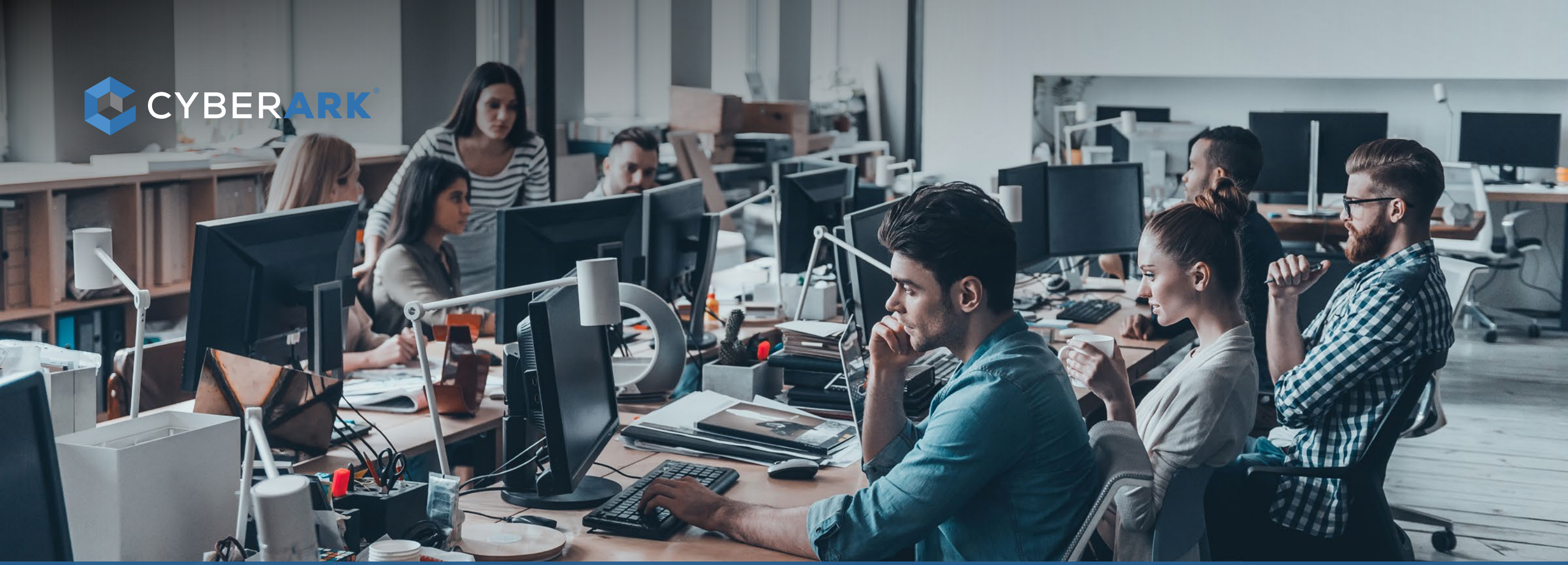


EBOOK

5 ESSENTIAL ELEMENTS OF A COMPREHENSIVE ENDPOINT SECURITY STRATEGY

DIGITAL TRANSFORMATION REQUIRES A FRESH LOOK AT ENDPOINT SECURITY

Today's digital workforce looks very different than it did even five years ago. Employees and contractors are spread out across multiple offices and geographies. Some work from home or from shared workspaces. Most use a variety of devices and cloud applications to do their jobs.

The cloud has eroded the once well-defined network perimeter, exposing your business to increasingly sophisticated and damaging cyber attacks. Inadequately protected desktops, laptops (even macOS!) and servers all provide entry points for attackers to steal data and wreak havoc.

Endpoint attacks, such as phishing and ransomware, can disrupt your business, damage your company's reputation and result in lawsuits or fines. In fact, endpoint attacks cost large enterprises over $7 million on average or about $440 per compromised device.[1] It should come as no surprise that in a recent CyberArk survey of 1,000 IT security decision makers, 60 percent of respondents included external attacks, such as phishing, on their list of greatest security risks and 59 percent included ransomware.[2]

CISOs and IT leaders are fighting back, taking a defense-in-depth approach to endpoint security to reduce exposure. This eBook reviews the five essential elements of a comprehensive endpoint security strategy for your digital business. A multi-layered endpoint security plan can help you can shore up vulnerabilities, improve your security posture and mitigate risk.

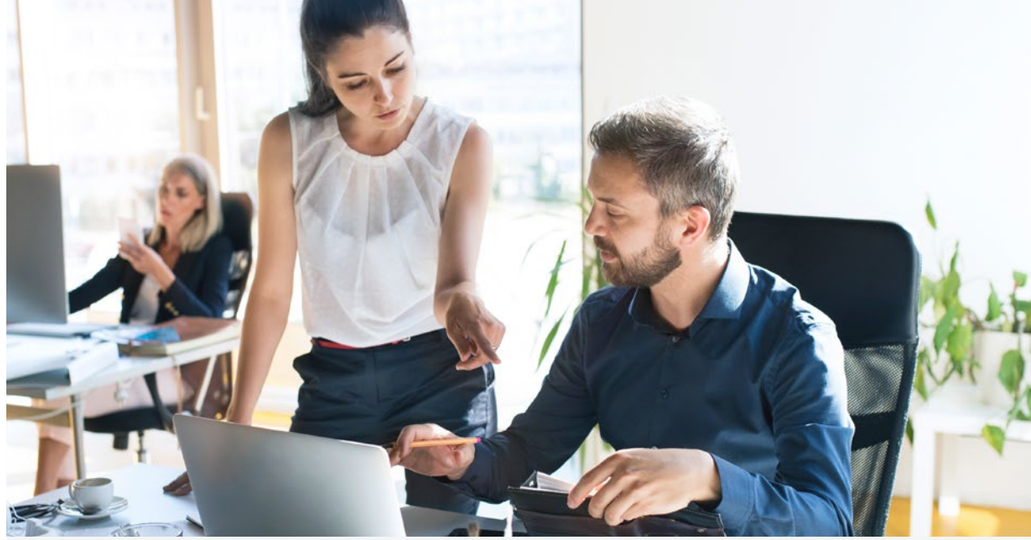
The average economic loss from an endpoint attack exceeds $7 million[1]

[1] 2018 State of Endpoint Security Risk, Ponemon Institute
[2] CyberArk Global Advanced Threat Landscape 2019 Report

A DEFENSE-IN-DEPTH ENDPOINT SECURITY STRATEGY PROTECTS AGAINST A WIDE ARRAY OF THREATS

Digital transformation poses a variety of challenges for security, compliance and risk management professionals. Today's digital businesses are exposed to a wide array of threats –from debilitating ransomware attacks to costly data breaches. Malicious attackers, cybercriminals and even shady competitors can use readily available open source tools to gain access to endpoints and traverse your network to steal confidential information or disrupt services.

Forward-thinking organizations take a defense-in-depth approach to endpoint security, instituting an assortment of security controls to protect against a wide range of threats. 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.



Endpoint

Noun

Any device that provides an entry point to corporate assets and business applications and represents a potential cybersecurity vulnerability. Examples include desktops, laptops and servers.

Five Essential Endpoint Security Strategy Elements

A comprehensive endpoint security strategy includes five essential elements:

- Endpoint detection and response (EDR) tools
- Antivirus and next-generation antivirus protection tools
- Privilege management solutions
- Application patching tools and best practices solutions
- Operating system patching tools and best practices

ENDPOINT DETECTION & RESPONSE

Detect and respond to advanced active attacks on endpoints

ELEMENT ONE:
ENDPOINT DETECTION AND RESPONSE TOOLS

Endpoint detection and response tools let you proactively identify and investigate suspicious activity on endpoints. Most EDR solutions continuously monitor, record and analyze endpoint activities, helping IT and security professionals efficiently uncover and mitigate advanced threats.

According to Gartner, an EDR solution has the capability to:

- Detect security incidents
- Contain the incident at the endpoint
- Investigate security incidents
- Provide remediation guidance

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.

ELEMENT TWO:
ANTIVIRUS AND NGAV PROTECTION TOOLS

Antivirus (AV) and next-generation antivirus (NGAV) protection tools help you to detect and remove various forms of malware. Traditional antivirus solutions identify and block malicious programs by inspecting files and looking for the signature patterns of known viruses. Traditional antivirus tools, while effective when they were first introduced, 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 mitigate only 50 percent or fewer of attacks.[3]

Next-generation antivirus protection solutions 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 antivirus 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.

ANTIVIRUS/NGAV

Prevent malware infection using a variety of techniques

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

PRIVILEGE MANAGEMENT

Manage local administrator rights while maintaining user productivity

ELEMENT THREE: PRIVILEGE MANAGEMENT SOLUTIONS

Endpoint 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.[4]

Endpoint privilege management 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. By instituting application controls, which prevent known malicious applications from running and restrict the operation of unsanctioned applications, you can reduce risk and uncertainty.

Industry analysts, including **Gartner**, call out privileged access management as a top priority for security and risk management leaders.[5] And the **Center for Internet Security** (CIS) recommends controlling use of privileged administrative accounts as a **best practice**.

[4] The Forrester Wave™: Privileged Identity Management, Q4 2018
[5] Gartner, Smarter with Gartner, Gartner Top 10 Security Projects for 2019, June 18, 2019

ELEMENT FOUR:
APPLICATION PATCHING TOOLS AND BEST PRACTICES

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

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.[6] 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

APPLICATION PATCHING

Apply application updates to address security issues

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

OS PATCHING

Provides OS level security bug fixes

ELEMENT FIVE: OPERATING SYSTEM PATCHING TOOLS AND BEST PRACTICES

Leading endpoint operating system vendors routinely issue software updates to fix bugs and address security issues. Just like application updates, you need to be vigilant with endpoint OS updates to keep your digital business safe. 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 operating system 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 every 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 for today's digital businesses. 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 endpoint security—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 often exploit endpoint administrator accounts to gain a foothold in a network, and then move laterally to penetrate or disrupt higher-value targets.

Endpoint privilege management solutions restrict privileged access, granting users the minimum set of rights required to perform their jobs, strengthening security, without impairing user productivity. Endpoint privilege management solutions mitigate threats at the endpoint of entry, preventing lateral movement and the spread of malware, helping you reduce risk and improve digital transformation outcomes.

About CyberArk

CyberArk is the global leader in privileged access security, a critical layer of IT security that protects data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 500, to protect against external attackers and malicious insiders.

CyberArk Endpoint Privilege Manager lets you enforce least privilege security at the endpoint, helping block and contain threats and reduce the risk of information being stolen or encrypted and held for ransom. The solution protects against credentials theft attempts and controls applications, stopping attacks at the point of entry before they can take hold and inflict serious damage. An essential element of a comprehensive endpoint security strategy, CyberArk Endpoint Privilege Manager protects Windows Servers, Windows PCs and Macs and can be easily and quickly deployed as a SaaS solution.

LEARN MORE

03.20. Doc. 50320