Achieve ransomware resilience with AWS and Palo Alto Networks

Table of contents

NIST and your evolving security landscape

Increasingly, organizations are prioritizing cybersecurity—something Amazon Web Services (AWS) prioritizes as part of its job-zero philosophy. But ransomware, in particular, demands a carefully crafted plan for businesses to stay secure.

Ransomware attacks are expected to increase by 700 percent and at least 75 percent of IT organizations will face one or more attacks by 2025. The average ransom that cybercriminals demand rose 144 percent between 2020 and 2021, according to the 2022 Ransomware Threat Report produced by Unit 42, an arm of Palo Alto Networks.

While ransomware is on the rise, so is the sophistication and availability of solutions and services that keep businesses protected. A large selection of cybersecurity vendors paired with robust guidance from different experts has left businesses with two important missions:

1. Develop an informed ransomware strategy. Businesses must understand how to create an effective resiliency plan that leverages technology solutions for ongoing protection.
2. Choose the right vendor. Businesses must determine which cybersecurity provider can effectively protect against ransomware as threats continuously evolve.

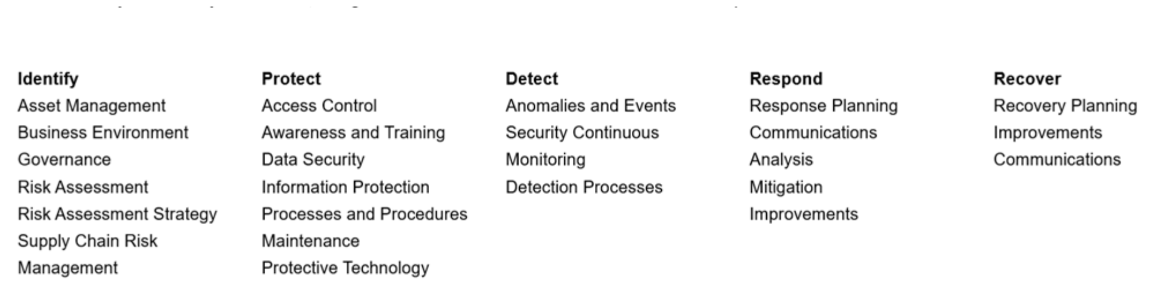
Ransomware -
Malicious software designed to block access to a computer system and/or data until a sum of money is paid

Leveraging NIST for applications and cloud infrastructure

To enable stronger cybersecurity for businesses big and small, the U.S. National Institute of Standards and Technology (NIST) developed a cybersecurity framework (CSF) that includes five key functions of a secure infrastructure: identify, protect, detect, respond, and recover.

Considered the gold standard for security best practices, the framework is a strong basis for fostering ransomware resilience.

In this eBook, you'll learn how AWS and Palo Alto Networks provide solutions that allow businesses to align their ransomware readiness practices to the NIST CSF.



Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection		Mitigation	
Risk Assessment Strategy	Processes and Procedures		Improvements	
Supply Chain Risk Management	Maintenance			
	Protective Technology			

Ransomware resilience with AWS and Palo Alto Networks

Adhering to the NIST CSF is easy for businesses that operate on AWS infrastructure and utilize Palo Alto Networks' tools and services. Together, AWS and Palo Alto Networks provide the broadest set of integrated security capabilities.

As part of their strategic partnership and shared commitment to customer satisfaction, AWS and Palo Alto Networks consistently work together to develop and innovate. By layering best-in-class solutions from Palo Alto Networks and a host of security features that make up the AWS environment, customers can enjoy benefits unique to this pairing.

Comprehensive security without having to choose
Businesses have found themselves onboarding new security solutions for every new breed of threat, and now work with an average of 45 cybersecurity-related tools that only offer point-to-point solutions. Because solutions from Palo Alto Networks are designed to correlate findings from AWS and third-party solutions, customers can easily consolidate security alerts into a single dashboard. As a result, businesses can avoid solution overlap, optimize costs, and improve efficiency in the absence of navigating back and forth among multiple platforms.

Easy-to-use, natively integrated safeguards
Designed to work together in the cloud, Palo Alto Networks offers seamless integration with AWS services. Palo Alto Networks solutions ingest 100 percent of findings from AWS tools, including those essential to monitoring, tracking inventory, and configuration. Beyond deep knowledge of AWS infrastructure, Palo Alto Networks works hand-in-hand with AWS product teams to create solutions designed to help customers bolster security.

Scalable solutions that work for everyone
The scalability of the AWS Cloud combined with the pace of innovation from Palo Alto Networks means customers have cybersecurity solutions that evolve with their changing needs. For example, Palo Alto Networks' Next-Generation Firewalls (NGFW) use Gateway Load Balancer and are managed through AWS Firewall Manager—ensuring scalability as enterprises need it. Each time AWS develops a new product, Palo Alto Networks is invited to learn about it during the beta phase, providing the opportunity to integrate solutions by the time it launches on the market.

Through the AWS shared responsibility model, AWS is responsible for the security "of" the cloud while customers take responsibility for security "in" the cloud.

Identify your attack surface

The first of the core functions outlined in NIST, "Identify" requires assessing your attack surface to minimize it. Categories in this function include establishing an asset management program, uncovering internal and external vulnerabilities, and outlining policies that manage risk in a way that aligns with business needs.

Understand your ransomware readiness
With the shift to remote and hybrid work structures, evaluating Remote Desktop Protocol (RDP) has become a key aspect of identifying where ransomware may be deployed. RDP is the most popular vector for ransomware point of entry—in 2020, 50 percent of ransomware was deployed via RDP.

Leveraging the built-in safeguards of the AWS Cloud and expert guidance from Unit 42, Palo Alto Networks' global threat intelligence team, you can accurately assess your cloud landscape and security posture through a Ransomware Readiness Assessment. Organizations can strengthen their processes and technology to mitigate the threat of ransomware based on the latest threat intelligence and collective input from a team of experts. Unit 42 assesses your current ability to defend against and respond to ransomware attacks, and then assists in developing a ransomware prevention playbook so you have a plan in place.

System management made easy with AWS
Use your attack surface assessment to improve the way you configure your AWS environments. Start by defining configuration policies for your servers via AWS Management Console, where you can access a single web interface to retrieve and manage resources living in the AWS Cloud. AWS Systems Manager State Manager will automatically apply those configurations across your Amazon Elastic Cloud Compute (Amazon EC2) instances at a time and frequency that you define. AWS Systems Manager automates patching for managed nodes, and you can also apply patches to operations systems and applications. For continuous management, use Amazon Inspector to automate vulnerability management at scale. Amazon Inspector scans AWS workloads for software vulnerabilities and unintended network exposure, reducing mean time to remediation.

Smart move: Domain Name System (DNS) attacks are growing in popularity—85 percent of malware uses DNS to initiate command-and-control procedures. Why? The high volume of traffic makes it easier for malicious actors to hide their activity. Pay special attention to DNS activity with DNS Security Service from Palo Alto Networks, a cloud-based platform that uses advanced predictive analytics and machine learning. It provides your firewalls with malicious domain data collected from the threat intelligence community, and if a bad actor attempts to use DNS for command and control or data theft, this solution will disrupt the attack. The service aggregates intelligence from the largest customer base of any other vendor in cybersecurity, getting smarter over time.

Protect your environment

Two essential capabilities that can protect your business from ransomware are the ability to identify both known and unknown threats and being able to stop ransomware early once it appears by restricting lateral movement across the system. NIST guidance for this function suggests protection for identity and access management (IAM) control and regular maintenance of organizational resources and protective technology.

Tackle known and unknown ransomware

Cortex XDR from Palo Alto Networks provides security powered by artificial intelligence (AI) for complete endpoint protection. It matches behavior against existing digital profiles to pinpoint known ransomware and can identify completely different breeds of ransomware — including anomalies indicative of an attack. Once ransomware is identified, Cortex XDR provides deep contextual analysis, root cause information, a sequence of events, and runs investigations even if endpoints are not connected to the network—reducing investigation time.

For further protection, Palo Alto Networks offers Wildfire, a Malware Analysis Engine that detects brand new, targeted malware and advanced persistent threats. When WildFire identifies something—whether from XDR or on its own—it automatically propagates across every product from Palo Alto Networks, including firewalls, URL filtering systems and Internet of Things (IoT) security systems.

Advanced URL Filtering, a subscription-based, multi-layered solution that stops unknown web-based attacks, provides real-time URL analysis and malware prevention. It was designed for high-performance URL lookups and is configured through your URL filtering profile.

If your organization relies on the Internet of Things, consider implementing IoT Security to protect from the known and unknown. It secures all your IoT systems, from the devices you see to the ones you don't—the latter being a common blind spot for businesses.

Restrict lateral movement

Segmentation is key to preventing lateral movement, and essential to following the "protect" portion of the NIST framework. Effectively compartmentalizing your infrastructure makes it difficult—and at times impossible—for malicious actors to spread ransomware further after they've successfully breached a system. Palo Alto Networks helps cloud users do this by sorting segmentation based on who users are, their privilege levels, and other factors—blocking data leakage and communications.

AWS services, as well as Cortex XDR, allow you to effectively compartmentalize your infrastructure and set strategic boundaries.

- Set up Network Access Control Lists (NACLs) in AWS to regulate traffic in and out of subnets. You can set up NACLs with rules similar to your security groups for an additional layer of security.
- Create rules in AWS Config to authorize access to different apps. Configure operating systems or use Palo Alto Networks to allow only authorized applications on computers.
- Implement fine-grained permissions with AWS Identity and Access Management (IAM). This offering can protect your AWS infrastructure and resources by instilling least-privilege access to assets and allowing customized access around specific conditions.

Detect bad actors across the stack

Timely discovery, continuous monitoring, and verifying the effectiveness of protective measures are hallmarks of NIST's "detect" function in the CSF. 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 to your workload are detectable from within your infrastructure—ransomware criminals can scan your organization from the outside, which requires specific tools to detect.

Securing cloud workloads by uncovering blind spots

Prisma Cloud from Palo Alto Networks offers full-lifecycle security, full-stack protection, and real-time visibility for containerized and serverless AWS environments, applications, and data. Businesses can secure configurations and hosts, scan code, and integrate safeguards with the developer tools they're already using. It offers Identity-based Microsegmentation, enforces permissions, and secures identities all in one platform. With Cloud Workload Protection, organizations receive alerts on potential vulnerabilities, which helps businesses maintain a strong level of detection as they scale—as well as facilitates compliance.

Visibility facilitates detection

Just like your ability to respond relies on your ability to detect, your ability to detect relies on the visibility into your infrastructure. Palo Alto Networks protects your AWS workloads with VM Series Virtual Next-Gen Firewall by consolidating your security management. It eliminates visibility gaps that result from using disparate network security tools and allows users to discover threats more easily. VM Series goes beyond simple port blocking with integrated security services, inspecting every inbound and outbound packet for known and unknown threats.

Blind spots that make ransomware easier to introduce often include weak cryptography, abandoned marketing portals, and unpatched or end-of-life systems. In an innovative approach to detection, Cortex Xpanse continuously monitors and uncovers your digital attack surface across the entire internet. By routinely discovering assets that your IT staff is unaware of—and therefore may not know to monitor—you can feel confident that you're filling detection gaps.

Track and detect with AWS

Keeping logs makes it easier to detect when malicious activity begins. With AWS CloudTrail, you can log all API calls. For additional risk context and anomaly detection, use Amazon GuardDuty to correlate activity in your AWS environment with threat intelligence from multiple sources.

Visibility into activity allows for more effective detection. Amazon Virtual Private Cloud (Amazon VPC) Flow Logs monitor all network activity going in and out of your VPC, and with Amazon CloudWatch you can monitor your AWS environment and generate alerts. Amazon Macie can identify sensitive data, classify, and label it, and track its location and access.

Smart move: Protecting your environment means keeping your data safe. Enterprise Data Loss Prevention (DLP) from Palo Alto Networks is a practical way to minimize breaches and ensure compliance. Enterprise DLP consistently identifies where sensitive data lives across your business, monitors data on the move, and restricts where it can go. This solution can prevent unsafe transfers of information and detect corporate policy violations down to a single data point—from an image file to one social security number.

Respond quickly with automation

Whether a ransomware attack fails or is caught early, fast response times are critical—but not all teams have the resources to react rapidly. In NIST's guidance for this function, 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.

AWS customers can amplify their automation use through a variety of cloud tools. AWS Systems Manager allows users to build an effective automated incident management and response solution to security events, and Amazon Detective uses automation and machine learning to collect log data from your AWS resources to conduct incident investigations more effectively.

Save time, resolve faster
Cortex XSOAR from Palo Alto Networks unburdens security teams by automating up to 95 percent of all response actions requiring human review, reducing the time teams invest on low-level alerts. The solution ingests alerts across sources—including AWS Security Hub and Amazon GuardDuty—allowing businesses to parse, manage, and accelerate action on threat intelligence at scale. Using logic, Cortex XSOAR follows an automation playbook that makes precise calls about automating responses. Customers who use Cortex XSOAR see 75 percent fewer incidents, and when incidents do occur, teams resolve them 90 percent faster.

Incident response with Unit 42
Not every business has the expertise to thoroughly remediate system vulnerabilities, or IT team to respond to threats fast. Unit 42 offers professional services to help with incident response that can be a valuable extension for any team. Services include ransomware investigation, cloud incident response, business email compromise containment and recovery, web application attacks, and fast, scalable response to advanced persistent threats. In dealing with ransomware specifically, Unit 42 assists organizations from assessment to recovery in various ways, such as acquiring and validating decryption keys to monitoring for follow-up attacks.

Recover with tools and expert guidance

After releasing its CSF, NIST's National Cybersecurity Center of Excellence published a special report that offered further guidance on responding to ransomware. Recommendations emphasized the importance of enterprise data backup, prevention of data alternation, and ease of restoration best practices.

Backup and restore

Speed your recovery with AWS Backup, which enables you to centrally deploy data protection policies to configure, manage, and govern your backup activity across your organization's AWS accounts and resources. Other essential back and restore tools from AWS include:

- Amazon S3 Glacier Vault helps prevent data loss. Create a policy that denies users the ability to delete an archive, test the policy, and then lock it so it becomes immutable.
- Amazon Machine Image (AMI) can replace an Amazon EC2 image.
- Amazon CloudWatch and AWS Lambda can automate recovery actions like deploying an entire AWS environment and application, failing over to a different AWS region, restoring data from backups, and more.
- Turn on S3 bucket versioning to rollback to known good object state.

Recovery, everywhere

Palo Alto Networks offers features that facilitate recovery from a ransomware attack across its product portfolio. Its Maintenance to Recovery tool (MRT) enables users to perform recovery tasks to firewalls and appliances, such as reverting to default settings. Prisma Cloud automatically backs up all data and configuration files periodically and allows users to restore specific backups and create new backups. Finally, Unit 42 is available on demand to assist with a strategic recovery plan.

Best practices for ransomware resilience

While AWS and Palo Alto Networks help businesses implement comprehensive safeguards against ransomware, it's important to support them with regularly applies best practices. In addition to requiring multifactor authentication, integrating endpoint detection, encrypting data, and keeping your security team's skills up to date, consider these additional practices.

Periodically run through checklist of must-haves

- 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
- Employ standard user accounts versus accounts with administrative privileges https://aws.amazon.com/about-aws/whats-new/2021/05/introducing-incident-manager-aws-systems-manager/
- 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, your risk of experiencing a ransomware attack is heightened.

Test your incident response plan

Incident response plans are critical, so be sure to periodically review your organization's policies and procedures for responding to security events. Refer to the AWS Security Incident Response Guide, which includes a section on security incident response simulations. You can also use Incident Manager in AWS Systems Manager to automate your response.

Conduct penetration testing

Using trained and certified professionals to try to hack into your environments, apps, and data sources can reveal your soft security spots, but in a controlled scenario. Penetration testing is an effective way to discover unknown vulnerabilities and gauge the effectiveness of your security setup. You can carry out security assessments or penetration tests against your AWS infrastructure without prior approval for a subset of permitted services, provided these activities align with the policy defined on the AWS Penetration Testing webpage.

Aligning to the NIST Cybersecurity Framework in the AWS Cloud

More public and private organizations around the world are choosing to follow the NIST CFS—which is why AWS compiled a detailed guide to help customers align their cloud infrastructure to NIST recommendations. Referencing this detailed whitepaper will help cybersecurity professionals using the AWS Cloud identify key capabilities of AWS service offerings so they can align to the NIST CSF—and better protect the safety and resiliency of their data. Read it here.

See optimal security outcome with AWS and Palo Alto Networks

Cultivate your organization's ransomware readiness with best-in-class security services and solutions.

Visit Palo Alto Networks in AWS Marketplace today ›