CROWDSTRIKE

Take a Hike, Ransomware

Deter ransomware with CrowdStrike protection for your AWS environments

aws PARTNER

- Public Sector
- Amazon Linux Ready
- Marketplace Seller
- Security Software Competency

CrowdStrike eBook

Table of Contents

Introduction

ARE YOU CONFIDENT IN YOUR ORGANIZATION'S ABILITY TO PREVENT RANSOMWARE?

Smart preparation and ongoing vigilance are effective counters. And you have allies in ransomware defense. CrowdStrike and Amazon Web Services (AWS) have a host of services and solutions that help prevent, protect against, mitigate, and recover from ransomware attacks.

RECOGNIZING RANSOMWARE

Today's ransomware attacks can take several forms, including:

- Encrypting ransomware: In this instance the ransomware systematically encrypts files on the system's hard drive, which becomes difficult to decrypt without paying the ransom for the decryption key. The actors ask for payment in Bitcoin, MoneyPak, PaySafeCard, Ukash, or a prepaid debit card.
- Screen lockers: These completely lock you out of your computer or system, so your files and applications are inaccessible. A lock screen displays the ransom demand, possibly with a countdown clock to increase urgency and drive victims to act.
- Scareware: This tactic uses pop-ups to convince victims they have a virus, then directs them to download fake software to fix the issue.

$1.79 million

the average ransomware payment according to CrowdStrike's annual Global Security Attitude Survey

According to Gartner, by 2025, ransomware attacks are expected to increase by

700%

and at least 75% of IT organizations will face one or more attacks[1]

[1]Gartner, Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware, January 2021.

How prepared are you for ransomware?

TO FIND OUT, ASK YOURSELF THESE QUESTIONS:

When it comes to responding to a ransomware attack, do you have

- An incident response plan?
- Data backup and restoration strategy?
- List of key contacts to help address issue, like internal team members, law enforcement authorities, relevant partners

As you protect your company from attacks, do you:

- Use antivirus software at all times?
- Keep computers fully patched?
- Block access to ransomware sites?
- Allow only authorized apps?
- Restrict personally owned devices on work networks?
- Use standard user accounts versus accounts with administrative privileges?
- Avoid using personal apps like email, chat, and social media from work computers?
- Run an antivirus scan before opening external files?

If you answered no to even one of these questions, you could be at risk for a ransomware attack. That might come as a shock to you, because you might have thought that you are protected. Most likely, the fact that you probably answered yes to at least a few means you have a good base from which to start.

The good news is that CrowdStrike and AWS offer services that can help you say no to ransomware instead of no to these questions. By aligning with the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), these solutions help you prepare for ransomware.

AWS provides a foundation for ransomware protection

AWS helps protect millions of active customers across the globe from threats like ransomware. These customers represent diverse industries with a range of use cases, including large enterprises, startups, educational institutions, and government organizations. Because of the scale and reach of these customers, AWS has broad visibility and a deep perspective on cloud security, which it rapidly reinvests back into its infrastructure and services.

FOLLOW EXPERT GUIDANCE AS PART OF MITIGATING RISK

Best practices, recommendations, and AWS services can help you lower the risk of a ransomware attack and recover quickly if your organization is affected.

- **MIGRATION:** AWS offers migration recommendations in the Cloud Adoption Framework Security Perspective. This perspective provides guidance and best practices to help you build a comprehensive approach to cloud computing across your organization and throughout your IT lifecycle.
- **WORKLOADS:** The workload best practices in the Well Architected Security Pillar describe how to take advantage of cloud technologies to protect data, systems, and assets. You can improve your security posture and then check workloads against these recommendations. The Well Architected Tool in the AWS Management Console helps you review the state of your workloads and compares them to the latest AWS architectural best practices.
- **INFRASTRUCTURE:** Trusted Advisor uses checks to evaluate your AWS environments. These checks include recommendations for optimizing your infrastructure, improving security and performance, reducing costs, and monitoring service quotas.
- **SECURITY POSTURE:** The AWS Security Hub Foundational Security Best Practices is a standard set of controls that detect when deployed accounts and resources deviate from security best practices. It monitors your AWS accounts continuously and provides actionable and prescriptive guidance on how to improve and maintain your organization's security posture.

7 Tips for preventing ransomware

As a leader in cybersecurity, CrowdStrike has compiled effective security controls and practices you can put in place to reduce your risk of a ransomware outbreak.

1. **Practice good IT hygiene**
   The primary benefit of IT hygiene is to give you complete network transparency. This perspective provides a bird's eye view, as well as the power to drill down and proactively clean out your environment.

2. **Improve resiliency of internet-facing applications**
   CrowdStrike has observed exploits on single-factor authentication and unpatched internet-facing applications, even from big game hunting ransomware actors.

3. **Harden endpoints**
   Ransomware actors may target poor Active Directory configurations or leverage publicly available exploits against unpatched systems or applications.

4. **Use offline backups to ransomware-proof your data**
   When developing a ransomware-proof backup infrastructure, keep in mind threat actors often target online backups. Therefore, maintaining offline backups of your data allows for a quicker recovery in emergencies.

5. **Implement an identity and access management (IAM) program**
   Organizations can improve their security posture by implementing a robust identity protection program to understand on-premises and cloud identity store hygiene. Ascertain gaps, analyze behavior, and implement risk-based conditional access to detect and stop ransomware.

6. **Develop and pressure-test an incident response plan**
   Recognizing ransomware and responding quickly and effectively can be the difference between a major incident and a near miss. Incident response plans and playbooks help facilitate that speedy decision making.

7. **Know when to ask for help**
   Calling in experts to help investigate, understand, and improve the situation can make the difference between a minor incident and a major breach. In some instances, organizations become aware of threat actor activity within their environment but may lack the visibility to address the problem or the right intelligence to understand the nature of the threat.

Protect against ransomware with the CrowdStrike Falcon platform

CrowdStrike secures the most critical areas of enterprise risk—endpoints, cloud workloads, identity, and data—to stay ahead of today's threats and successfully stop ransomware. A massive data set of over a trillion events per day plus threat actor intelligence fuel behavioral indicators of attack (IOAs) to identify and help block ransomware. Expert threat hunters layer on the protection to proactively see and stop the stealthiest of attacks.

PREVENT

Harness the power of cloud-scale AI and a massive data set — 5 trillion events per week — to prevent ransomware in real time

DETECT

Identify ransomware behaviors with indicators of attack and stop the rapid encryption of files before it take hold

RESPOND

Strengthen your team and your security posture with CrowdStrike's seasoned security experts at your side

PREDICT

Understand your adversary to know what to look for and anticipate the next serious threat

Prevent ransomware in real time

Taking proactive action to stop ransomware early means using artificial intelligence (AI) to put actionable data at your fingertips to automatically prevent threats. By restricting lateral movement across your AWS environments and regular maintenance of organizational resources, you can stop ransomware in real time.

The CrowdStrike Security Cloud is one of the world's largest unified, threat-centric data fabrics, powering the next generation of protection and elite threat hunting to stop breaches. The CrowdStrike Security Cloud routinely correlates trillions of security events per day with indicators of attack, the industry's leading threat intelligence and enterprise telemetry from across customer endpoints, workloads, identities, DevOps, IT assets and configurations. Using world-class AI, the CrowdStrike Security Cloud creates actionable data, identifies shifts in adversarial tactics, and maps tradecraft in the patented Threat Graph to automatically prevent threats in real time across CrowdStrike's global customer base.

Falcon Prevent delivers cloud-native, next-generation antivirus (NGAV) to protect against ransomware. Through machine learning and artificial intelligence, Falcon Prevent provides state-of-the-art prevention that examines behavior-based indicators of attacks. This approach stops sophisticated ransomware threats—before they inflict damage.

Falcon Cloud Security includes cloud security posture management (CSPM). It delivers continuous monitoring of your AWS environments to proactively report misconfigurations and suspect behaviors along with compliance documentation and recommended remediations. Falcon Cloud Security detects and prevents misconfigurations and control plane threats, minimizes blind spots and helps prevent ransomware.

Falcon Cloud Security was built to protect dynamic cloud environments and containers. Comprehensive breach protection for workloads, containers, and Kubernetes allows you to build, run, and secure cloud-native applications with speed and confidence.

Detect vulnerabilities in endpoints, identity, and containers

Locking up your data, assets, intellectual property, and infrastructure is only part of defending against ransomware—you also need to detect attempts to get in at the network level, and constantly revisit the effectiveness of what you have in place. For example, not all vulnerabilities are detectable from within your infrastructure. Ransomware criminals can scan your endpoints from the outside, which requires specific tools to detect.

Falcon Insight is an endpoint detection and response (EDR) tool that delivers complete endpoint visibility to detect suspicious activity and ensure breaches are stopped. Falcon Insight accelerates security operations, allowing users to minimize efforts spent handling alerts and reduce time to investigate and respond to attacks.

Falcon Identity Protection protects workforce identities everywhere—for any user, location, application and deployment. Secure Active Directory (AD), enables secure, frictionless remote access, and extends multi-factor authentication everywhere.

Falcon Cloud Security unifies CSPM and breach protection for AWS workloads and containers. The cloud-native solution provides end-to-end protection from the host to the cloud and everywhere in between. Go beyond ad-hoc approaches with a unified platform.

Respond fast, early, and at scale

Whether a ransomware attack fails or is caught early, fast response times are critical—but not all teams have the resources to react rapidly. A sufficient response plan focuses on containment—preventing expansion of malicious activities, conducting forensic analysis to determine impact, and analyzing the effectiveness of your response. Automation can help businesses do all these things at scale.

CrowdStrike Falcon Complete is a hands-off and worry-free managed detection and response (MDR) solution that provides the people, process, and technology required to handle all aspects of endpoint, cloud workload, and identity security. From onboarding and configuration to maintenance, monitoring, incident handling, and remediation, Falcon Complete helps you respond fast to ransomware with experts managing your CrowdStrike solution.

Predict ransomware's next move to stay ahead

Staying one step ahead of ransomware is often the best defense. Predictive security can support security operations centers (SOC) that may be struggling with alert fatigue and don't have the time or expertise to track how ransomware evolves. Automating investigations with a solution informed by the latest threat intelligence can help you anticipate ransomware's next move and enable faster, better decisions.

CrowdStrike Falcon Intelligence brings built-in adversary intelligence to supercharge your SOC and incident response teams so they can stay ahead of ransomware. CrowdStrike Falcon Intelligence delivers the critical intelligence you need, while eliminating the resource-draining complexity of incident investigations. By integrating threat intelligence into endpoint protection, CrowdStrike Falcon Intelligence helps you automatically perform investigations, speed responses, and enable security teams to move from a reactive to a predictive, proactive state.

Visit CrowdStrike in
AWS Marketplace
to start your free trial.

Conclusion

Ransomware can hobble your systems, steal your data, and put a dent in your company's bank account. But with smart preparation, ongoing vigilance, and the right technology, you can just say no to ransomware.

CrowdStrike and AWS offer services and solutions that can keep your data, workloads, applications, and environments protected against ransomware. With these offerings, you can take proactive measures to reduce the likelihood and impact of ransomware in your AWS environments.