elastic

# 利用 Elastic 助力您的数据安全合规

# 执行摘要

随着网络安全威胁形势日益复杂——网络攻击变得更加频繁、更具针对性、更隐蔽且技术更先进——构建强大且全面的数据安全势在必行。与网络安全相关的法律要求和潜在责任也愈发复杂和严苛，这使得基于风险的安全策略成为绝对必要。

为了跟上不断扩大的安全相关监管要求，防止可能造成破坏性影响的业务中断，并防范因安全漏洞而引发的代价高昂的诉讼风险，企业应采取全面、战略性的网络安全方法。未能做到这一点，不仅会使企业面临重大的法律和财务后果，还会对其运营和声誉造成无法挽回的损害。

本白皮书探讨了组织如何利用 Elastic 履行安全义务，构建真正有韧性的网络威胁防御体系。Elastic 强大、灵活且可扩展的解决方案帮助企业满足多样化、多方面的合规和运营网络安全需求，包括：

- 提升跨攻击面数据的可见性与可搜索性
- 简化合规请求的数据提取流程
- 简化威胁检测与修复的自动化流程
- 监控和展示您的安全态势
- 丰富的威胁情报

下文，我们将概述各法律框架中通用的基础安全概念；审视未能以基于风险且合规的方式实施这些概念可能导致的后果；并阐述组织如何利用 Elastic 的平台和解决方案来帮助满足合规义务并降低安全风险。

***请注意：****本白皮书仅供参考，不构成法律建议。请咨询您的法律顾问以获取法律建议。*

  

# 基础安全原则及相关合规义务

现代安全合规环境由一系列针对特定司法管辖区、特定行业和特定数据的要求拼凑而成。因此，组织的责任因其所在地、业务开展地、处理的数据类型及处理方式（包括数据的敏感性和业务性质）而异。

例如，一家全球性金融机构可能同时受美国联邦《格拉姆-里奇-比利雷法案》（“GLBA”）、纽约州金融服务部（“NYDFS”）《网络安全条例》、欧盟《数字运营弹性法案》（“DORA”）和欧盟《网络与信息安全指令 2》（“NIS2 指令”）等法律的约束。

而一家在美国上市的零售商可能需要遵守一系列不同的要求，例如支付卡安全领域的 PCI 数据安全标准（“PCI-DSS”）、财务报告系统安全领域的《萨班斯-奥克斯利法案》（“SOX”）要求，以及美国各州的数据泄露通知法。当然，还不能忽视隐私法律及其对个人信息保护的信息安全要求。

除了这些强制性要求外，许多公司还针对各种不同的第三方安全框架（如 ISO 27001、SOC 2、NIST CSF 或英国 Cyber Essentials）持有自愿性认证。

尽管存在这些差异，但法定、监管、自律及行业框架——以及通用的安全最佳实践——在很大程度上都围绕着一套核心安全原则。下文，我们将探讨这些原则的关键部分，并提供它们如何与各种框架相契合的示例。

  

# 数据清单、映射和分类

组织必须先了解其拥有哪些数据（即数据清单流程）、数据所在位置（数据映射）以及数据的敏感性（数据分类），才能部署基于风险的安全控制措施。

这些流程在发生数据泄露事件时也至关重要，以便公司能更好地判断受影响的数据是否会触发法定、监管或合同约定的泄露通知义务。因此，数据清单、映射与分类要么是多个框架明确要求的，要么是合规的必要前提。例如：

- *FTC 保障规则*（16 CFR § 314），该规则对受 GLBA 约束的特定金融机构提出了实施要求，要求受监管的金融机构在风险评估过程中识别并评估客户信息的敏感性。
- *HIPAA 安全规则*（45 CFR § 164.308）同样要求相关实体清点和保护受保护的电子健康信息（“ePHI”）。
- 根据欧盟《通用数据保护条例》（“GDPR”）第 30 条，组织必须维护处理活动记录，这实际上就要求建立数据清单和映射以证明合规性。
- 美国各州的泄露通知义务通常仅在涉及该州居民的特定类型的敏感个人数据遭到泄露时才会触发。因此，在数据泄露场景中，公司必须能够确定受损数据集中包含哪些数据类别。
- NIST SP 800-53 和 CIS 控制措施等框架强调数据分类，以确保保护措施与数据敏感性相匹配。通过建立清晰的清单和分类方案，公司可以更有信心地实施访问控制、监控敏感数据流、满足监管义务，并降低未经授权披露的风险。

  

# 基于角色的访问控制

基于角色的访问控制（“RBAC”）是旨在确保个人仅能访问其履行职责所需的系统和数据（即“最小权限”原则）的措施。持续应用的 RBAC 可降低恶意内部人员未经授权访问的风险，并有助于限制入侵的影响范围。许多法律和行业框架都明确要求或强烈推荐 RBAC：

- 根据欧盟《通用数据保护条例》（GDPR），只有经过正式授权且有必要知悉的人员才能访问个人数据。更进一步，该法规将未经授权的访问定义为数据泄露的一种情况。
- 马萨诸塞州《个人信息保护标准》（201 CMR 17.04）要求在该州开展业务的公司实施安全的访问控制措施，将包含敏感个人信息的记录和文件的访问权限仅限于履行职责需要此类信息的人员。
- HIPAA 安全规则规定，对 ePHI 的访问权限应仅限于有合法知情权的人员。
- 欧盟 DORA 第 9(4) 条要求受监管的金融机构实施策略，将对资产的物理或逻辑访问限制在仅用于合法且经批准的功能和活动所需的范围内。
- NIST SP 800-53、ISO/IEC 27001 和 CIS 控制措施（例如 CIS 控制措施 6）等行业标准也强调 RBAC 是基础的访问管理实践。

  

# 日志记录和监控

安全事件日志是公司用于检测安全事件的最重要资源之一。反映诸如访问日期和时间、执行的操作以及执行操作的用户等信息的日志，对于验证系统访问是否授权以及调查潜在未授权活动至关重要。实时或近实时地监控日志也是及时发现和处理威胁的关键。

然而，对于拥有复杂、多样系统且每天可能产生海量日志的组织来说，日志管理可能是一项挑战。此类组织必须依靠技术解决方案来有效地聚合日志并监控其中的异常活动。法律和行业框架都强调了日志记录与监控的重要性：

- 支付卡行业数据安全标准 (PCI-DSS) 要求所有存储、传输或处理支付卡数据的公司记录并监控对系统组件和持卡人数据的所有访问。
- HIPAA 安全规则强制要求实施审计控制，以记录和检查包含 ePHI 的系统中的活动。
- SOX 第 404 条要求管理层和审计人员评估并报告上市公司财务报告内部控制的有效性。此类审计人员会依据 COBIT 等框架评估这些控制措施，而 COBIT 要求对用户活动、对财务系统的访问以及财务数据的更改进行审计日志记录。
- NIST CSF 的“检测”部分规定公司应记录安全事件并保持持续的安全监控，这对于根据例如欧盟 GDPR 第 32 条、欧盟 NIS2 第 23 条或欧盟 DORA 第 19 条等要求及时报告可通知事件也是不可或缺的。

  

# 入侵检测与响应

不幸的是，在当今的威胁形势下，每个组织都是网络攻击的潜在目标。组织必须维护入侵检测系统和流程，以便在不可避免的入侵企图发生时能够响应安全事件。这些系统至关重要，使公司能够快速识别和响应攻击，防止其升级为严重事件。然而，入侵检测系统和事件响应流程很少能开箱即用；相反，公司必须建立活动基线，并根据公司的独特属性定制告警标准。这种定制化提高了告警的准确性，并有助于确保事件根据其严重性得到恰当的分类和处理。入侵检测和响应是众多法律和行业框架的核心：

- 美国联邦、州及国际数据泄露通知法要求在规定时限内报告数据泄露事件。虽然通常认为 GDPR 规定的报告时限最短（在确定发生需报告的数据泄露后 72 小时内），但值得注意的是，DORA 要求重大信息和通信技术 (“ICT”) 相关事件在发现后四小时内报告。
- NYDFS 网络安全条例第 500.16 条要求受监管实体制定事件响应计划，以快速响应网络安全事件并从中恢复。
- DORA 还要求受监管的金融机构制定详细的事件响应计划。
- NIST CSF 规定公司需维护详细的“检测”和“响应”控制措施，以检测和响应安全事件。

  

# 不合规的代价

未能实施合规且有效的安全控制，可能会使公司及其领导层和董事会面临重大的法律、财务和声誉风险。从实际角度来看，监控工具或流程无效的组织面临着长期未经授权访问的风险，这可能使攻击者能够对公司进行侦察，更逼真地模仿授权活动，同时窃取数据或为勒索软件攻击奠定基础。不完整的日志记录也可能导致无法确定可疑或意外活动是否经过授权，从而引发过度通知或通知不足。

在发生数据泄露或网络安全事件时，数据映射和清单不充分可能导致难以识别受影响的数据。这可能导致通知受影响方和监管机构的延误。而这种延误反过来又会增加受害者遭受的潜在损害，违反监管报告时限，并因额外的损害赔偿要求、监管制裁以及进一步的执法和诉讼成本，加剧恢复和修复的即时负担。对于 B2B 供应商而言，这也可能使得更难识别哪些客户受到了事件影响。

未能满足诸如隐私法为保护个人信息而施加的强制性安全要求，可能导致巨额罚款、处罚及其他法律责任。所有企业还面临着因其信息在事件中遭泄露的原告提起的疏忽、违约或其他诉讼（通常是集体诉讼）的风险。值得注意的是，《加州消费者隐私法案》(CCPA) 为因公司未能维护“合理”安全措施而导致其敏感数据遭泄露的原告设立了私人诉讼权。根据 HIPAA、CCPA 或欧盟 GDPR 等法规，制裁和损害赔偿可能迅速达到七位数。

除了直接的合规处罚外，安全措施不力造成的声誉损害也可能非常严重。遭遇数据泄露或未能遵守安全法规的公司可能会失去客户信任，面临公众抵制，经历重大业务中断，并对其品牌价值造成长期影响。上市公司在安全失误被广泛宣传后，股价也可能面临下跌风险。风险包括客户流失，以及因未能充分保护客户数据而可能面临的赔偿要求，最终导致业务和收入损失。鉴于这些重大后果，公司应认真对待安全问题，适当投资于合规义务履行和降低安全风险。

  

# 利用 Elastic 实现合规

Elasticsearch Platform 是 Elastic 的两个开箱即用解决方案 Elastic Observability 和 Elastic Security 的基础。组织可以利用 Elastic 开放且灵活的平台来履行其合规义务，并应对跨多个渠道的关键网络安全风险。最重要的是，Elastic 的解决方案天生具有敏捷性和可扩展性；它们可以部署在多种系统和平台上并从中收集数据，其搜索能力可用于无数用例。以下是 Elastic 如何用于支持安全计划核心要点的几个示例：

## 数据映射和分类

Elastic 可以通过索引跨环境的结构化和非结构化数据来支持数据映射工作，使组织能够集中了解其数据的类型和位置。利用自定义标签、元数据和机器学习，Elastic 可以帮助识别数据中的模式（例如，个人数据、财务记录、系统日志），从而更容易根据敏感性或监管义务对数据进行分类。虽然 Elastic 并非专门的数据分类引擎，但其强大的搜索和分析功能可以集成到更广泛的数据治理计划中，帮助跟踪和清点跨云和本地系统的数据。

## 基于角色的访问控制 (RBAC)

虽然 Elastic 本身不是 RBAC 工具，但该平台可以摄取组织各系统的日志，帮助识别权限管理中的漏洞。组织可以分析访问模式，以确定用户组可能需要或不需要访问哪些系统，并据此为访问权限的分配提供依据。Elastic 还帮助我们的客户从各个系统摄取组访问策略，使公司能够基于这些数据生成报告，以便在审计或合规调查中证明访问权限的强制执行情况。此外，Elastic 在其 Elastic Security 和 Kibana 界面中包含内置的 RBAC 功能。管理员可以定义角色，限制用户对特定索引、仪表板或操作（如查看与编辑）的访问，从而支持最小权限访问原则。

  

# 日志记录和监控

Elastic 的核心优势之一和最常见的用例在于大规模聚合、存储和分析日志。使用 Elastic Agent，公司可以从终端、服务器、云服务和应用程序中摄取日志。这些日志被索引到 Elasticsearch 中，从而可以在 Kibana 中进行实时分析和可视化。Elastic 支持长期日志保留、告警和异常检测，使其成为理想的日志聚合和安全监控解决方案，也是一种有效的合规报告工具。其可观测套件还提供应用程序性能监测 (APM)、指标和运行状态监测，以实现全面的基础架构可视性。

许多法规，例如美国联邦政府机构的 M-21-31，要求组织在特定时间段内存储日志。Elastic 的数据分层结构使数据能够根据访问和使用的频率和速度，实现经济高效的数据存储。Elasticsearch logsdb 索引模式 **可将日志数据的存储占用空间减少 高达 65%**，在提高可见性和合规性的同时，使所有数据可立即用于分析。

仅举例，约克大学将其安全信息与事件管理 (SIEM) 系统迁移至 Elastic Security，以增强网络安全能力、提高运营效率并降低成本。通过在服务器、台式机和笔记本电脑上部署约 9,000 个 Elastic Agent，并收集来自大学混合云基础设施（包括 Google Cloud、AWS、Azure 和本地服务器）的日志，该大学每天摄取 500 GB 数据，存储 35 TB 日志。它还与 Palo Alto Networks 防火墙、Cloudflare 和 Duo 等安全工具连接，确保跨各种平台的全面监控。此设置支持在海量数据中快速搜索，将查询时间从几小时缩短到几秒。

# 入侵检测和响应

Elastic Security 包括终端检测和响应 (EDR) 功能，并集成了威胁情报源以支持入侵检测。它使安全团队能够使用行为分析、攻击映射和自定义检测规则来监测已知和未知的威胁。借助集中式日志记录，分析师可以快速关联跨系统的事件，在上下文中调查告警，并编排响应工作流。Elastic还支持通过与第三方安全编排、自动化与响应 (SOAR) 平台集成实现自动化响应，使其成为提升事件响应准备和威胁搜索的强大工具。这些高级功能降低了发生入侵的可能性，并在成功入侵发生时加快响应速度，从而减轻与事件相关的潜在法律责任。

  

领先的数字平台和转型服务商 AHEAD 通过将 Elastic Security 集成到其托管安全服务中，显著增强了入侵检测和响应能力AHEAD 现在将客户端安全数据摄取到运行于 Elastic Cloud 上的 Elastic 中，在那里数据被丰富、聚合，并连接到威胁情报源。Elastic 也是该公司 SOAR 系统的数据源。AHEAD 安全分析师还可以利用 AI 驱动的告警，突出安全事件中的相关信息，减少手动筛选海量数据所需的时间，并有助于降低误报的负担。

# 结论

随着网络安全威胁形势不断给组织带来复杂挑战，遵守日益增多的安全和数据隐私相关法规要求并降低风险也变得更加复杂。未能做到这一点，不仅会使企业面临重大的法律和财务后果，还会对其运营和声誉造成损害。Elastic 可以帮助 CIO 和 CISO 加强其组织对各种法律要求的合规性，尤其是在数据映射与分类、RBAC、日志记录与监控以及入侵检测与响应等领域。

  