亚马逊云科技

2021 Security Day

亚马逊云安全：我们在哪里，我们要去哪里

主要内容

1) 2020安全产品的亮点
2) 新的安全产品
3) 2021要面对的十大安全焦点

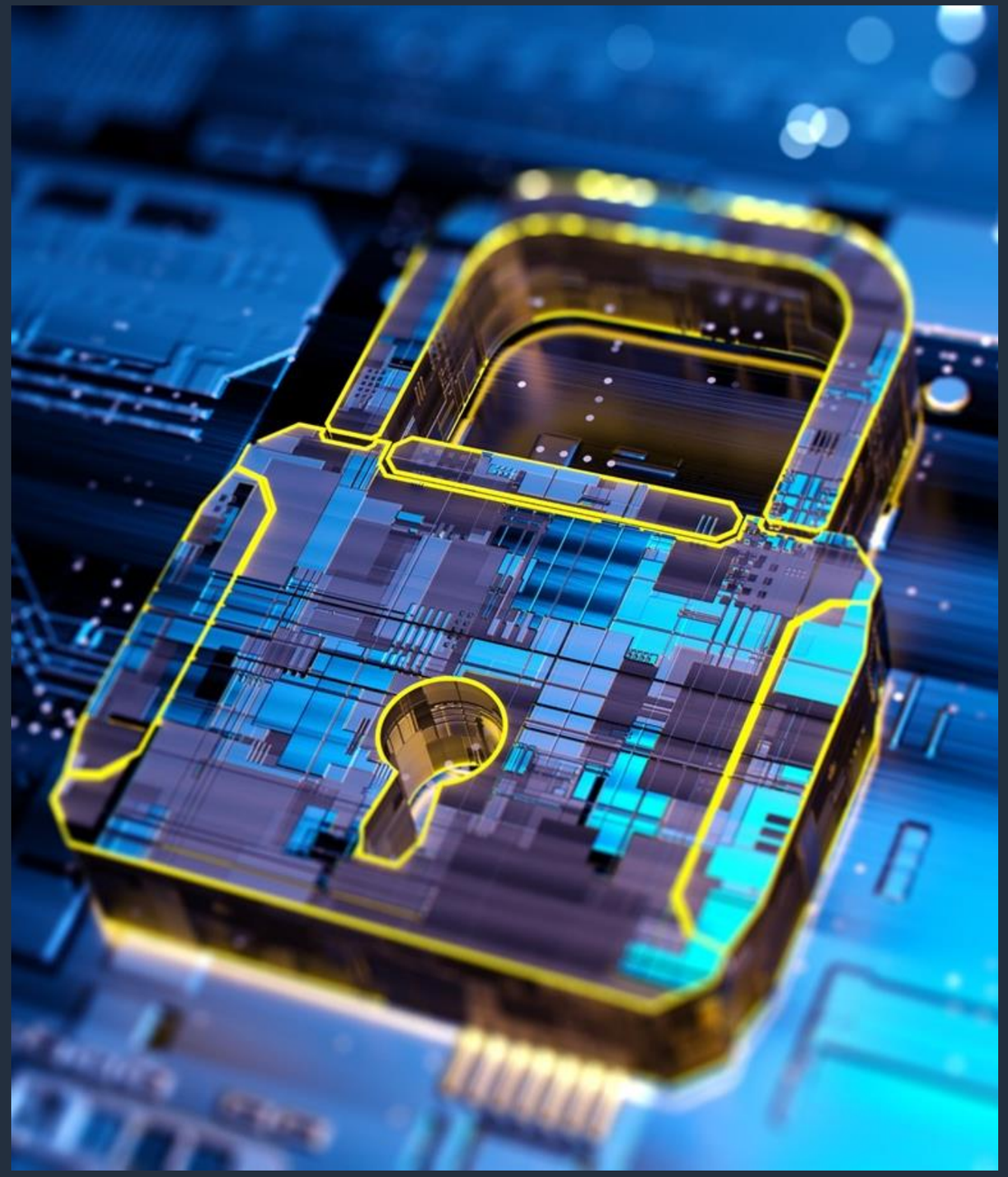
2020安全产品的亮点

亚马逊云科技

2020安全产品的亮点

危胁检测

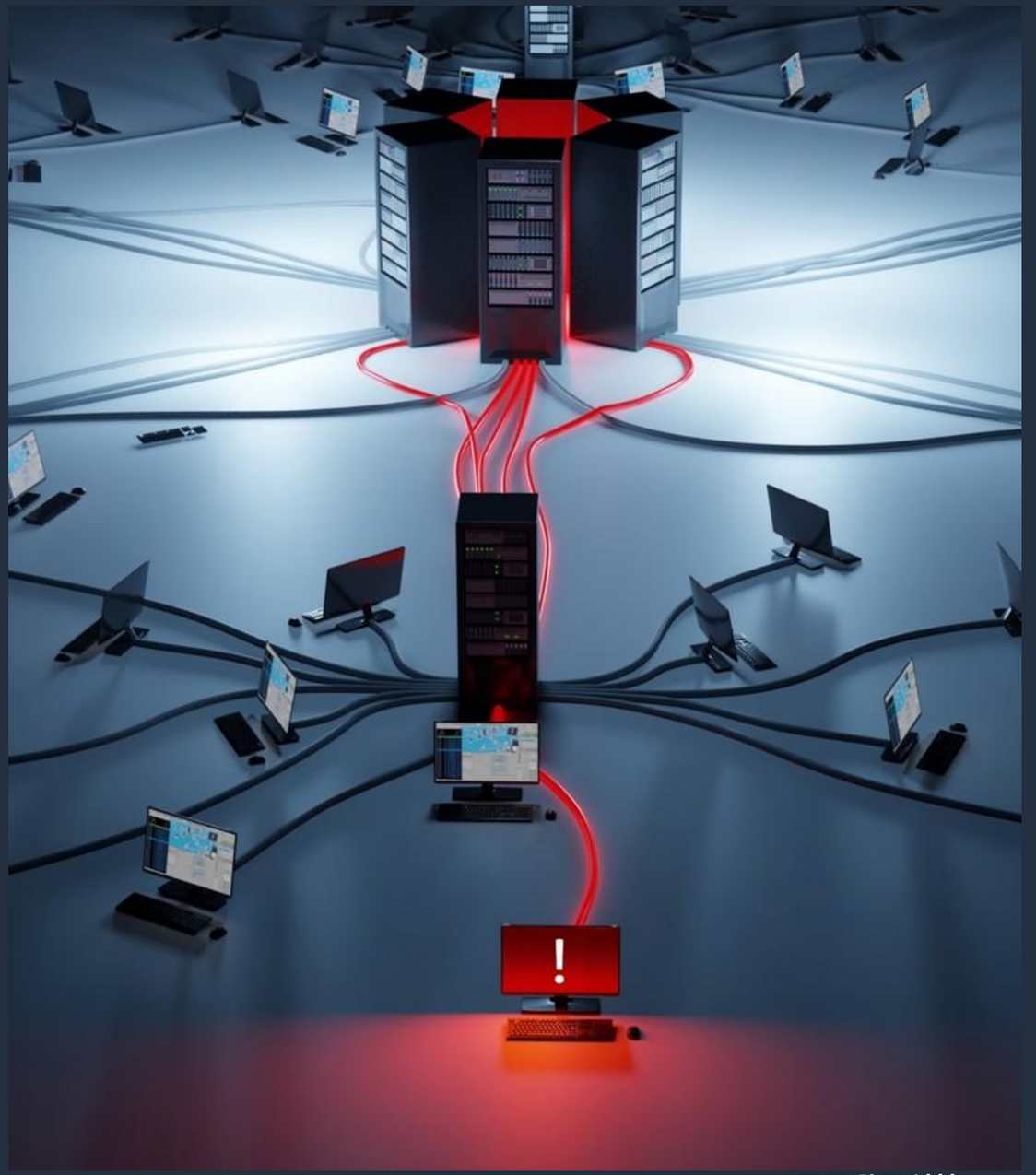
Amazon GuardDuty 扩展了危胁检测的覆盖面，在原来的VPC流日志，DNS日志，CloudTrail日志的基础上，加入了对S3日志的分析，实现对存储数据的入侵检测。



2020全产品的亮点

危胁检测

Amazon GuardDuty 通过集成AWS Organizations 提供多账户支持，因此可以跨所有现有账户和新账户启用 GuardDuty，并且可以将组织中各账户的发现结果聚合到一个 GuardDuty 管理员账户中，以便进行管理。

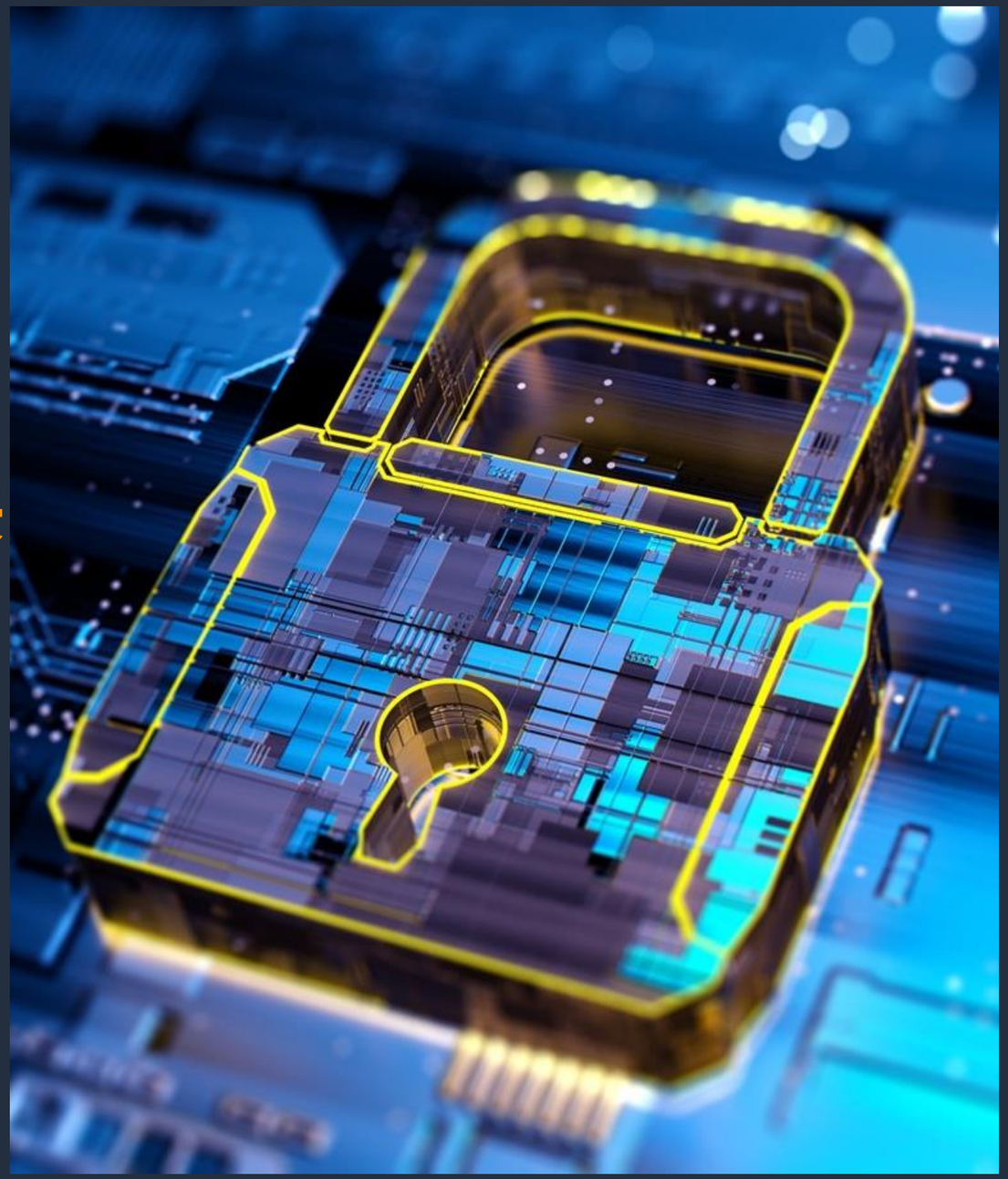


2020安全产品的亮点

危胁检测

Amazon GuardDuty 现已在 AWS 中国区域推出

- **对所有账号无条件，不设上限提供免费试用30天**
- **不会影响用户的应用性能，可直接上生产环境**
- **一键开启，无需代理**



2020安全产品的亮点

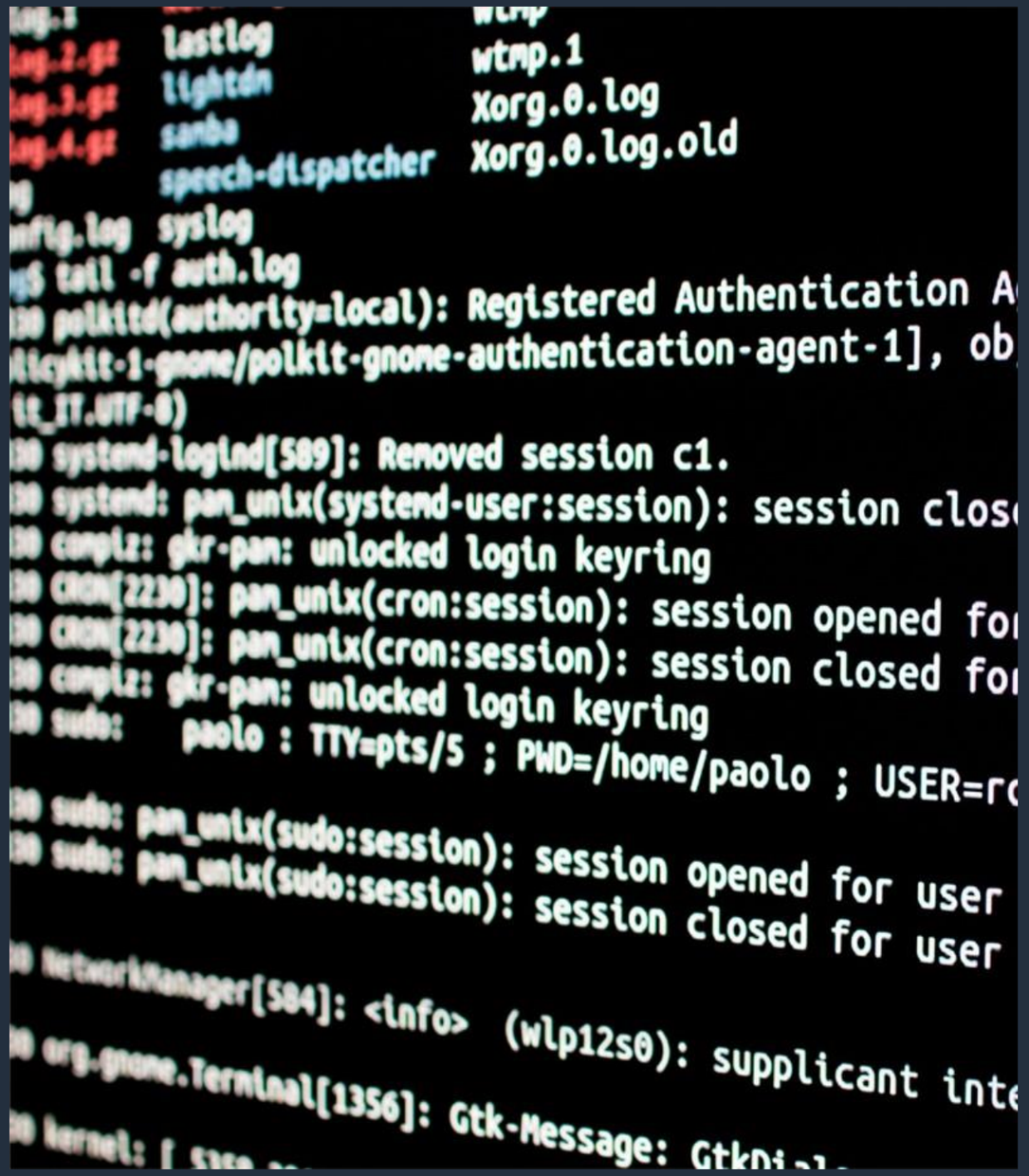
基础架构安全

Firewall Manager防火墙管理工具现在支持WAF，包括托管规则 (AMR)。Firewall Manager 是一种安全管理工具，可跨账户和资源集中配置和管理防火墙规则，包括 WAF、Shield 和 VPC 安全组。除了合作伙伴托管的应用商店规则之外，客户现在还可以跨账户和资源集中启用 托管规则。

2020安全产品的亮点

基础架构安全

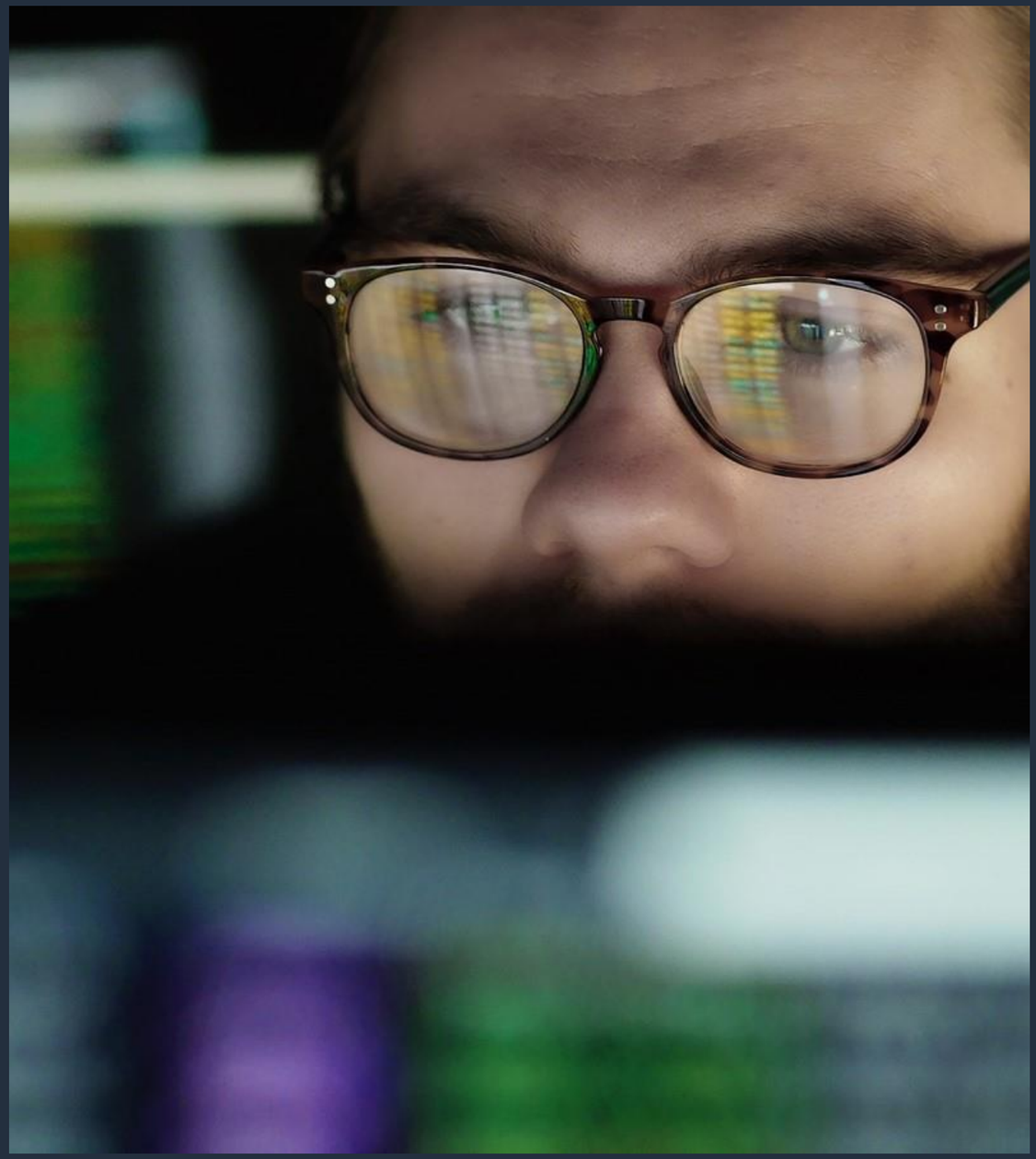
Firewall Manager防火墙管理工具现在支持将WAF、Shield 和 VPC 安全组的日志进行集中管理。



2020安全产品的亮点

身份认证

Amazon Detective 引入了IAM角色会话分析。启动此功能后，可自动整理关于IAM角色在角色会话中所执行的活动的数据，确定API调用来自于哪个特定主体（EC2实例，IAM用户，联合身份用户）。



2020安全产品的亮点

身份认证

通过IAM Access Analyzer对Organizations里的访问策略进行持续分析，并报告相关发现，包括可公开访问的资源，可跨账户访问的资源，可外部访问的资源。

IAM Access Analyzer 现已在 AWS 中国区域推出

2020安全产品的亮点

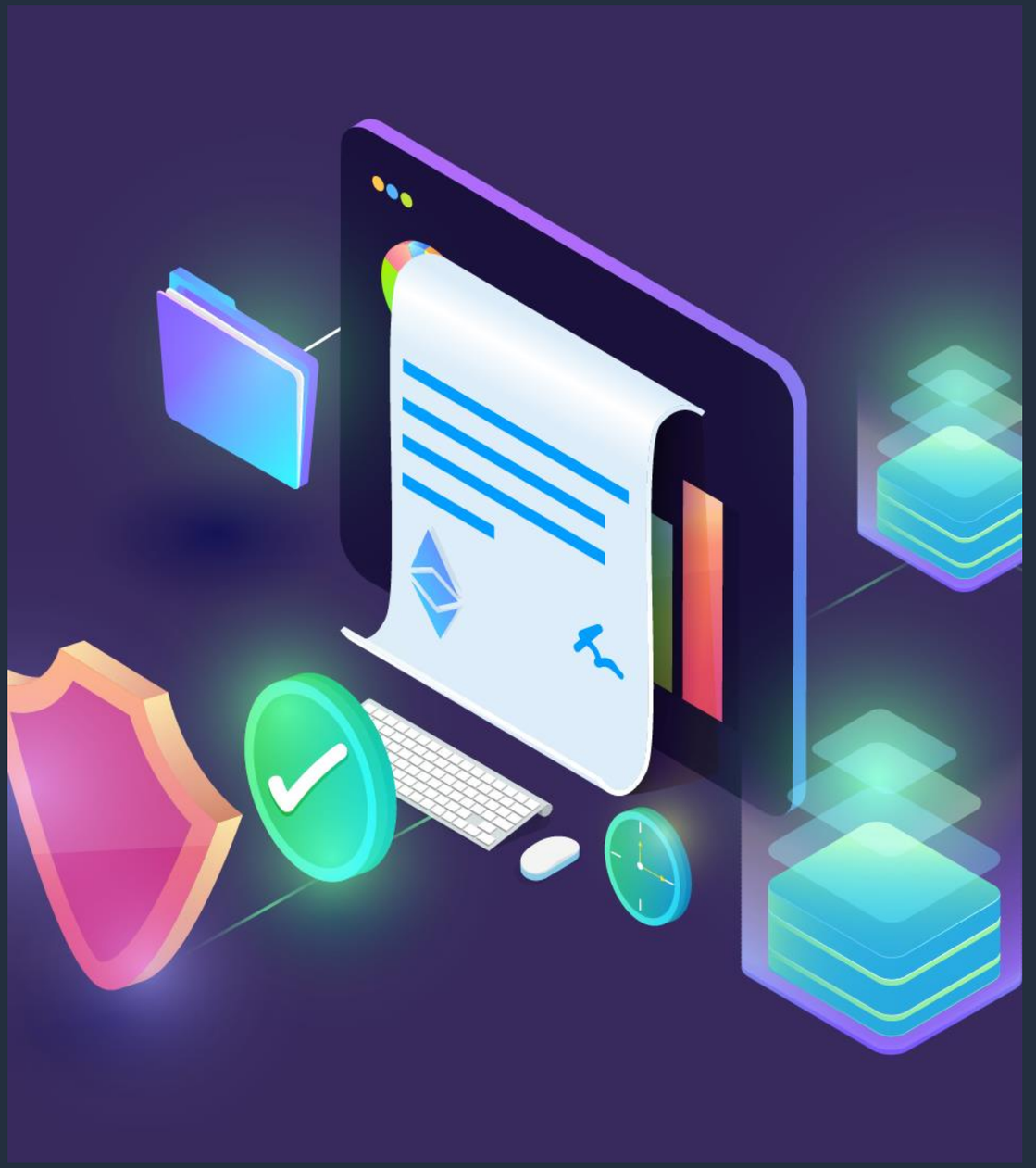
身份认证

Single Sign-on 通过CloudFormation 能够在构建新账户的同时自动化账户分配。

2020安全产品的亮点

身份认证

ACM PCA私有证书现在支持与其他账户或在一个Organizations内共享私有CA。



2020安全产品的亮点

数据保护

金融，国防，媒体 和娱乐以及生命科学等行业的用户需要处理高度的数据，处理过程需要防止内部和外部危胁。通过 Nitro Enclaves, 可以在任何由Nitro系统提供支持的EC2实例上创建隔离环境。

2020安全产品的亮点

数据保护

Amazon Macie 为客户减少80%的成本

2020安全产品的亮点

事件响应

Amazon SecurityHub 现已在 AWS 中国区域推出

- **对所有账号无条件，不设上限提供免费试用30天**
- **不会影响用户的应用性能，可直接上生产环境**
- **一键开启，无需代理**
- **对安全事件进行汇聚分析，并用合规标准进行持续监控和评分**

新的安全产品

亚马逊云科技

Audit Manager

可持续对应用做风险和合规分析，并产生可用于审计的报告和证据

自动化地收集证据

自动将合规要求匹配到相关资源

按需产生自定的可用于审计的报告

确保报告和证据的完整性，不被窜改

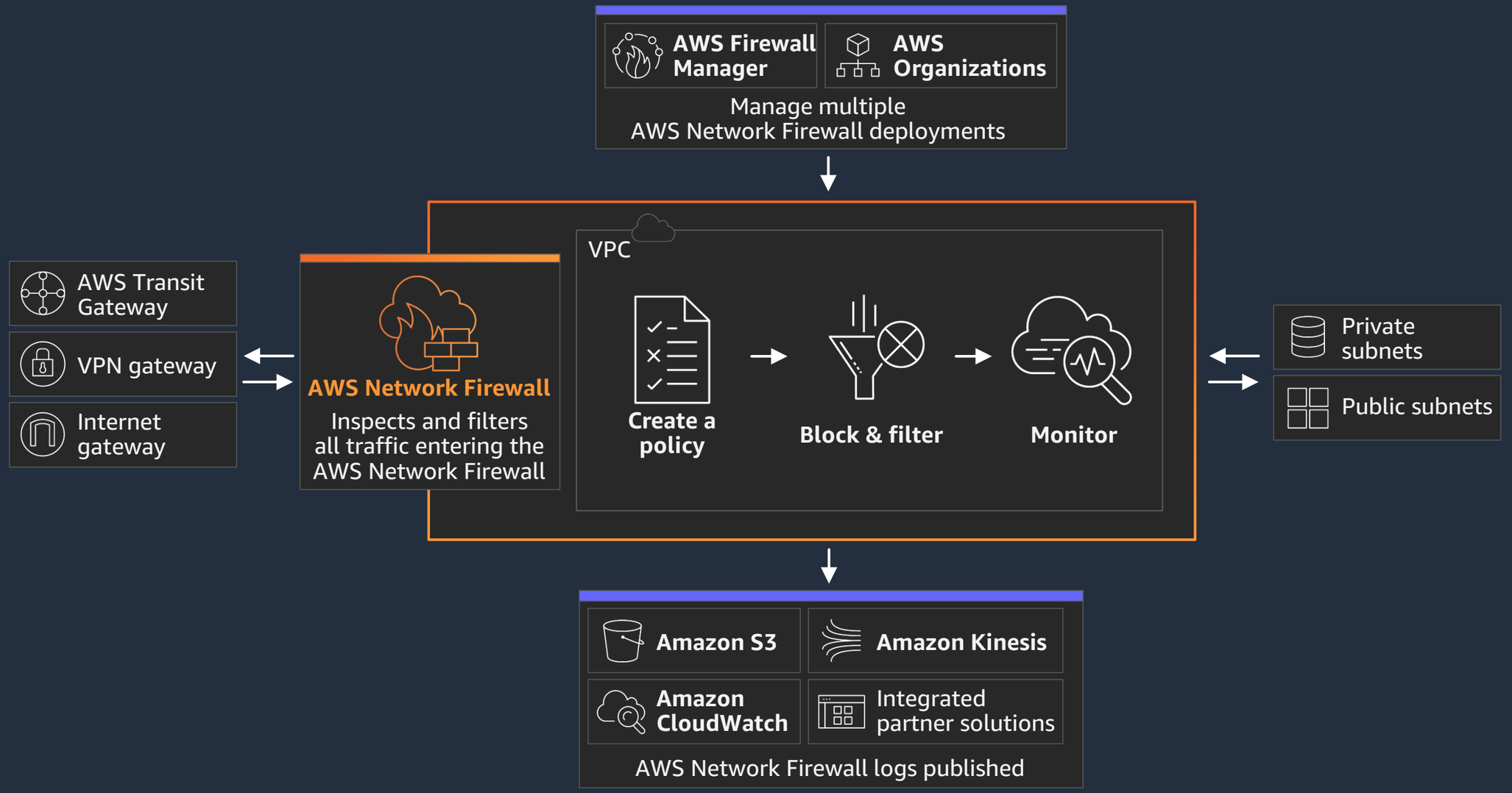
使用案例

- 从手工收集到自动收集
- 持续合规
- 内部风险评估
- 减少人工干预

免费试用

1. 进行Audit Manager Console界面
2. 使用预置好的框架或都自定义框架
3. 指定资源的内部审计负责人
4. 基于收集到的证据产生可用于审计的报告

Network Firewall



亚马逊云科技

2021要面对的十大安全焦点

亚马逊云科技

十大需要注意的安全问题

1. 使用Organizations
2. 了解整个应用和服务使用情况
3. 使用数据加密
4. 整合人员的访问
5. 留意账户的公开访问
6. 边缘服务的防护
7. 补丁管理
8. 张驰有度的防护
9. 透明可见
10. 团队多样化及培训

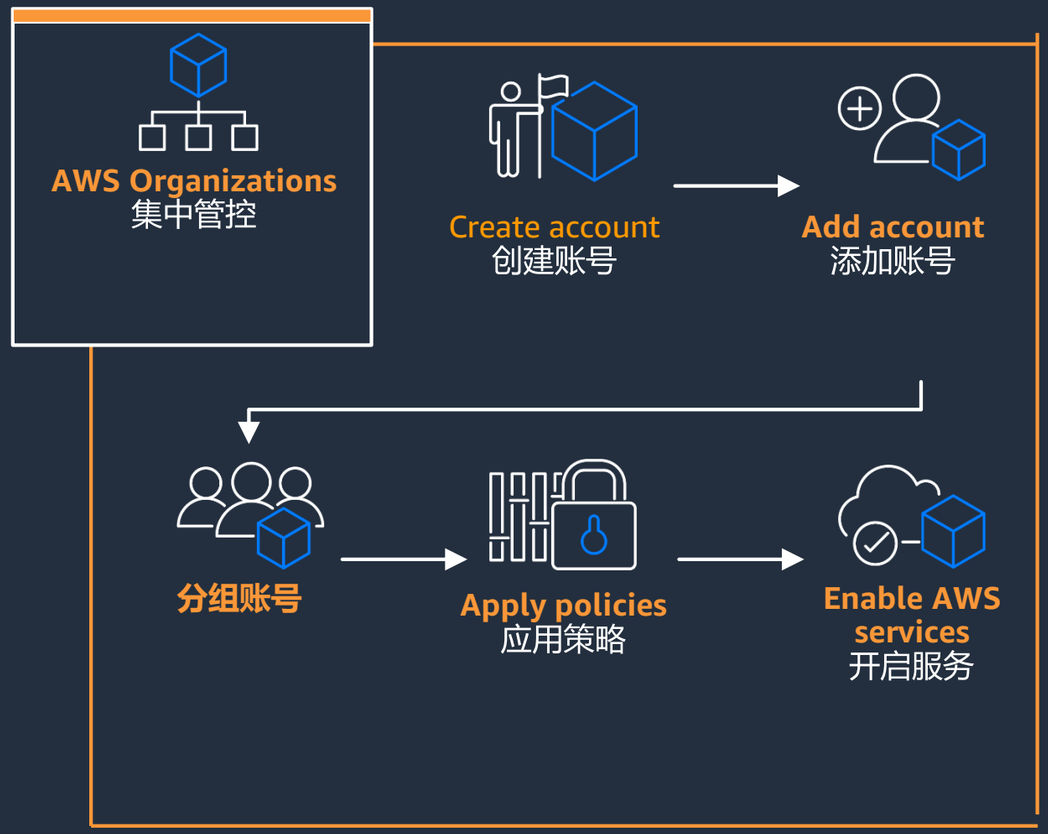
使用Organizations

集中管理和监控整个账户环境

包括:

- 集中配置
- 安全机制设置
- 审计要求
- 资源分享

Organizations 是免费服务



了解整个应用和服务使用情况

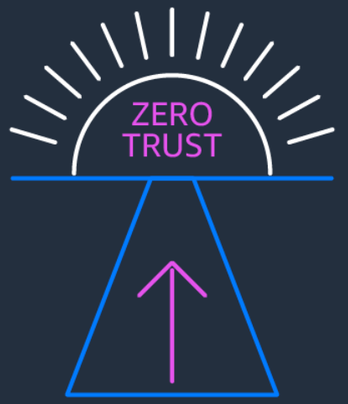
通过以下服务主动进行改进，提高安全水平

Tools:

- AWS IAM Access Analyzer
- AWS Config
- AWS Security Hub

整合人员的访问

- 对会话打标签，并建立对应的策略
- 基于零信任的原则进行设计



留意账户的公开访问

- 默认阻止对S3存储桶的公开访问
- 对需要公开访问的内容，要遵循最小路径和最小授权的原则

边缘安全

- 对边缘服务 CloudFront, R53, AGA加载 Shield advanced或者WAF，实现抗D

补丁管理

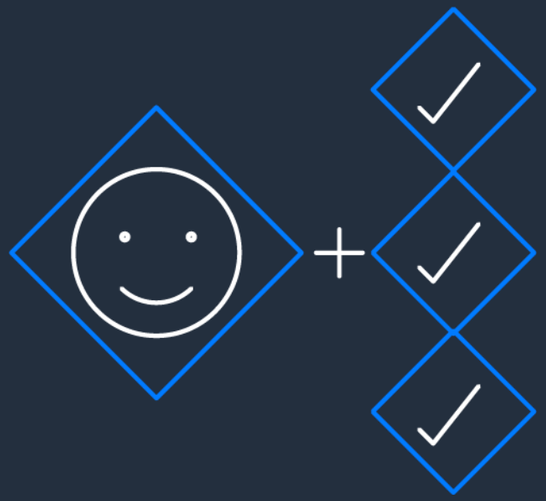
- 通过Inspector来发现相关漏洞，可能通过System Manager来打补丁

张驰有度

- 结合实际需要，打造张驰有度的防护

透明可见

- 要发现根本原因
- 发现安全事件发生的原因
- 减少对业务的影响的同时，提供安全水平
- 可视化，可总结，可报告



团队多样化及培训

- 团队成员的多样性，以及更宽广的视野，多方面来设计安全
- 团队安全能力的建设

两个方向—区域/行业合规的介绍及最佳实践

- 分六大区域，中国，东南亚，日韩，欧盟，南美，北美，来介绍区域合规要求及最佳实践
- 按行业行规，PCI-DSS, HIPPA, TISAX等来介绍行业合规要求及最佳实践

两个方向—提供更多的试用服务

- GuardDuty, SecurityHub, Inspector, Audit Manager等服务都提供了试用，鼓励更多的用户来试用。
- 不影响生产环境，一键开启，免费的试用
- 安全的第一步，就是试用

亚马逊云科技

谢谢！