



Beating Ransomware

How To Protect, Detect & Recover from Ransomware
with AWS Security + AWS Storage

Huy Tran

Senior Solution Architect
Amazon Web Services

Agenda

What is Ransomware?

AWS Security Best Practices

AWS Data Resiliency Best Practices

AWS Partner Solutions

Putting It All Together



What is Ransomware?



What Is Ransomware?

MALWARE THAT RANSOMS YOUR DATA

Ransomware is a form of malware that **perpetually blocks access** to business-critical information and systems unless a ransom is paid.



Locker Ransomware

Does not encrypt files; instead, unauthorized users **lock the victims out of their devices and prevent them from having access.**



Crypto Ransomware

Prevents users from **accessing important files by fully or partially encrypting their data.**

What Is Wiperware?

RANSOMWARE BUT WITHOUT CHANCE OF RECOVERY

Wiperware is a form of malware whose sole intent is to **cause chaos and unrecoverable destruction of data.**

It can often mask as ransomware or use ransomware as a decoy.

First observed during Ukrainian war to eliminate government and cultural records such as birth certificates, property ownership records, educational credentials, etc.

SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

CYBERWARFARE

Ransomware Used as Decoy in Destructive Cyberattacks on Ukraine

Ransomware was used as a decoy in some of the recent data-wiping cyberattacks against organizations in Ukraine, Symantec reports.

ars TECHNICA

WIPE OUT —

Effective, fast, and unrecoverable: Wiper malware is popping up everywhere

Wiper malware from no fewer than 9 families has appeared this year. Now there are 2 more.

TE

Security

US says destructive wiper malware targeting Ukraine could 'spill over' to other countries

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

CRY, CRY, CRY —

Never-before-seen malware is nuking data in Russia's courts and mayors' offices

CryWiper masquerades as ransomware, but its real purpose is to permanently destroy data.

DAN GOODIN - 12/2/2022, 12:57 PM

Ransomware Business Models

Locker Ransomware

Blocks access to systems and data using compromised credentials until a ransom is paid.

Payment typically in crypto.

In all cases, no guarantees of...

1. Complete data recovery after payment.
2. Having exfiltrated data deleted after payment.
3. Still having exfiltrated data leaked or sold after payment.
4. Avoiding future attacks after history of payment.
5. Future extortion and attacks for more money.
6. Additional malware and backdoors being implanted.

Crypto Ransomware

Blocks access by encrypting some or all files and demands a ransom from the victim in exchange for a decryption key.

Payment typically in crypto.

Double, Triple & Quadruple Extortion

Double: Exfiltrates data from target, then encrypts target's system and demands ransom.

Triple: Sustained DDoS attacks to increase leverage to pay the ransom.

Quadruple: Direct end user contact to add even more leverage and ruin reputation.

Most Recent: Informing SEC of data breaches that violate the "four day rule".

Ransomware As A Service (RaaS)

Threat actors democratize ransomware tools via subscription or pay-for use service.

RaaS operator shares revenue from ransoms paid.

Some tools become open-sourced to add more features and accelerate innovation.

Ransomware Incidents are More Likely When...



**Technical maintenance
is behind schedule**

- Patching not up to date
 - Irregular untested data backups
 - Only focusing on recovery instead of protection
-



**Employee skill levels
create security risks**

- Security awareness low
 - Vulnerable to social engineering
 - Lack of multi-factor authentication (MFA)
-



**Security strategy
doesn't prepare for incidents**

- Overly permissive credentials
 - Open trust model allows malware to spread
 - No clear governance model
-

Ransomware is a growing business risk

By 2025, **75%** of all IT organizations will face **one or more ransomware threats** (Gartner, 2021).



Increased Incident Rates & Sophistication Levels

83% of successful ransomware attacks feature **double or triple extortion tactics**.



Recovery Costs Skyrocketing

\$4.54M: Average Ransomware Recovery Costs

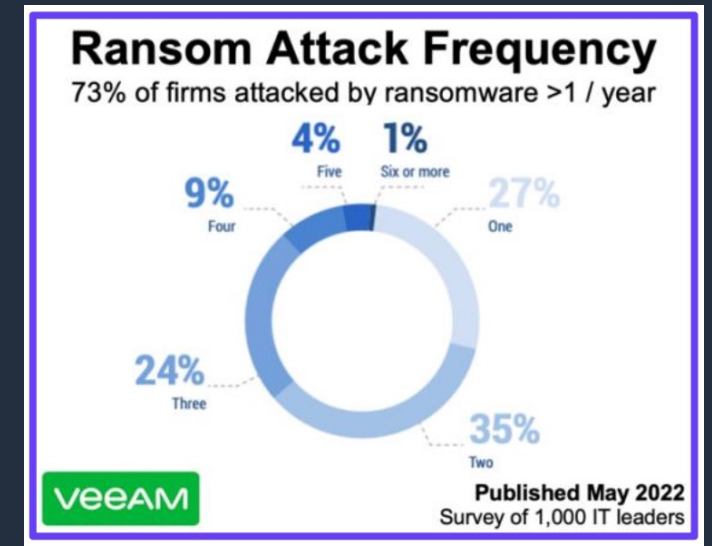
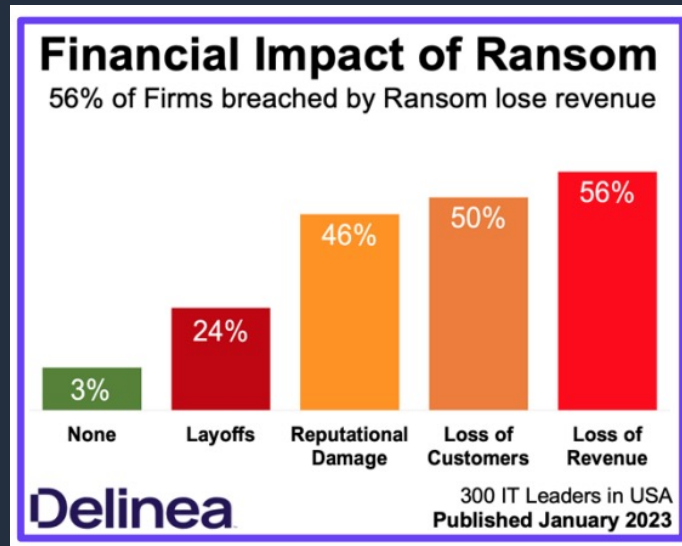
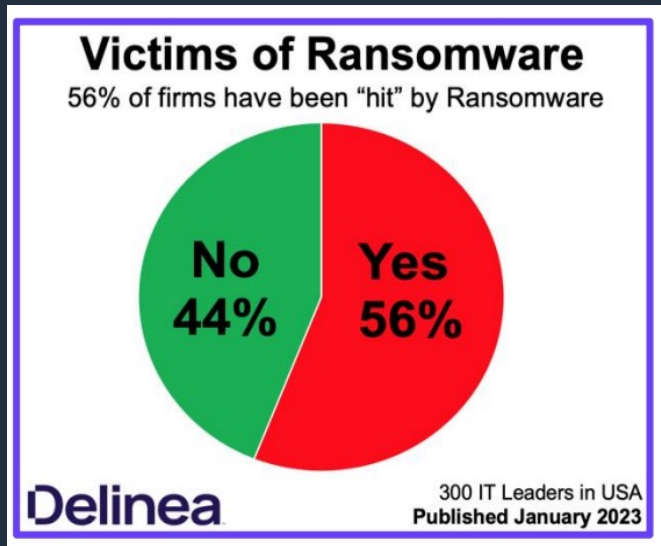


Significant Business Impact

\$5.3M: Average Ransom Paid By Enterprise Customers
\$812,360: Average Ransom Paid
22 Days: Average Downtime

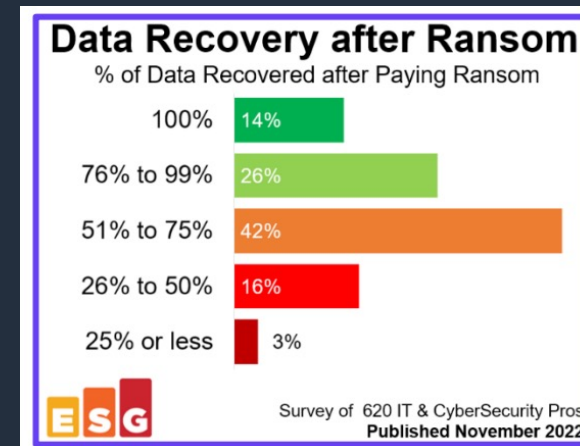
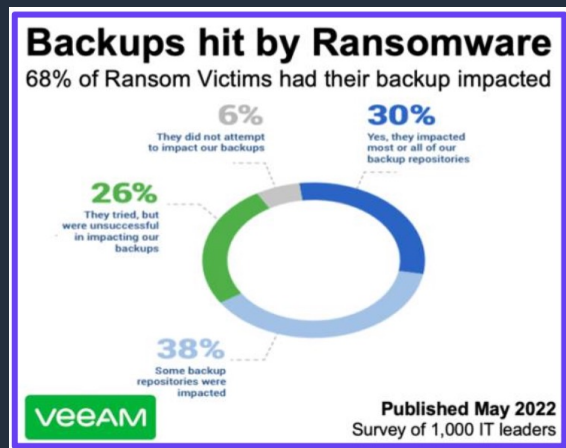
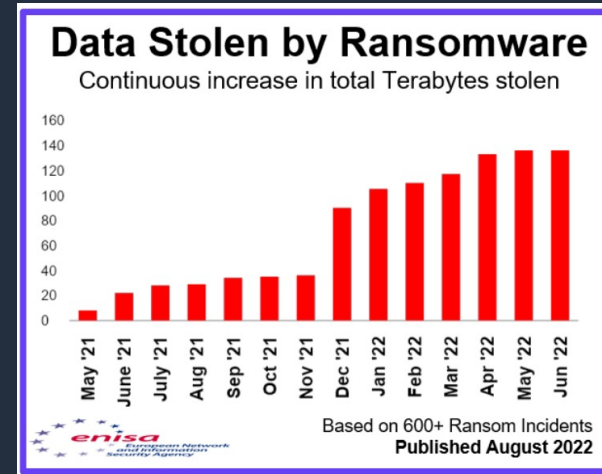
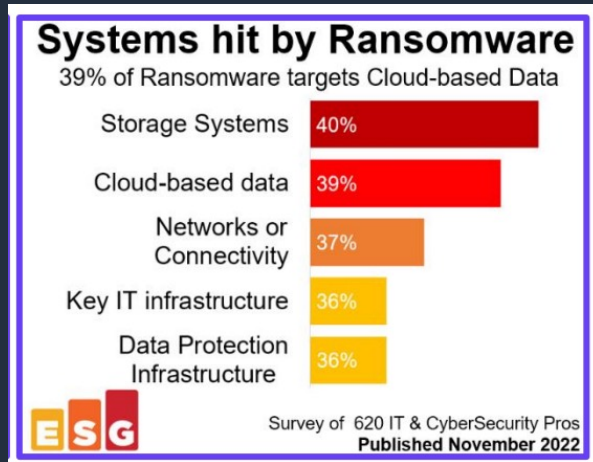
Impact To Our Customers

RANSOMWARE IS A GROWING THREAT WITH CRITICAL IMPACTS TO BUSINESS



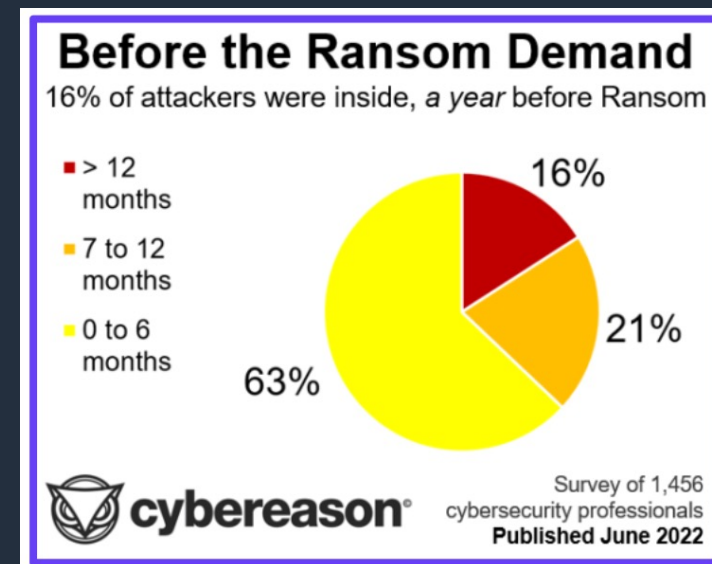
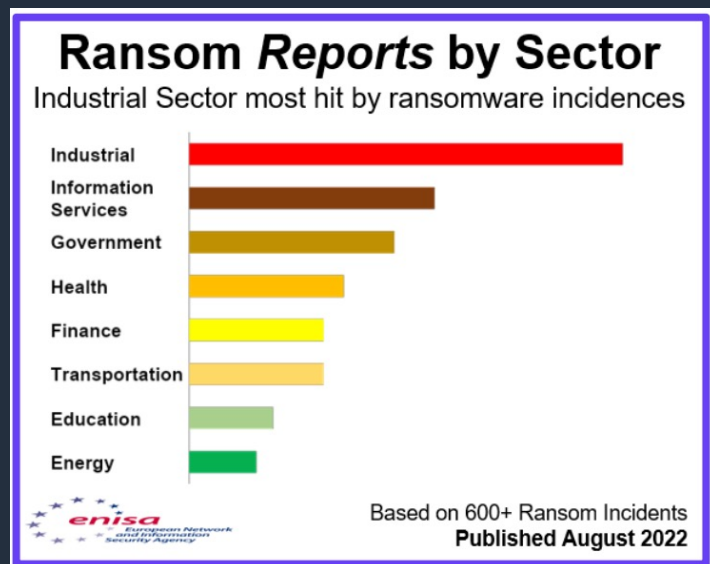
Impact On Data Storage & Backups

RANSOMWARE IS A GROWING THREAT WITH CRITICAL IMPACTS TO BUSINESS



Ransomware Targets & Methods

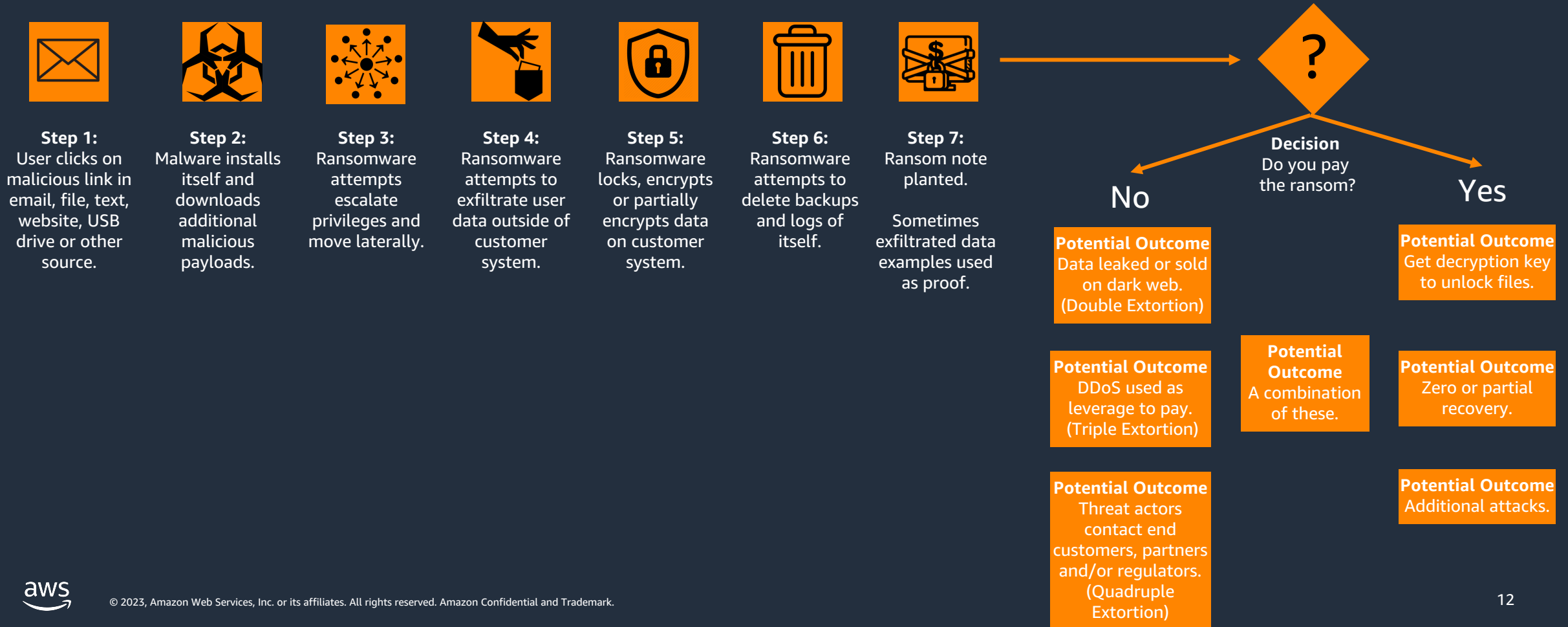
RANSOMWARE IS A GROWING THREAT WITH CRITICAL IMPACTS TO BUSINESS



This is what we call “dwell time” and why *protection* and *detection* are critical parts of the ransomware story!

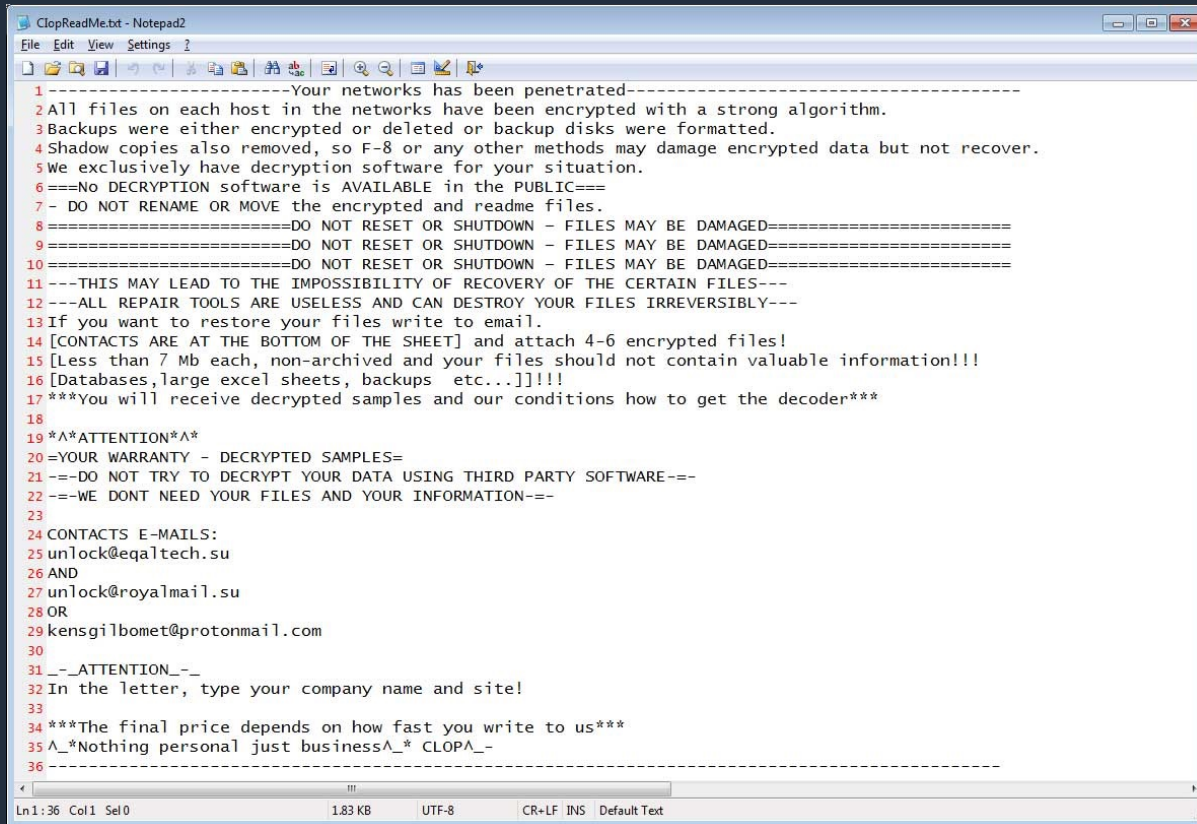
How Ransomware Works

SOME SCENARIOS OBSERVED



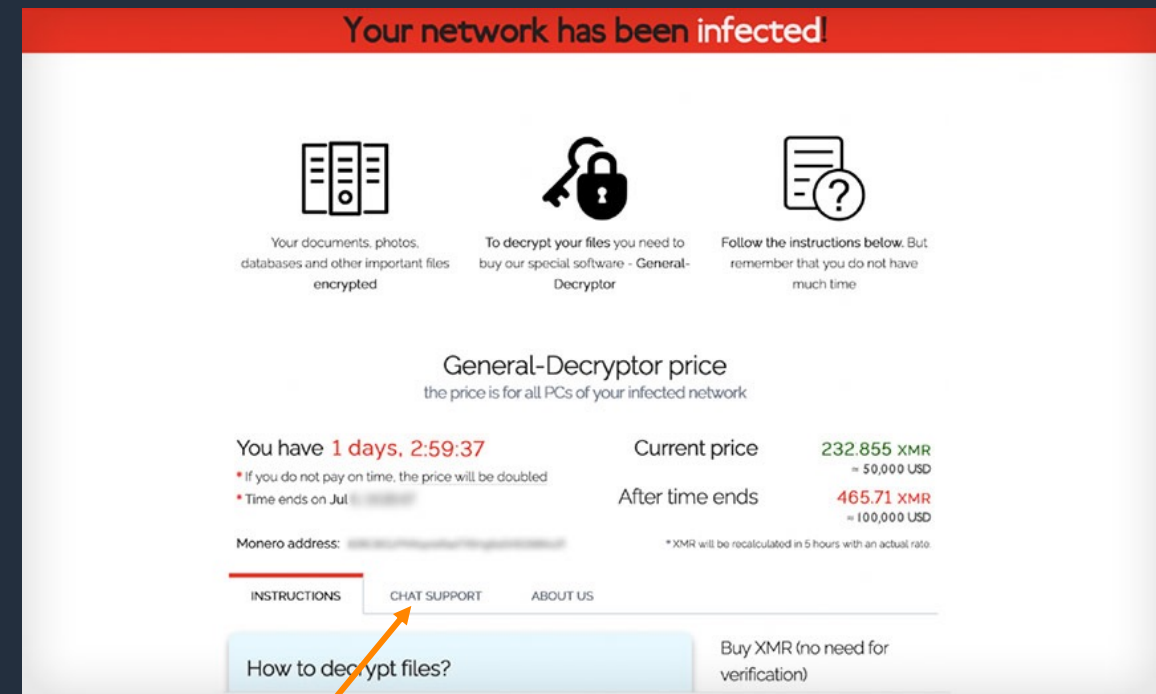
What Ransom Notes Look Like

SOMETIMES TERRIBLE UI/UX. SOMETIMES MORE ELEGANT.



```
1 -----Your networks has been penetrated-----
2 All files on each host in the networks have been encrypted with a strong algorithm.
3 Backups were either encrypted or deleted or backup disks were formatted.
4 Shadow copies also removed, so F-8 or any other methods may damage encrypted data but not recover.
5 We exclusively have decryption software for your situation.
6 ===No DECRYPTION software is AVAILABLE in the PUBLIC===
7 - DO NOT RENAME OR MOVE the encrypted and readme files.
8 =====DO NOT RESET OR SHUTDOWN - FILES MAY BE DAMAGED=====
9 =====DO NOT RESET OR SHUTDOWN - FILES MAY BE DAMAGED=====
10 =====DO NOT RESET OR SHUTDOWN - FILES MAY BE DAMAGED=====
11 ---THIS MAY LEAD TO THE IMPOSSIBILITY OF RECOVERY OF THE CERTAIN FILES---
12 ---ALL REPAIR TOOLS ARE USELESS AND CAN DESTROY YOUR FILES IRREVERSIBLY---
13 If you want to restore your files write to email.
14 [CONTACTS ARE AT THE BOTTOM OF THE SHEET] and attach 4-6 encrypted files!
15 [Less than 7 Mb each, non-archived and your files should not contain valuable information!!!
16 [Databases,large excel sheets, backups etc...]]!!!
17 ***You will receive decrypted samples and our conditions how to get the decoder***
18
19 *A*ATTENTION*A*
20 =YOUR WARRANTY - DECRYPTED SAMPLES=
21 --DO NOT TRY TO DECRYPT YOUR DATA USING THIRD PARTY SOFTWARE--
22 --WE DONT NEED YOUR FILES AND YOUR INFORMATION--
23
24 CONTACTS E-MAILS:
25 unlock@eqaltech.su
26 AND
27 unlock@royalmail.su
28 OR
29 kensgilbomet@protonmail.com
30
31 _-ATTENTION_-
32 In the letter, type your company name and site!
33
34 ***The final price depends on how fast you write to us***
35 ^_Nothing personal just business^_* CLOP^_-
36 -----
```

Clop Example



Your network has been infected!

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - General-Decryptor

Follow the instructions below. But remember that you do not have much time

General-Decryptor price
the price is for all PCs of your infected network

You have **1 days, 2:59:37**

Current price **232.855 XMR**
= 50,000 USD

After time ends **465.71 XMR**
= 100,000 USD

Monero address: [redacted] *XMR will be recalculated in 5 hours with an actual rate

INSTRUCTIONS | **CHAT SUPPORT** | ABOUT US

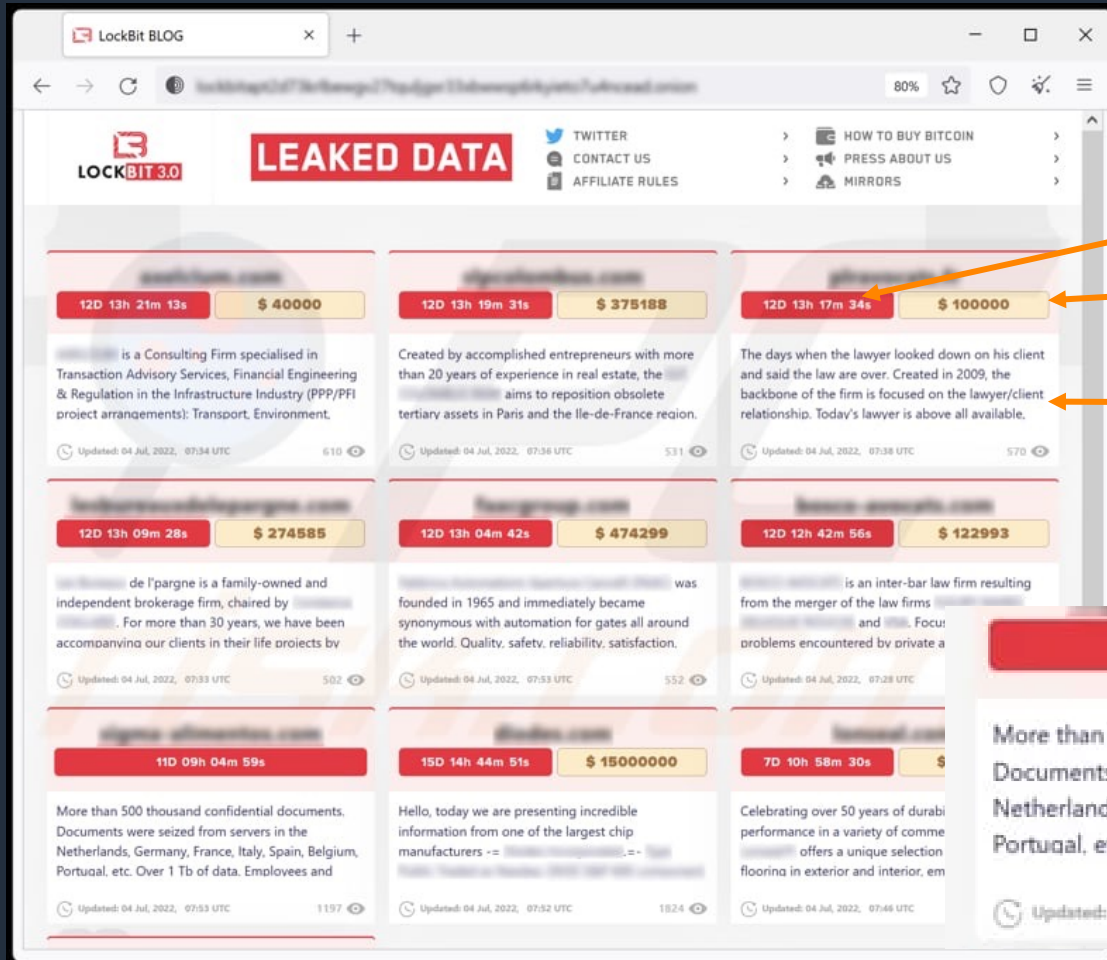
How to decrypt files? Buy XMR (no need for verification)

24/7 Customer Support!

REvil Example

LockBit 3.0 Marketplace For Leaked Data

EXFILTRATED DATA CAN BE LEAKED, EXTORTED, AND SOLD



Ransom Deadline

Price For Data

Summary of Target

Of Buyers Watching



Quad Extortion: Direct End Customer Contact

From: Administrator <[redacted]>
Sent: Monday, June 19, 2023 8:43:06 PM
To: [redacted] <[\[redacted\]@student.manchester.ac.uk](mailto:[redacted]@student.manchester.ac.uk)>
Subject: !!!Manchester.ac.uk Cyber Incident 06.06.2023 Data leakage!!

This Message Is From a New External Sender
You have not previously corresponded with this sender. Please exercise caution when opening links or attachments included in this message.

Hello,

We would like to inform all students, lecturers, administration, and staff that we have successfully hacked manchester.ac.uk network on June 6 2023.

We have stolen 7TB of data, including confidential personal information from students and staff, research data, medical data, police reports, drug test results, databases, HR documents, finance documents, and more. and more. The administration is fully aware of the situation and had been in discussion with us for over a week. They, however, value money above the privacy and security of their students and employees. They do not care about you or that ALL your personal information and research work will soon be sold and/or made public!

The persons responsible for the situation include: Professor Dame Nancy Rothwell, Professor Luke Georghiou, Patrick Hackett, Professor Colette Fagan, Professor Nalin Thakkar, Professor Graham Lord, Professor Keith Brown, Professor Martin Schröder, Adèle MacKinlay, Carol Prokopyszyn.

This is our last warning.

Source: <https://www.bleepingcomputer.com/news/security/hackers-warn-university-of-manchester-students-of-imminent-data-leak/>



Quad Extortion: Informing The SEC Of Material Breach

The screenshot shows a web browser window with the URL <https://tcr.sec.gov/TcrExternalWeb/faces/pages/intake.jspx>. The form contains the following elements:

- A list of radio button options for complaint categories:
 - General trading practices or pricing issues
 - Manipulation of a security
 - Insider trading
 - Material misstatement or omission in a company's public filings or financial statements, or a failure to file
 - Municipal securities transactions or public pension plans
 - Specific market event or condition
 - Bribery of, or improper payments to, foreign officials (Foreign Corrupt Practices Act Violations)
 - Initial coin offerings and cryptocurrencies
 - Other
- A prompt: "Please select the specific category that best describes your complaint."
- A dropdown menu with the selected value "Failure to file reports".
- A prompt: "* Is this supplemental information to a previous complaint?"
- A dropdown menu with the selected value "No".
- A prompt: "* In your own words, describe the conduct or situation you are complaining about."
- A text area containing the following text:

We want to bring to your attention a concerning issue regarding MeridianLink's compliance with the recently adopted cybersecurity incident disclosure rules.

It has come to our attention that MeridianLink, in light of a significant breach compromising customer data and operational information, has failed to file the requisite disclosure under Item 1.05 of Form 8-K within the stipulated four business days, as mandated by the new SEC rules.

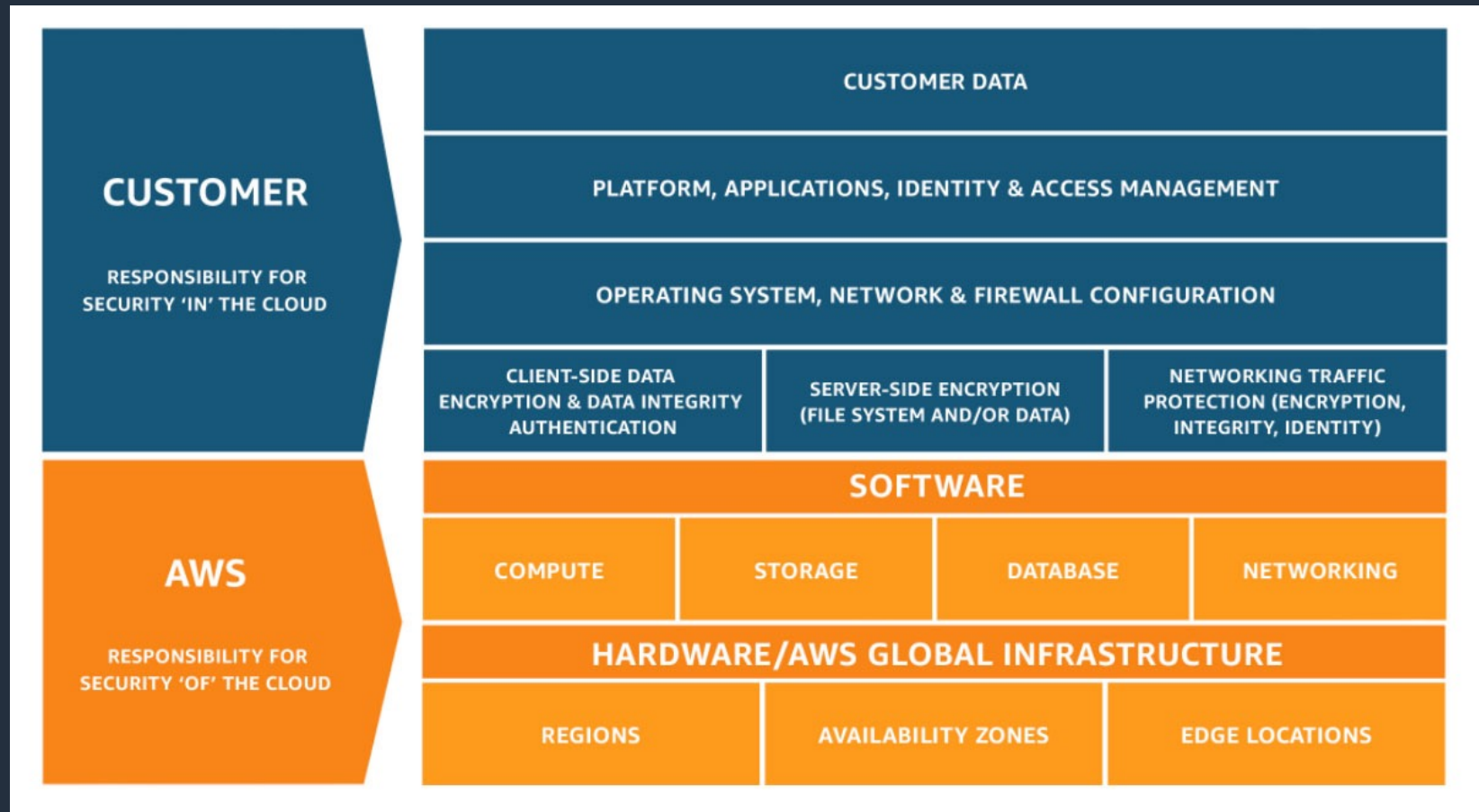
Source: <https://www.bleepingcomputer.com/news/security/ransomware-gang-files-sec-complaint-over-victims-undisclosed-breach/>

AWS Security Best Practices



Shared Responsibility Model For Security

RESPONSIBILITY FOR SECURITY OF THE CLOUD VS. SECURITY IN THE CLOUD



National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is the industry gold standard.



IDENTIFY

Identify an organization's critical functions, assets and processes and how cybersecurity risks could disrupt them



PROTECT

Define safeguards necessary to protect critical infrastructure services



DETECT

Implement the right measures to identify threats and cyber risks promptly



RESPOND

Define the measures necessary to react to an identified threat



RECOVER

Strategic plans to restore and recover any capabilities damaged during a cybersecurity incident

What is defense-in-depth?

LAYERED SECURITY TO ISOLATE THREATS

Policies, Procedures & Awareness

Threat Detection & Incident Response

Identity & Access Protection

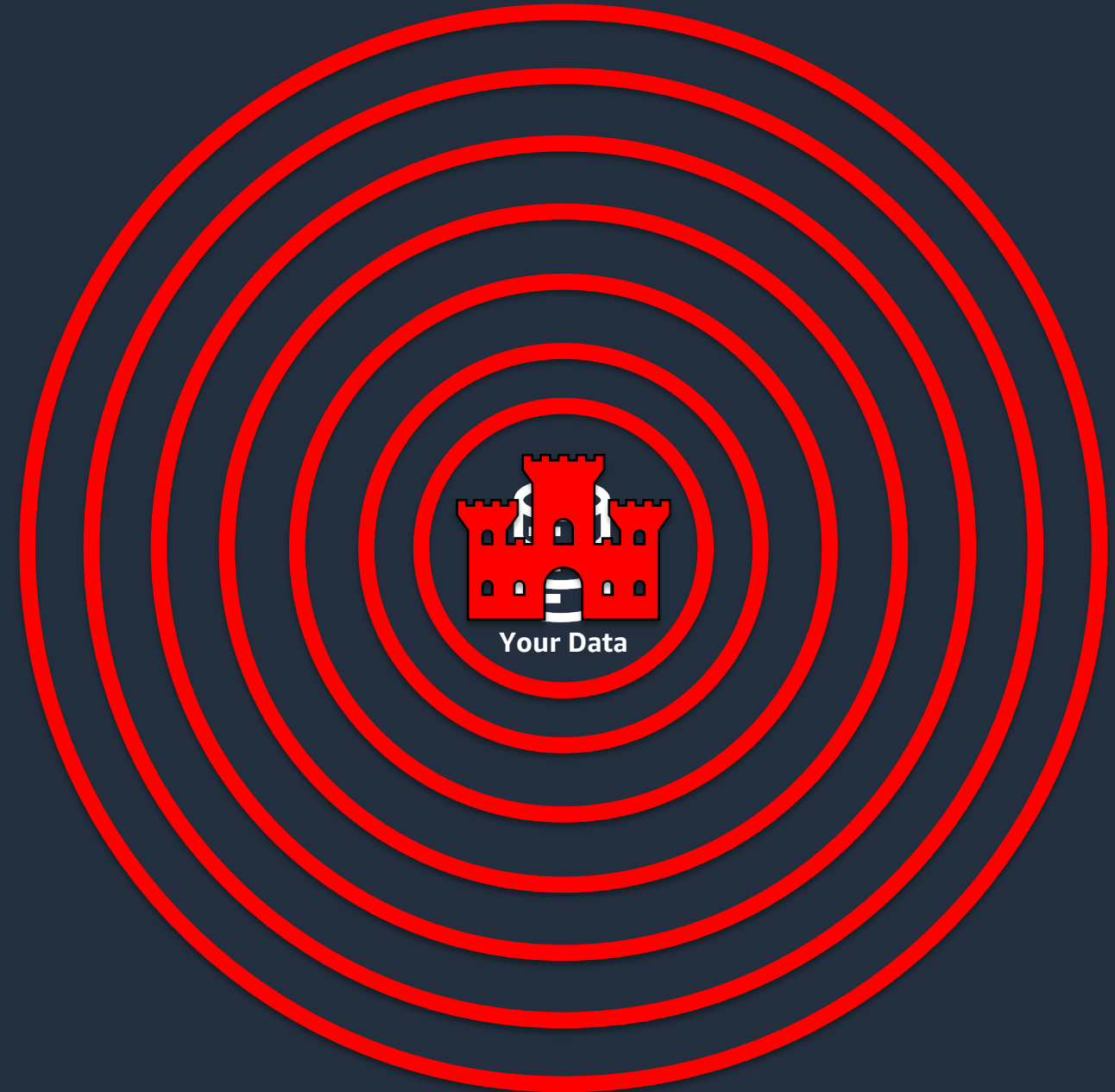
Perimeter Protection

Network & Edge Protection

Infrastructure Protection

Application Protection

Data Protection



Defense-in-depth layered security services

ALIGNING AWS SECURITY SERVICES TO THE NIST CYBERSECURITY FRAMEWORK



AWS Organizations



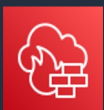
AWS Shield



AWS Certificate Manager



AWS KMS



AWS Network Firewall



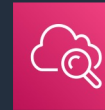
Amazon GuardDuty



Amazon Macie



Amazon Security Lake



Amazon EventBridge



AWS Step Functions



AWS OpsWorks



AWS Security Hub



AWS WAF



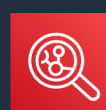
AWS Firewall Manager



AWS CloudHSM



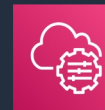
AWS Secrets Manager



Amazon Inspector



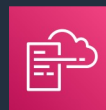
AWS Security Hub



AWS Systems Manager



AWS Lambda



AWS CloudFormation



AWS Config



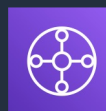
AWS Trusted Advisor



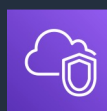
Amazon Cognito



IAM



AWS Transit Gateway



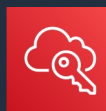
Amazon VPC



AWS Systems Manager



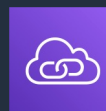
AWS Control Tower



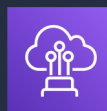
AWS IAM Identity Center



AWS Directory Service



Amazon VPC PrivateLink



AWS Direct Connect



Amazon Detective



Amazon CloudWatch



AWS CloudTrail



Amazon S3 Glacier



CloudEndure Disaster Recovery



Snapshot








Archive

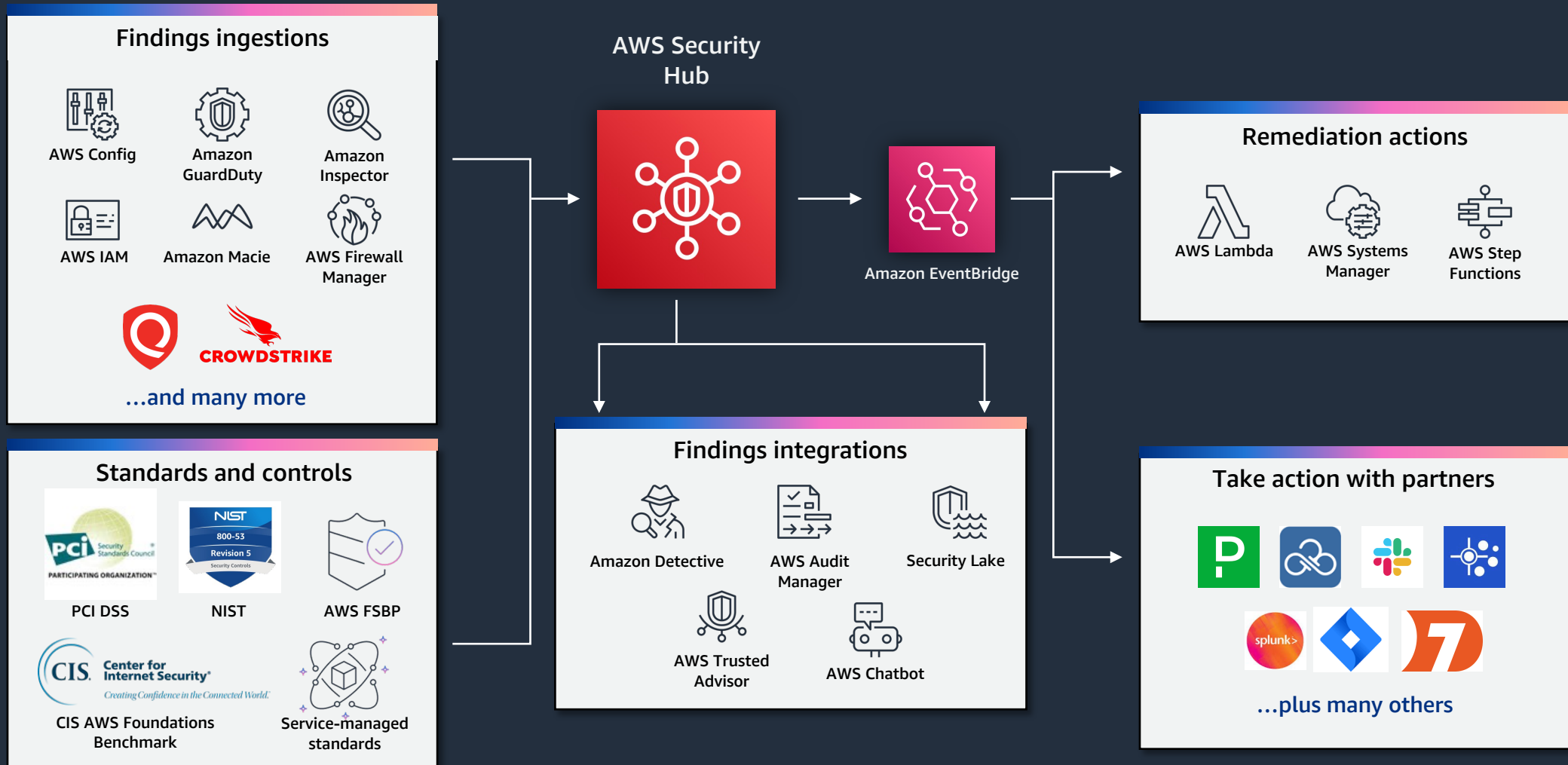


Layered AWS Core Security

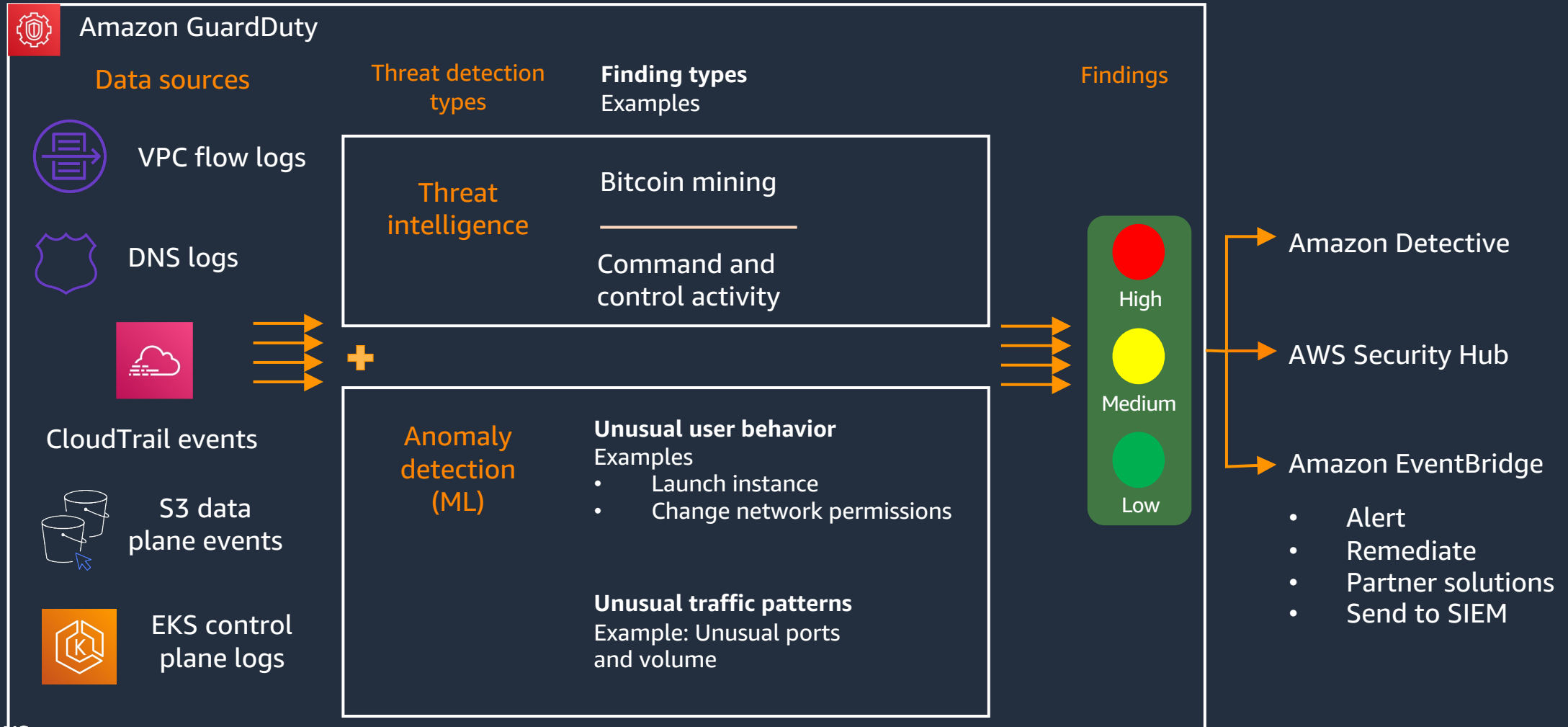
MINIMUM RECOMMENDATIONS FOR AWS SECURITY DOMAINS & CORE SECURITY SERVICES

 Threat Detection & Monitoring	 Network & Application Protection	 Data Protection	 Privacy & Compliance	 Identity
<div data-bbox="377 721 718 913" style="border: 1px solid white; padding: 5px;"> <p>AWS Security Hub</p> <p>Amazon GuardDuty</p> <p>Amazon Inspector</p> </div> <p>Amazon Detective</p> <p>Amazon Security Lake</p> <p>Amazon CloudWatch</p> <p>AWS Config</p> <p>AWS CloudTrail</p> <p>Amazon VPC Flow Logs</p> <p>AWS IoT Device Defender</p>	<div data-bbox="751 721 1093 778" style="border: 1px solid white; padding: 5px;"> <p>AWS Shield Advanced</p> </div> <p>AWS Firewall Manager</p> <p>AWS WAF – Web Application Firewall</p> <p>AWS Network Firewall</p> <p>Amazon VPC</p> <p>Amazon VPC Lattice</p> <p>Route53 - DNS Firewall</p> <p>AWS Verified Access</p> <p>AWS Systems Manager</p>	<div data-bbox="1126 721 1467 963" style="border: 1px solid white; padding: 5px;"> <p>AWS Key Management Service (KMS)</p> <p>AWS Secrets Manager</p> <p>Amazon Macie</p> </div> <p>AWS CloudHSM</p> <p>AWS Certificate Manager</p> <p>AWS Private CA</p> <p>AWS VPN</p> <p>AWS Signer</p> <p>Server-Side Encryption</p>	<p>AWS Audit Manager</p> <p>AWS Artifact</p> <p>AWS Well-Architected</p> <p>AWS Wickr</p>	<p>AWS Identity & Access Management (IAM)</p> <p>AWS IAM Identity Center</p> <p>Amazon Cognito</p> <p>AWS Directory Service</p> <p>AWS Resource Access Manager</p> <p>AWS Organizations</p> <p>AWS Verified Permissions</p>

AWS Security Hub

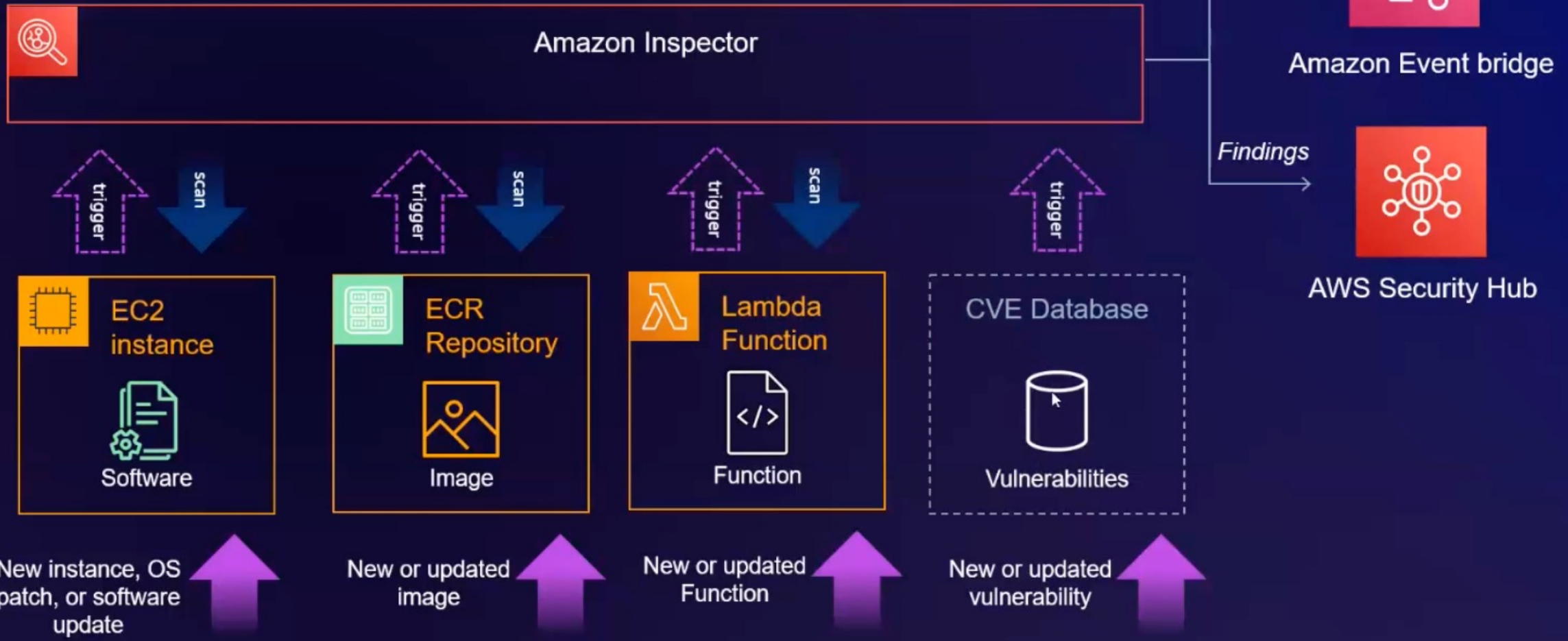


Amazon GuardDuty



Amazon Inspector

Amazon Inspector is an automated vulnerability management service that **continually** scans workloads for software vulnerabilities and unintended network exposure



AWS Key Management Service (KMS)

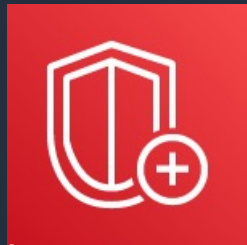


- AWS KMS lets you create, manage, and control cryptographic keys across your applications
- AWS KMS is incorporated in over 100 AWS services to encrypt sensitive data and create digital signatures.
- Supports AWS Managed Keys or Customer Managed Keys (CMK) for Bring Your Own Keys (BYOK).
- Supports Keep Your Own Keys (KYOK) with external key managers using AWS-XKS.
- Enables support for hybrid post-quantum TLS.

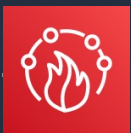
AWS Shield Advanced

ADVANCED DDOS PROTECTION AND COST PROTECTIONS

Protected Resources



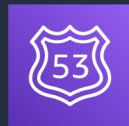
AWS Shield Advanced



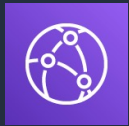
AWS Firewall Manager for Centralized Management



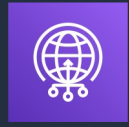
AWS WAF for Application protection



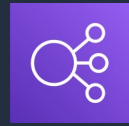
Amazon Route53



Amazon CloudFront



AWS Global Accelerator



Elastic Load Balancing



Elastic IP



Infrastructure and application protection (L3-7)



Application attack detection and automatic mitigation with AWS WAF



Near real-time events visibility and alerting



Health-based detection and proactive event response



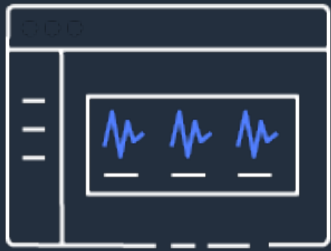
24/7 Support of AWS Shield Response Team



Cost protection for scaling during an attack

Amazon Macie

DISCOVER AND PROTECT YOUR SENSITIVE DATA AT SCALE



Gain visibility
and evaluate

- Bucket inventory
- Bucket policies



Discover
sensitive data

- Inspection jobs
- Flexible scope



Centrally manage
at scale

- AWS Organizations
- Managed & custom data detections



Automate and
take actions

- Detailed findings
- Management APIs

Security Accelerates Migrations & Increases Data Gravity

SECURITY EARNS TRUST. TRUST INCREASES DATA GRAVITY ON AWS.

+11%

Increase In Total AWS
Monthly Spend*

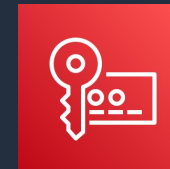
...on non-security
workloads when
customers use at least
the four Core Security
Services together.



AWS Security Hub



Amazon GuardDuty



AWS Key
Management
Service (AWS KMS)

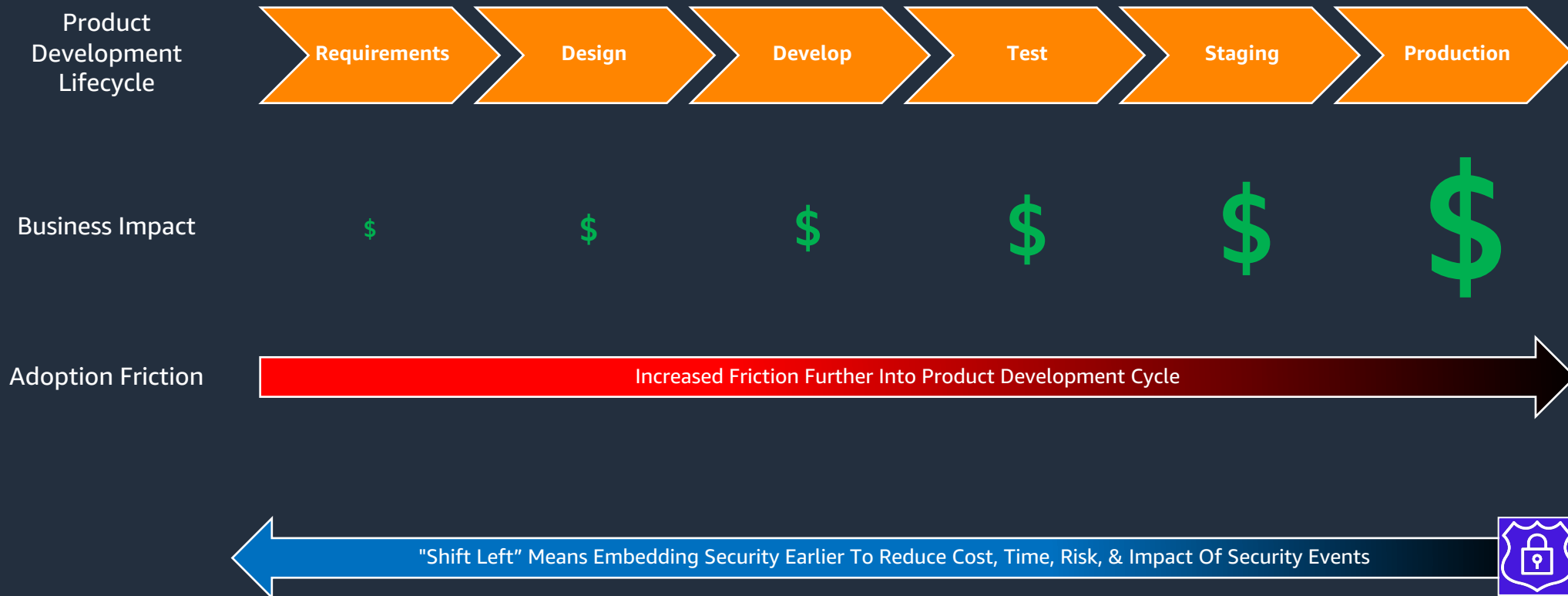


AWS Shield
Advanced

* Source: "Preliminary Results for ESS Adoption Analysis" Econometrics Study, February 10th, 2022.

What Does “Shift Left” Mean?

EMBEDDING SECURITY EARLIER REDUCES FRICTION, RISK, TIME, COST, AND BUSINESS IMPACT



Putting It All Together



Top 10 Best Practices For Ransomware Protection

IDENTIFY, PROTECT, DETECT, RESPOND & RECOVER

1) Leverage a security framework like NIST CSF.

6) Implement centralized logging and monitoring with CloudTrail, Security Hub, and Amazon Security Lake.

2) Automate patching & systems hardening with Amazon Inspector.

7) Implement and test backup and restore processes regularly with AWS Backup and AWS Disaster Recovery.

3) Use short-lived, temporary credentials with AWS IAM.

8) Prepare and exercise an incident response plan.

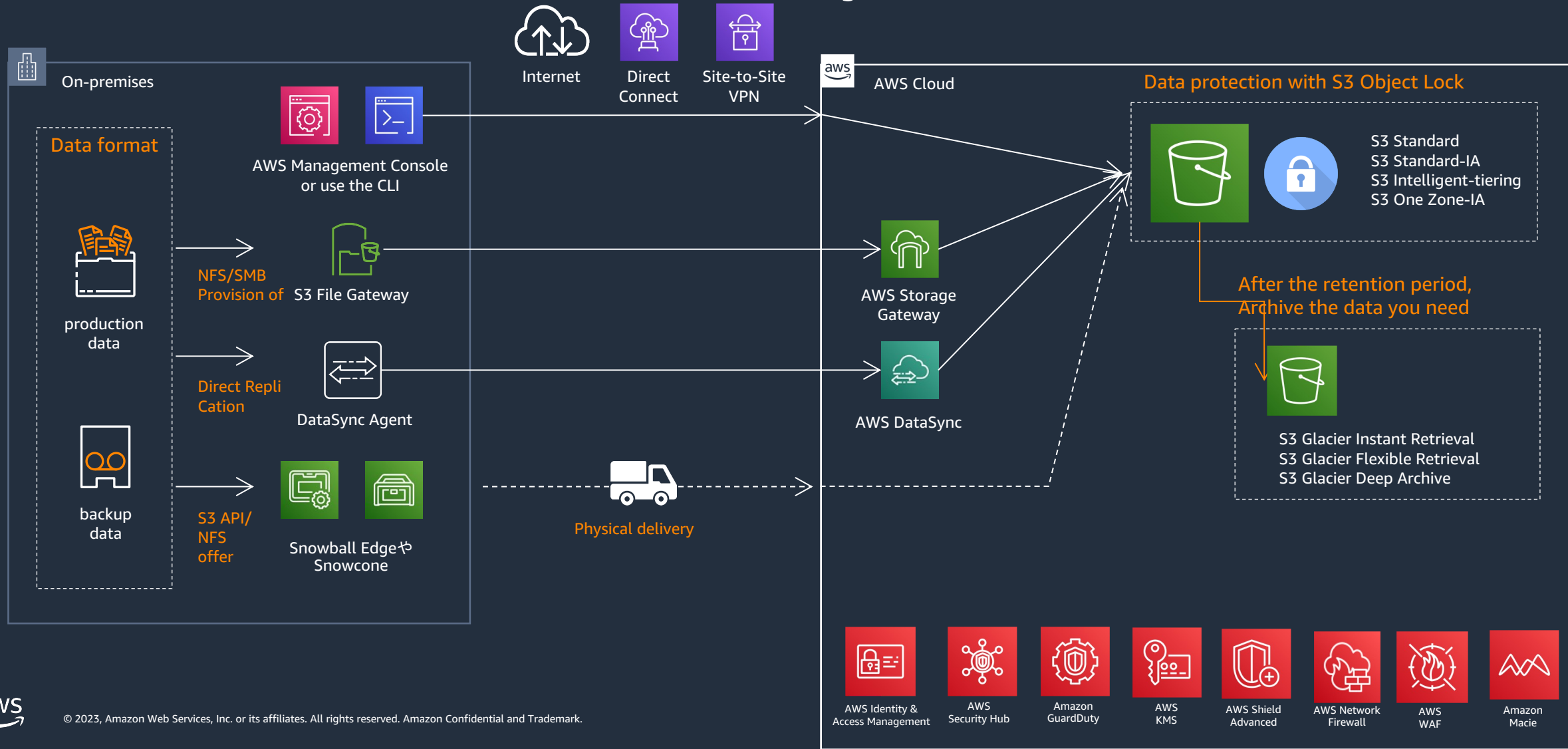
4) Implement multi-account structure with VPC isolation, ingress and egress policies in AWS Network Firewall.

9) Perform security posture self-assessments.

5) Use immutable infrastructure with no human access (e.g. AWS Backup Vault Lock, MFA on Delete)

10) Automate security guardrails and response actions.

Ransomware Protection & Recovery Best Practices



Key Takeaways

- ➔ Ransomware continues to increase and evolve as a business threat.
- ➔ Customers should have a strategy to identify, protect, detect, respond and recover from ransomware.
- ➔ AWS provides integrated Security and Storage solutions against ransomware.
- ➔ AWS + our partners deliver “better together” protection.

Additional Resources



Learn More

- [Protecting Against Ransomware With AWS](#)
- [Ransomware 101](#)
- [Ransomware FAQ](#)
- [How to Protect & Recover from Ransomware First Call Deck](#)
- [Download eBook: Protecting Your AWS Environment From Ransomware](#)
- [Blog: How To Approach Threat Modeling](#)
- [Blog: Top 10 Security Best Practices for Securing Data in Amazon S3](#)
- [Customer Workshop: Securing And Protecting Your Data In S3](#)



Getting Started

Check Your Customer's Security Posture

Run a FREE [Security Health Improvement Program Score \(SHIP\)](#) report

AWS Services

- [Amazon S3](#)
- [AWS Backup](#)
- [AWS Security Hub](#)
- [Amazon GuardDuty](#)
- [AWS Key Management Service \(KMS\)](#)
- [AWS Shield Advanced](#)
- [AWS Macie](#)



Get Help

Get Help

- [AWS Security Incident Response Guide](#)
- [AWS WWSO Security Wisdom](#)
- [AWS WWSO Security Specialists](#)
- [AWS Professional Services](#)
- [AWS Partner Solutions for Ransomware](#)
- [AWS ISV Partner Summary](#)
- [AWS Ransomware Partner Solution Matrix](#)

Stay Informed

- Subscribe to [SecurityBytes Newsletter](#)
- Join [#wwso-security-field-enablement](#)
- Join [#wwso-security-newsfeed](#)



Q&A



Thank you!

Huy Tran