granting users the minimum set of rights required to perform their jobs, strengthening security, without impairing user productivity. This mitigates threats at the endpoint of entry, prevents lateral movement and the spread of malware, ultimately helping you reduce exposure and prevent the encryption of ransomware.

About CyberArk

As the established leader in privileged access management, CyberArk offers the most complete and flexible set of Identity Security capabilities to enforce privilege and enable access across any device, anywhere at just the right time. Powered by AI behavior and risk analytics, CyberArk's Identity Security Platform delivers continuous protection and just-in-time access for any identity – human or machine – as you support a distributed workforce, embrace the cloud and new cloud technologies, and develop customer experiences rooted in trust.

With CyberArk, you add a critical line of defense against ransomware attacks by removing local admin rights and providing just-in-time access to privilege when needed. Combined with Application Control, Credential Theft Blocking and Privilege Deception capabilities, CyberArk provides a comprehensive solution to ransomware protection.

Pre-built integrations and integrations through the CyberArk marketplace underpin our defense-in-depth approach. Expanded capabilities cover threat intelligence, asset data, and other indicators of endpoint security health.

LEARN MORE

03.20. Doc. 50320