CYBERARK®

EBOOK

Best Practices for Ransomware Protection

What to know and do about your business's biggest existential threat

Table of Contents

A Growing, Pervasive Threat

Ransomware has never been more prevalent — or profitable — than it is right now. What started as the exclusive domain of highly skilled and opportunistic cybercriminals has evolved into an underground industry in which virtually anyone can get their hands on pre-built tool kits and plans to launch ransomware attacks at a frightening pace.

Many enterprise security teams continue to search for a “silver bullet” for preventing ransomware, but protecting against ransomware attacks is more of a mentality and a posture than it is about compiling a particular set of tools. As ransomware attacks continue to become more selective, strategic, sophisticated and easier to pull off, enterprises need to change their mindsets and general approach to protecting their most precious assets.

This eBook will introduce you to the most important strategies, insights and steps you can take to minimize your risk of suffering a catastrophic ransomware attack and help mitigate the damage when an attacker inevitably penetrates your perimeter security.

Compared with a year ago, ransomware attacks have increased by

151%

in the first six months of 2021, compared with a year ago.[1]

[1]Seals, Tara. *“Ransomware Volumes Hit Record Highs as 2021 Wears On.”* www.threatpost.com. August 3, 2021.

Multiple Sources, Vectors, and Potential for Damage

Most security threats to a business — physical break-ins via tailgating, stolen documents and leaked access to sensitive information — are perpetrated by a single entity, often with brute force or little in the way of sophistication.

But ransomware attacks are different. They can come from any angle at any time and can be executed by virtually anyone because ransomware has been democratized in a way that dramatically lowers the bar of technical know-how and skill.

Today, there are nefarious groups offering pre-packaged malware-as-a-service such as the Krypton Stealer, professional attackers who breach a security perimeter and sell the breach plan for profit and artificial intelligence (AI) powered malware clients that do the heavy lifting for a would-be attacker.

The result is a thriving underground industry of illicit activity that's wreaking havoc on businesses big and small across industries, markets and geographies — and it's only getting worse.

"Ransomware-as-a-service providers account for 80% of each payment from an attack."[2]

[2] Schwartz, Matthew J. *"Ransomware: Average Business Payout Surges to $111,605."* www.bankinfosecurity.com. April 30, 2020.

Reasons anyone can launch a ransomware attack

- ✓ Introduction of malware as-a-service
- ✓ Access brokers selling breach plans for profit
- ✓ AI-powered attack programs

Ransomware costs billions in damage

- ✓ Malicious emails are up 600% due to COVID-19[3]
- ✓ An insurance company paid a $40 million ransom in 2021, the largest ransomware payout ever[4]
- ✓ Ransomware damages are expected to top $265 billion worldwide by 2031, up from $20 billion in 2021[5]
- ✓ High-value targets like healthcare organizations dedicate only around 6% of their budget to cybersecurity measures[6]

[3] Associated Press. *"The Latest: UN warns cybercrime on rise during pandemic."* www.abcnews.com. May 22, 2020.
[4] Chang, Brittany. *"One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack."* www.businessinsider.com. May 22, 2021.
[5] Braue, David. *"Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031."* www.cybersecurityventures.com. June 3, 2021.
[6] Landi, Heather. *"Could patients be at risk during a hospital cyberattack? It depends how far hackers are willing to go, expert says."* www.fiercehealthcare.com. November 23, 2020.

Old-School Techniques Are No Match For New-School Attacks

The primary reason ransomware attacks continue to increase in frequency and sophistication is because they work. Businesses paying a ransom to recover high-value and sensitive data confirm for attackers that the cyber attacks worked and encourage additional — and even repeat — attempts.

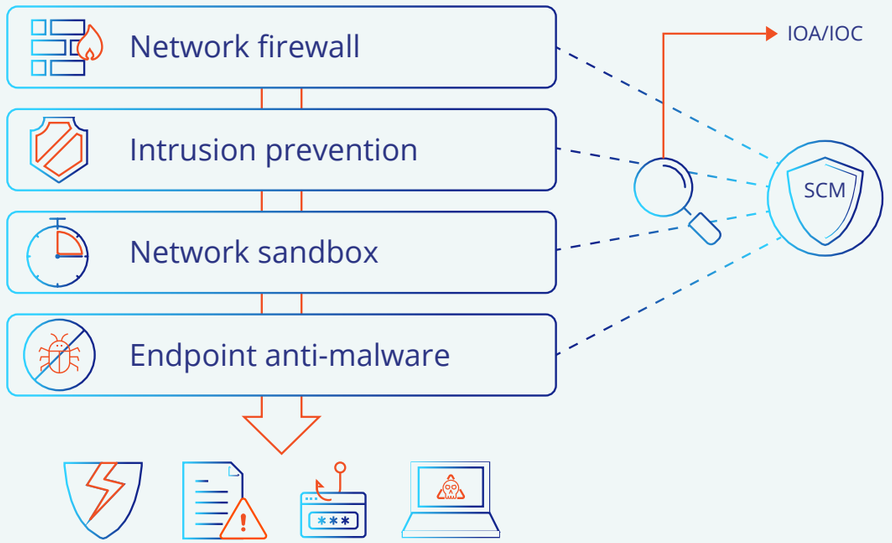
This is the result of too many businesses relying on an all-or-nothing protection strategy emphasizing intrusion prevention and monitoring technologies, rather than a more comprehensive and defensive security posture.

Much like the defense in an American football game must plan for everything the offense throws at them, IT and security teams need to somehow account for the myriad elements, angles and paths a ransomware attack can include.

Popular intrusion/monitoring solutions like endpoint detection and response (EDR), next-generation firewalls and cloud access brokers (CASBs) are designed to protect a traditional IT perimeter that no longer exists.

They rely on known threats and bad behaviors and will frequently miss targeted and zero-day (novel) threats. They also only address one part of a multi-step cyber-attack chain and can be frequently — if not easily — evaded as ransomware developers change behavioral patterns to trick detection tools.

Why the Existing Strategy Does Not Work



But ransomware attacks are multifaceted and multi-step efforts that need only a single unprotected privileged access point to rip through an entire environment. Attacks at endpoints are constant and prove daily they can succeed. Yet, it's what happens next that determines whether the attack is truly damaging or just a near-miss.

Organizations eager for a "silver bullet" in the form of intrusion and monitoring solutions are still at equally high risk of attack because the tools cannot overcome poor security fundamentals. Those who believe simply restoring data from backups or paying a ransom to alleviate a threat do nothing to remove the attackers from the network environment make repeat or ancillary attacks more likely.

Double extortion — exfiltrating data and threatening to leak it or sell it to the highest bidder — has become a preferred tactic of ransomware attackers who've suddenly rendered those backups and data recovery plans worthless as a hedge against paying ransoms.

And if they're relying solely on the good advice of their vendors regarding which tools and solutions to buy, they'll continue with incomplete and unproven security operations that leave them vulnerable to potentially catastrophic attacks.

Fool's Gold: Why your defense-in-depth "silver bullet" doesn't work

- ✓ Long planning timelines: At-risk systems remain at risk until a plan is approved and initiated
- ✓ Long period of data capture and analysis across thousands of users and millions of events slow responsiveness
- ✓ Policies undergo rigorous end user testing/ acceptance and the entire process starts over if proven to be not fit for purpose.

Common poor security fundamentals

- ✓ Limited end-user education and training about protecting workstations and applications
- ✓ Default elevated admin rights across mission-critical systems
- ✓ Security controls are dialed back in favor of user demands and business

5 Best Practices for Ransomware Protection and Damage Mitigation

Business and IT security leaders alike must stake out a more proactive, strategic and comprehensive security posture to protect their organizations from unnecessary and costly damages from inevitable ransomware attacks.

To accomplish that, they'll need to reshape their company's culture and mentality about security, as well as curate the right technologies, strategies and vendor partners. Here are the five best practices for protecting your business against ransomware attacks and large-scale damage.

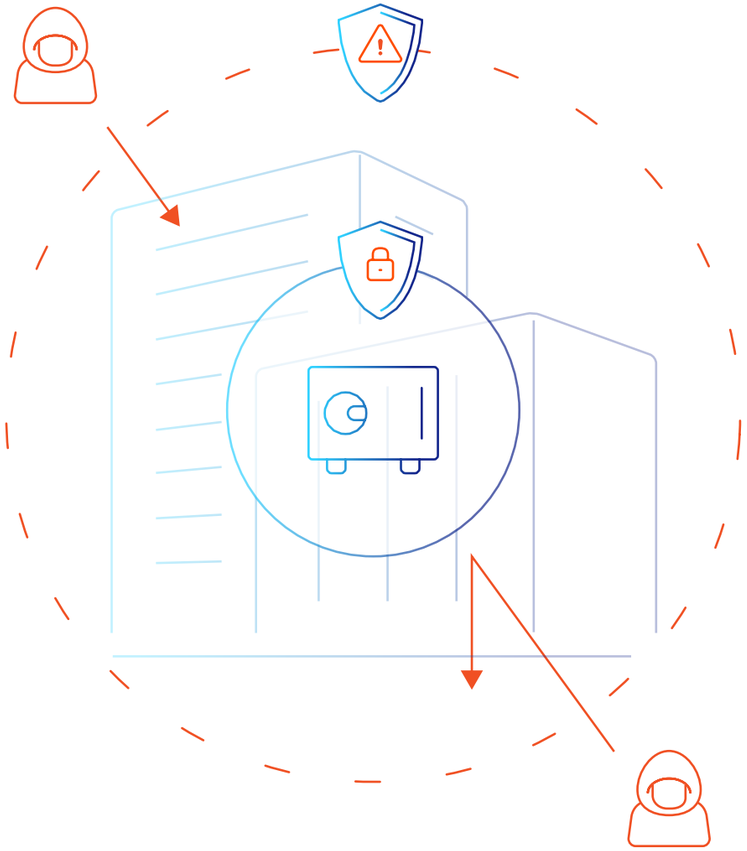
5 Best Practices at a Glance

1. Assume a breach
2. Revoke admin rights across your environment
3. Test and assess your protection and recovery protocols
4. Stack technology and strategies to make attackers' lives harder
5. Get outside help from a trusted partner

Best Practice: 1
CHANGE YOUR MINDSET AND SECURITY CULTURE

For most business leaders, security is a matter of choosing the right detection and remediation tools. But security isn't just a set of products; it's a posture and culture that permeates the organization.

It's important to recognize that today's attackers will always get through eventually. Assuming a breach makes it easier to recognize that the amount of damage they can do is determined by the strength of your company's foundational security practices. Begin by reframing your perspective and assumptions about cyber risk — realize that breaches will happen given enough time — and that adopting a purely defensive posture that focuses time, attention, and resources to mission-critical systems is a more effective strategy than trying to predict every potential attack vector.



KEY TAKEAWAY

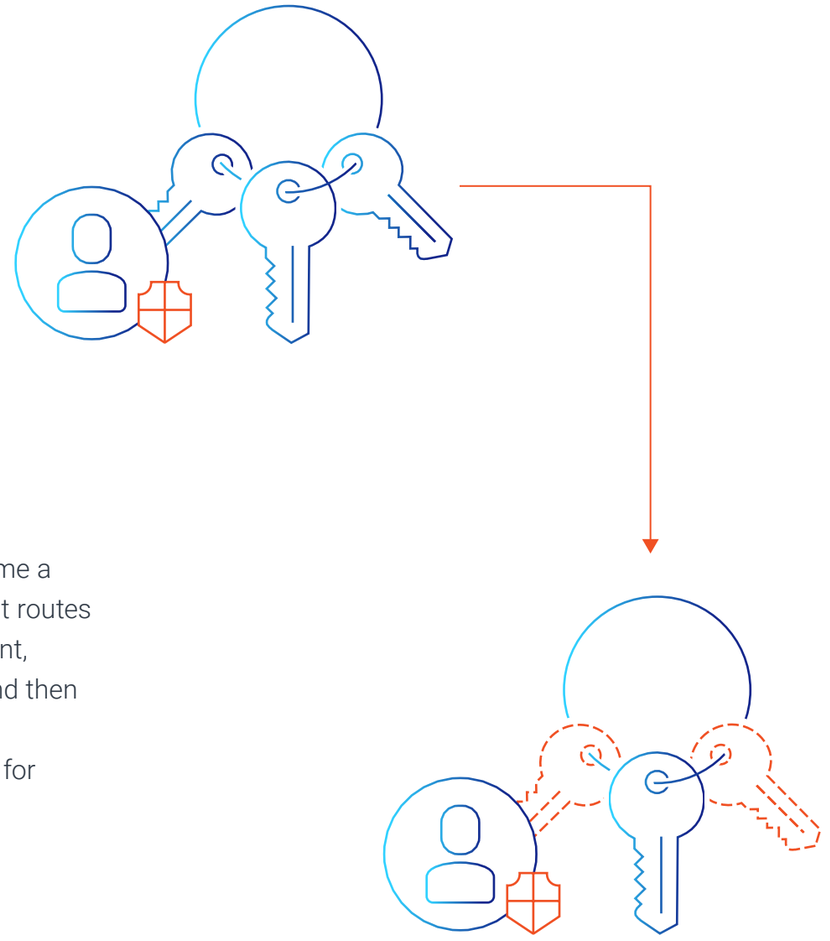
Breaches will happen, given enough time. Assuming a breach will help you prioritize protecting mission-critical systems and implement any and all security measures immediately instead of waiting for a comprehensive plan to take shape.

More importantly, you should also adopt an "agile" methodology for security, implementing all available changes immediately with the understanding that even if you have the best preventative controls in place, something could still slip through. How your organization plans for reacting to a breach — assuming one is coming — will streamline the recovery process and accelerate regaining trust in compromised environments.

Best Practice: 2
ADOPT A LEAST PRIVILEGE APPROACH

Privileged endpoints — those that grant or have administrator rights — are the key to ransomware attacks successfully accessing high-value data or information. Breaching admin rights-enabled endpoints supercharges attackers' ability to access high-value data to hold for ransom.

Start by defining roles and responsibilities in great detail across commonly targeted user groups like IT operations, helpdesks and development teams. Determine which systems and databases house business-critical data or other sensitive information like customer records, and use that analysis to strategically lock down high-risk, highly privileged systems by immediately revoking admin rights across the board.



KEY TAKEAWAY

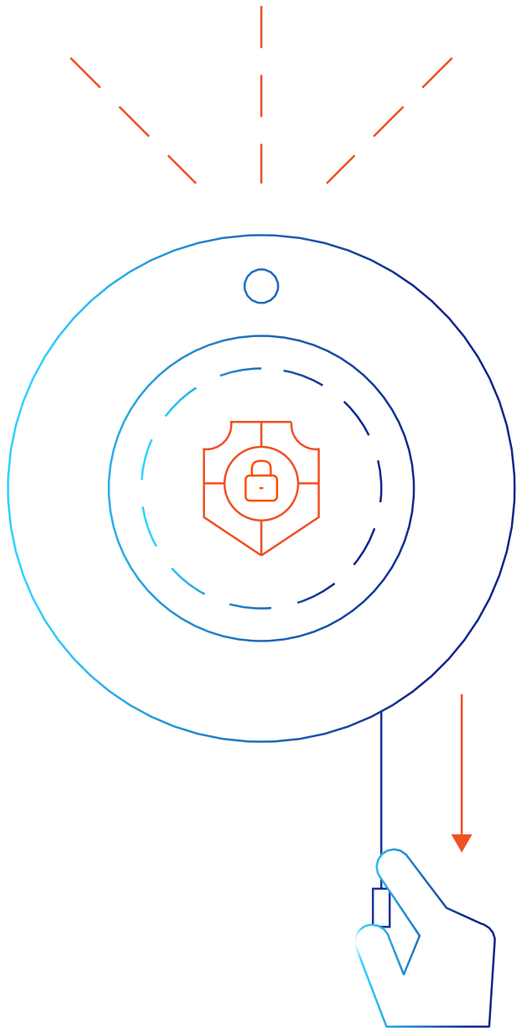
Emphasize protection of highly privileged systems by revoking admin rights and enforcing the minimal level of user rights, or lowest clearance level, that allows the user to perform their role.

To avoid unnecessarily interrupting daily work and organizational productivity, it's imperative to assume a breach and fully map the various lateral movement routes a hacker might take after entering your environment, ranking them in order of likelihood and severity, and then systematically grant administrator rights only to authorized users based on whether it's necessary for their job responsibilities.

Best Practice: 3
RUN FIRE DRILL SCENARIOS TO TEST YOUR DEFENSES

Even the best-laid plans can go awry. The fact is that security teams can't possibly plan for every attack scenario and avoiding massive damage from a ransomware attack is more than just accessing data backups to get back to work.

Instead, gather leaders from across the organization to assess, test and reassess your security protocols and standards. Critically evaluate your restore and recovery processes to identify potential obstacles to achieving recovery time objectives. Assess how much of your critical data is encrypted at rest, rather than just in transit, to help ensure maximum protection throughout the data lifecycle. And validate whether connections to your privileged access points follow the right protocols and limitations to address potential vulnerabilities or overlooked points of failure.



KEY TAKEAWAY

Ransomware attacks come from all angles and change tactics frequently. Continuously test and reassess your security protocols to determine whether certain connections, access rights and recovery processes align with your organizational goals.

The average downtime a company experiences after a ransomware attack is 21 days.[7]

[7] *"Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands."* www.coveware.com. 2021.

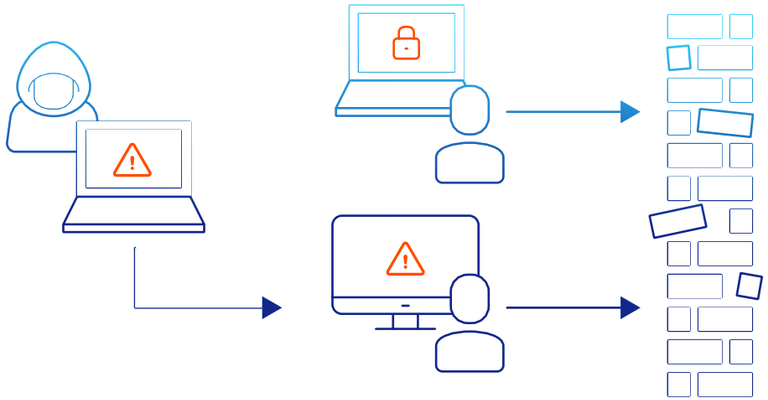
Best Practice: 4
MAKE ATTACKERS' LIVES DIFFICULT

Just because ransomware attacks are imminent doesn't mean they should be easy. There are many steps and strategies you can employ to make cybercriminals' lives miserable for attacking the wrong business.

For example, you can start all network users and applications with standard accounts that have no admin rights and elevate applications requiring admin rights on an as-needed basis.

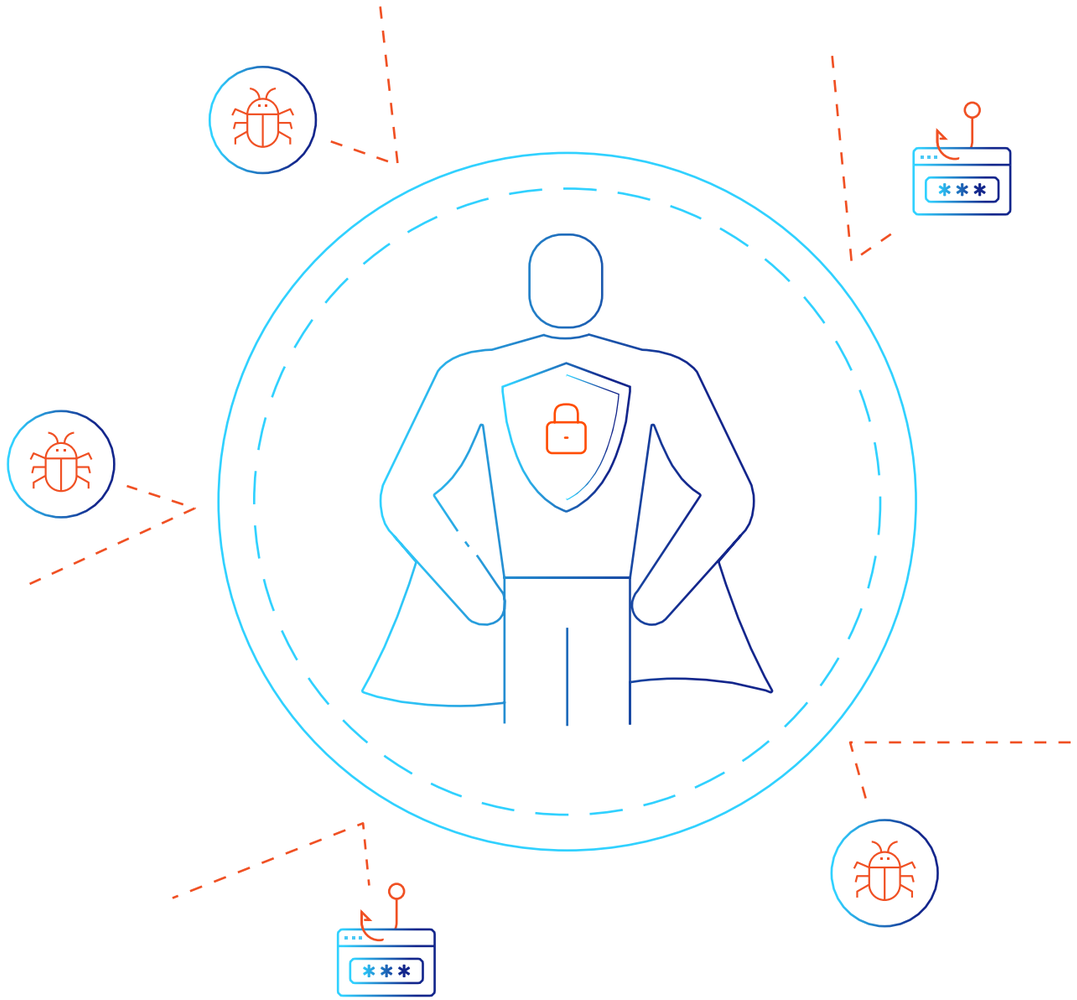
KEY TAKEAWAY

Make it more difficult for cybercriminals to steal high-value data for ransom by removing administrative rights across the network to shut off common attack vectors and closely monitor network activity for suspicious behaviors.



Removing admin rights will help shut off common attack vectors like phishing campaigns, remote desktop protocols (RDPs) and unauthorized local downloads by blocking attackers' abilities to tamper with security controls and make lateral movements throughout your network.

Supplement those steps by adding automated secrets and credentials management on critical targets such as backup servers to eliminate stolen tokens or keys as an entry method. You can also use a combination of application performance monitoring (APM) and security information and event management (SIEM) solutions to develop an audit trail for compliance reporting and closely observe any unusual behaviors that may indicate an intruder in your network.



Best Practice: 5
TAKE ON A RANSOMWARE PREVENTION PARTNER

Unless your core business is cybersecurity or you employ a legion of security professionals, there's a good chance you'll want some additional insight, expertise and resources. Outsourcing to a security partner can help you get an external perspective on the state of your security posture from teams of experts who specialize in ransomware trends. This allows you to focus on your core business.

Selecting an experienced partner will introduce you to proven, widely used protection strategies that have yet to be cracked, granting you additional resilience and protection from the onslaught of potential threats. More importantly, these partners can help you design a comprehensive, integrated solution to automate critical security functions and provide extensive remediation services that can help you accelerate recovery and fortify protections against recurring attacks.

KEY TAKEAWAY

Select an experienced partner with a proven track record for helping organizations design the right strategy to protect them from the onslaught of emerging cyberthreats.

Tools of the Trade to Put Best Practices into Place

Even the most thorough security strategies need the right tools, technologies and policies to be successful. Solutions like EDRs excel at providing continuous monitoring and in-depth analysis that can recognize and stop known ransomware attacks, while APMs scour your applications and network for suspicious activity.

But advanced ransomware protection must go much deeper, with purpose-built technologies that collectively deliver comprehensive preventative controls and detective mechanisms, architected with an “assume breach” approach to enhance defense against ransomware attacks.

These solutions help address cyber ransom from every aspect from the initial intrusion, all the way through data exfiltration and post-breach remediation efforts.

Least Privilege Approach

Least privilege technologies aim to eliminate vulnerabilities from the unnecessary granting of admin rights to human users or applications and include:

- **Built-in privilege management** to automatically enforce the minimal level of user rights — or lowest clearance level possible — without adversely impacting daily business operations.
- **Application control**, which allows only approved applications to run while restricting the connections and administrative rights of unapproved ones. With these tools, unknown applications run in "Restricted Mode," which prevents them from accessing corporate resources, sensitive data or the internet.
- **Just-in-time elevation** to manage user elevation and access on a by-request basis for a limited period of time with full audit of privileged activities.

Privilege Defense

Beyond simply locking down privileged access, privilege defense solutions help you ward off credential theft and other keys to achieve lateral movement within your environment after a breach.

- **Credential theft blocking** helps detect and block attempted theft of Windows credentials and those stored by popular web browsers and file cache credential stores.
- **Ransomware protection and detection** provides another layer of security to the endpoint, giving you the ability to detect ransomware with certainty and respond before the attack can cause damage.
- **Privilege deception** tools are powerful and unique defenses that detect an insider threat or an attacker impersonating an insider who tries to operate undetected. They can even lay decoy credential lures or other components in the attack path to reveal the unwitting attacker who takes the bait.

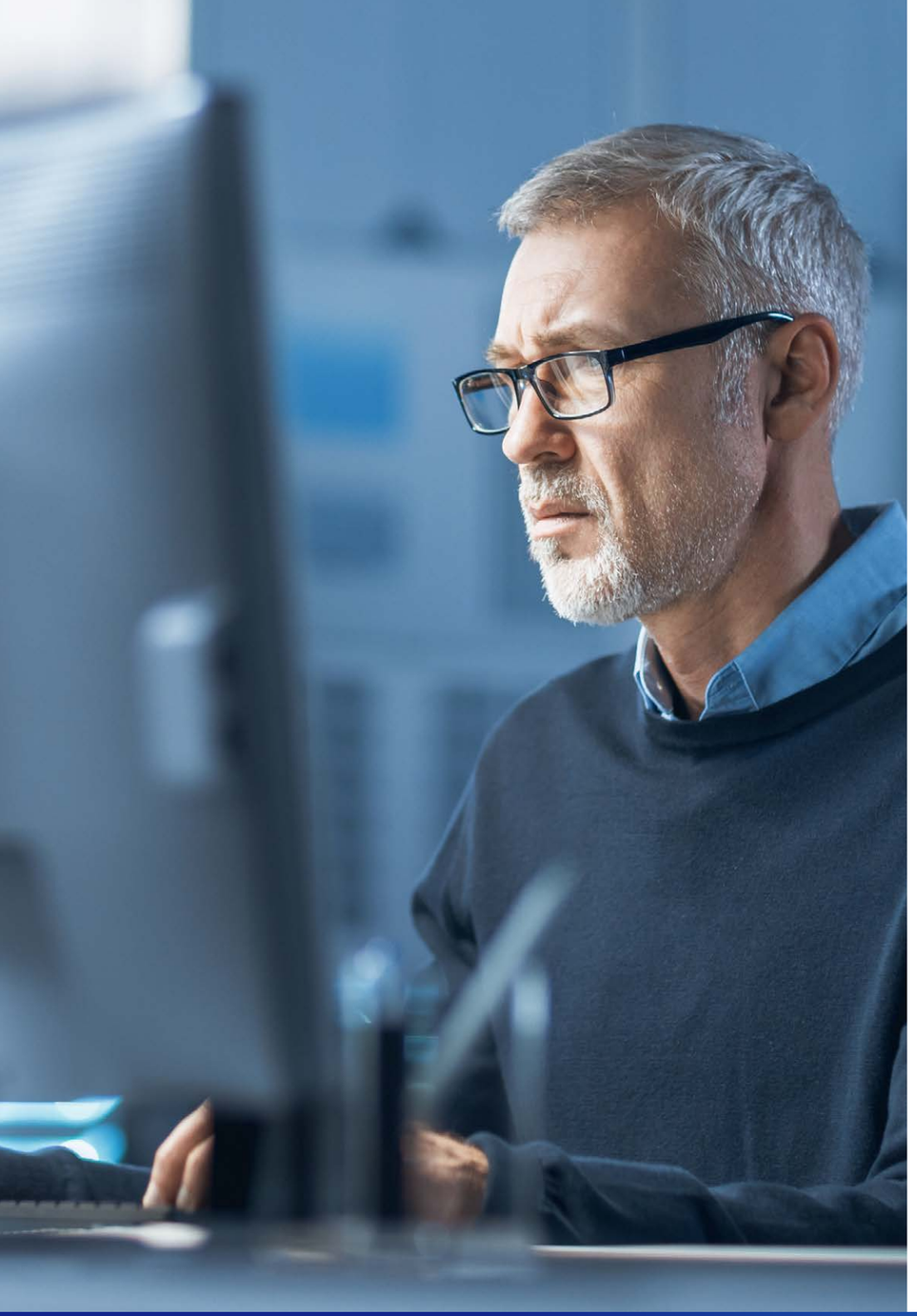
Number of Attacks Exploded

400%

Rise in Reported Cyber Attacks FBI, April 2020

800%

Rise in Ransomware Attacks MonsterCloud, August 2020



Privileged Access Management (PAM)

PAM suites protect sensitive applications, data and endpoints by eliminating credential exposure. Discovering and managing both human and non-human accounts, credentials and secrets is a foundational control in preventing privilege escalation and thwarting attack progression. Implementing session management isolates end users from direct access to target systems, preventing malicious code from propagating through the environment and mitigating the risk from coercion from insiders.

Red Teams and Remediation Services

Deploying a red team to continually test existing cyber ransom security controls against common tactics, techniques and procedures (TTPs) helps dissuade attacks. But when a breach inevitably occurs, time ticks away for stopping further progression and damage. Using incident response services that employ best practices to streamline post-breach remediation and recovery from ransomware attacks is essential to minimizing your loss.

Long-Term Challenges Demand Next-Gen Solutions

Ransomware — preventing it and dealing with its aftermath — has increasingly become an unwanted wrench in the wheel of modern business. A lower barrier to entry thanks to the commodification of ransomware through as-a-service offerings, the emergence of access brokers and massive investments in ransomware platforms from previous successful attacks continues to drive more frequent and sophisticated attacks.

Today, the average cost of recovery from a ransomware attack is more than $1.85 million per business, including an average ransom of more than $170,000 per instance.[8] The success of those attacks has resulted in 100% more organizations being impacted by ransomware attacks each week than last year.[9]

Ransomware isn't going away and to best protect your business against harmful attacks and potentially catastrophic data and financial losses, you need a comprehensive defense plan beyond mere point solutions.

CyberArk is the only Identity Security vendor to effectively address ransomware attacks from every aspect of the kill chain, providing enterprises of all shapes and sizes with the preventative controls and detective mechanisms, coupled with knowledge and expertise they need to stay out of harm's way.

Are you ready to learn how CyberArk's battle-tested technologies and assumed-breach philosophy can substantially improve your company's cybersecurity defenses?

REQUEST A DEMO

[8] Adam, Sally. *"The State of Ransomware 2021."* www.sophos.com and Vanson Bourne. February, 2021.
[9] *"The New Ransomware Threat: Triple Extortion."* www.checkpoint.com. April, 2021.

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

U.S., 09.21 Doc: WRQ-20

CYBERARK®