elastic

Utilizando a Elastic para melhorar sua conformidade em segurança de dados

Resumo executivo

À medida que o cenário das ameaças de segurança cibernética se torna cada vez mais sofisticado — com ataques cibernéticos mais frequentes, direcionados, furtivos e tecnicamente avançados — a necessidade de uma segurança robusta e abrangente de dados nunca foi tão crítica. Os requisitos legais e os possíveis passivos relacionados à segurança cibernética também estão se tornando mais complexos e exigentes, tornando indispensável uma abordagem de segurança baseada em riscos.

Para acompanhar a lista cada vez maior de requisitos regulamentares relacionados à segurança, evitar interrupções potencialmente devastadoras nos negócios e proteger-se contra o risco de processos judiciais dispendiosos decorrentes de violações de segurança, as empresas devem adotar uma abordagem holística e estratégica para a segurança cibernética. Não fazer isso não apenas expõe as empresas a consequências legais e financeiras significativas, mas também a danos operacionais e reputacionais irreparáveis.

Este white paper explora como as organizações podem usar a Elastic para cumprir suas obrigações de segurança e construir uma defesa verdadeiramente resiliente contra ameaças cibernéticas. A solução poderosa, flexível e escalável da Elastic ajuda as empresas a atender às variadas e multifacetadas necessidades de conformidade e segurança cibernética operacional, incluindo:

- Maior visibilidade e capacidade de busca dos dados em superfícies de ataque
- Extrações simplificadas de dados para solicitações de conformidade
- Detecção e automação otimizadas para remediar ameaças
- Monitoramento e demonstração da sua postura de segurança
- Inteligência de ameaças enriquecida

A seguir, apresentamos uma visão geral dos conceitos fundamentais de segurança que são comuns em todos os frameworks legais; analisamos as possíveis consequências da falha na implementação desses conceitos de maneira baseada em riscos e em conformidade com as normas; e ilustramos como as organizações podem usar a plataforma e as soluções da Elastic para ajudar a cumprir as obrigações de conformidade e mitigar os riscos de segurança.

Observação: *Este artigo é fornecido apenas para fins informativos e não se destina a constituir aconselhamento jurídico. Consulte seu assessor jurídico para obter orientação legal.*

Princípios fundamentais de segurança e obrigações de conformidade relacionadas

O cenário moderno de conformidade de segurança consiste em um mosaico de requisitos específicos de jurisdição, setor e dados. As responsabilidades das organizações, portanto, variam dependendo de onde estão localizadas, onde realizam negócios, quais dados processam e como, incluindo a sensibilidade desses dados e a natureza do negócio.

Por exemplo, uma instituição financeira global pode estar sujeita simultaneamente à Lei Gramm-Leach-Bliley (“GLBA”) federal dos EUA, à Regulamentação de Segurança Cibernética do Departamento de Serviços Financeiros de Nova York (“NYDFS”), à Lei de Resiliência de Operações Digitais da UE (“DORA”) e à Diretiva 2 de Segurança de Informações e Redes da UE (“Diretiva NIS2”), entre outras leis.

Por outro lado, uma empresa varejista americana de capital aberto pode estar sujeita a uma gama diferente de requisitos, como os Padrões de Segurança de Dados PCI (“PCI-DSS”) para segurança de cartões de pagamento, os requisitos da Lei Sarbanes-Oxley (“SOX”) para a segurança de sistemas de relatórios financeiros e as leis estaduais americanas de notificação de violação de dados. Sem, é claro, esquecer as leis de privacidade e seus requisitos de segurança da informação para a proteção de dados pessoais.

Além desses requisitos obrigatórios, muitas empresas também mantêm certificações voluntárias para uma variedade de frameworks de segurança de terceiros, como ISO 27001, SOC 2, NIST CSF ou o UK Cyber Essentials.

Apesar dessas diferenças, os frameworks legais, regulamentares, de autorregulamentação e da indústria — bem como as práticas recomendadas gerais de segurança — convergem em grande parte em torno de um conjunto central de princípios de segurança. Abaixo, analisamos os principais aspectos desses princípios e fornecemos exemplos de como eles se alinham a diversos frameworks.

Inventário de dados, mapeamento e classificação

As organizações não podem implantar controles de segurança baseados em risco sem antes compreender quais dados possuem (um processo conhecido como inventário de dados), onde estão localizados (mapeamento de dados) e a natureza sensível desses dados (classificação de dados).

Esses processos também são essenciais em caso de incidente de violação de dados, para que as empresas possam compreender melhor se os dados afetados podem acionar obrigações legais, regulatórias ou contratuais de notificação de violações. Por essas razões, o inventário, o mapeamento e a classificação de dados são explicitamente exigidos ou um pré-requisito necessário para estar em conformidade com múltiplos frameworks. Por exemplo:

- A *Regra de Salvaguardas da FTC* (16 CFR § 314), que implementa requisitos para certas instituições financeiras sujeitas à GLBA, exige que as instituições financeiras cobertas identifiquem e avaliem a sensibilidade das informações dos clientes como parte de seu processo de avaliação de risco.
- A *Regra de Segurança da HIPAA* (45 CFR § 164.308) também obriga as entidades abrangidas a inventariar e proteger informações eletrônicas protegidas de saúde (“ePHI”).
- De acordo com o Artigo 30 do Regulamento Geral de Proteção de Dados da UE (“GDPR”), as organizações devem manter um registro das atividades de processamento, o que efetivamente exige um inventário de dados e mapeamento para demonstrar conformidade.
- As obrigações de notificação de violação de cada estado dos EUA normalmente são acionadas somente se determinados tipos de dados pessoais confidenciais relacionados aos residentes desse estado forem comprometidos. Assim, em um cenário de violação de dados, as empresas devem ser capazes de determinar quais categorias de dados estão incluídas em um conjunto de dados comprometido.
- Frameworks como o NIST SP 800-53 e os Controles CIS enfatizam a classificação de dados para garantir que as proteções estejam alinhadas com a sensibilidade dos dados. Ao estabelecer um esquema claro de inventário e classificação, as empresas podem implementar controles de acesso com mais confiança, monitorar fluxos sensíveis de dados, cumprir obrigações regulatórias e reduzir o risco de divulgação não autorizada.

Controles de acesso por função

Controles de acesso baseados em funções (“RBAC”) são medidas projetadas para garantir que os indivíduos tenham acesso apenas aos sistemas e dados necessários para desempenhar suas responsabilidades (um conceito também conhecido como “privilégio mínimo”). RBACs aplicados consistentemente reduzem o risco de acesso não autorizado por insiders maliciosos e podem ajudar a limitar o alcance de uma invasão. Muitos frameworks legais e industriais exigem explicitamente ou recomendam fortemente o RBAC:

- Sob o GDPR da UE, apenas pessoas devidamente autorizadas com necessidade de saber podem acessar dados pessoais. Indo ainda mais longe, o regulamento define o acesso não autorizado como um caso de violação de dados.
- As Normas de Massachusetts para a Proteção de Informações Pessoais, 201 CMR 17.04, exigem que as empresas que operam em Massachusetts implementem medidas seguras de controle de acesso que restrinjam o acesso a registros e arquivos contendo informações pessoais sensíveis apenas àqueles que necessitam dessas informações para desempenhar suas funções.
- A Regra de Segurança da HIPAA determina que o acesso à ePHI seja restrito a quem tenha uma necessidade legítima de saber.
- O artigo 9.º, n.º 4, da DORA da UE exige que as instituições financeiras abrangidas implementem políticas que limitem o acesso físico ou lógico aos ativos apenas ao que é necessário para funções e atividades legítimas e aprovadas.
- Padrões do setor, como o NIST SP 800-53, o ISO/IEC 27001 e os controles CIS (por exemplo, CIS Control 6), também enfatizam o RBAC como uma prática fundamental de gerenciamento de acesso.

Logging e monitoramento

Os logs de eventos de segurança estão entre os recursos mais importantes que as empresas têm para detectar incidentes de segurança. Logs que refletem informações como datas e horários de acesso, ações realizadas e o usuário que as realizou são fundamentais para verificar se o acesso ao sistema foi autorizado e investigar possíveis atividades não autorizadas. Monitorar os logs em tempo real ou quase em tempo real também é fundamental para detectar e lidar com ameaças em tempo hábil.

O gerenciamento de logs pode ser um desafio para organizações com sistemas complexos e diversos que podem gerar grandes volumes de logs todos os dias. Tais organizações devem confiar em soluções técnicas para agregar logs de forma eficaz e monitorá-los em busca de atividade anômala. Os frameworks legais e da indústria enfatizam a importância do logging e do monitoramento:

- O Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI-DSS) exige que todas as empresas que armazenam, transmitem ou processam dados de cartões de pagamento registrem logs e monitorem todo o acesso aos componentes do sistema e aos dados do titular do cartão.
- A Regra de Segurança da HIPAA exige que controles para auditar registrem e examinem a atividade em sistemas que contêm ePHI.
- A Seção SOX 404 exige que a administração e os auditores avaliem e relatem a eficácia dos controles internos das empresas públicas sobre o relatório financeiro. Esses auditores avaliam esses controles em relação a frameworks como o COBIT, que exigem logging de auditoria da atividade do usuário, acesso a sistemas financeiros e alterações nos dados financeiros.
- O componente “Detectar” do CSF do NIST especifica que as empresas devem registrar logs de eventos de segurança e manter um monitoramento contínuo da segurança, o que também é indispensável para o relatório oportuno de incidentes notificáveis, por exemplo, de acordo com o artigo 32 do GDPR da UE, o artigo 23 do NIS2 da UE ou o artigo 19 do DORA da UE.

Detecção e resposta a intrusões

É um fato lamentável que, no cenário atual de ameaças, toda organização seja um potencial alvo de ataques cibernéticos. As organizações devem manter sistemas e processos de detecção de intrusão para responder a incidentes de segurança no inevitável caso de uma tentativa de intrusão. Esses sistemas são fundamentais para que as empresas identifiquem e respondam rapidamente a um ataque antes que ele se transforme em um incidente grave. No entanto, sistemas de detecção de intrusão e processos de resposta a incidentes raramente são eficazes logo de fábrica; em vez disso, as empresas devem estabelecer uma linha base de atividade e adaptar os critérios de alerta aos atributos únicos da empresa. Essa adaptação aumenta a precisão dos alertas e ajuda a garantir que os incidentes sejam devidamente classificados e tratados de acordo com sua criticidade. A detecção e resposta a intrusões são centrais em diversos frameworks legais e industriais:

- Leis federais, estaduais e internacionais de notificação de violações dos EUA exigem que as violações de dados sejam reportadas dentro de prazos específicos. Embora seja comum pensar que o RGPD impõe o prazo mais curto para o relatório (dentro de 72 horas após a constatação de uma violação de dados que deve ser comunicada), vale ressaltar que a DORA exige que incidentes significativos relacionados às Tecnologias da Informação e Comunicação (“TIC”) sejam comunicados em até quatro horas após a sua descoberta.
- A Seção 500.16 do Regulamento de Segurança Cibernética do NYDFS exige que as entidades regulamentadas tenham planos de resposta a incidentes para responder prontamente e se recuperar de incidentes de segurança cibernética.
- A DORA também exige que as instituições financeiras reguladas desenvolvam planos detalhados de resposta a incidentes.
- O CSF do NIST especifica que as empresas mantenham controles detalhados de “Detecção” e “Resposta” para detectar e responder a incidentes de segurança.

O custo da não conformidade

Deixar de implementar controles de segurança eficazes e em conformidade pode expor as empresas, seus líderes e seus conselhos de administração a riscos jurídicos, financeiros e de reputação significativos. Do ponto de vista prático, organizações com ferramentas ou processos de monitoramento ineficazes correm o risco de sofrer acesso não autorizado prolongado, o que pode permitir que um invasor realize reconhecimento da empresa e imite com mais precisão as atividades autorizadas, além de vazar dados ou preparar o terreno para um ataque de ransomware. O logging incompleto também pode tornar impossível determinar se uma atividade suspeita ou inesperada foi autorizada, o que pode levar a uma notificação excessiva ou insuficiente.

No caso de uma violação de dados ou incidente de segurança cibernética, o mapeamento e o inventário de dados inadequados podem causar dificuldades na identificação dos dados afetados. Isso pode resultar em atrasos na notificação das partes e reguladores afetados. Esses atrasos, por sua vez, aumentam os danos potenciais sofridos pelas vítimas, violam os prazos regulatórios de relatórios e agravam o ônus imediato da recuperação e remediação com reivindicações adicionais de indenização, sanções regulatórias e custos adicionais de fiscalização e litígio. Para fornecedores B2B, isso também pode dificultar identificar quais clientes foram impactados por um incidente.

O não cumprimento dos requisitos de segurança afirmativos, como os impostos pelas leis de privacidade para proteger as informações pessoais, pode resultar em penalidades substanciais, multas e outras responsabilidades legais. Todas as empresas também enfrentam o risco de negligência, quebra de contrato ou outras ações judiciais (geralmente em ações coletivas) de demandantes cujas informações foram violadas em um incidente. Notavelmente, a Lei de Privacidade do Consumidor da Califórnia (CCPA) estabelece um direito privado de ação para os demandantes cujos dados confidenciais foram violados como resultado da falha da empresa em manter medidas de segurança “razoáveis”. Sanções e danos de acordo com regulamentações como HIPAA, CCPA ou o GDPR da UE podem rapidamente atingir valores na casa dos milhões.

Além das penalidades diretas de conformidade, danos à reputação causados por deficiência de segurança também podem ser severos. Empresas que sofrem uma violação ou não cumprem as regulamentações de segurança podem perder a confiança dos clientes, enfrentar reações negativas públicas, enfrentar interrupções significativas nos negócios e sofrer impactos de longo prazo no valor da marca. Empresas de capital aberto também correm o risco de impacto no valor das ações após falhas amplamente divulgadas em segurança. Os riscos incluem perda de clientes e possíveis exigências de compensação por não proteger adequadamente os dados dos clientes, levando à perda de negócios e receita. À luz dessas consequências significativas, as empresas devem levar a segurança a sério, investindo adequadamente nas obrigações de conformidade e mitigando os riscos de segurança.

Utilizando a Elastic para conformidade

A Elastic Platform é a base para as duas soluções prontas para uso da Elastic: Elastic Observability e Elastic Security. As organizações podem usar a plataforma aberta e flexível da Elastic para cumprir suas obrigações de conformidade e lidar com os principais riscos de segurança cibernética em vários canais. Mais importante ainda, as soluções da Elastic são inerentemente ágeis e escaláveis; elas podem ser implantadas e coletar dados de uma ampla variedade de sistemas e plataformas, e seus recursos de busca podem ser utilizados para inúmeros casos de uso. Abaixo estão apenas alguns exemplos de como a Elastic pode ser usada para apoiar os princípios fundamentais de um programa de segurança:

Mapeamento e classificação de dados

A Elastic pode apoiar esforços de mapeamento de dados indexando dados estruturados e não estruturados entre ambientes, proporcionando às organizações visibilidade centralizada sobre os tipos e localizações de seus dados. Usando tags personalizadas, metadados e machine learning, a Elastic pode ajudar a identificar padrões em dados (por exemplo, dados pessoais, registros financeiros, logs do sistema), facilitando a classificação dos dados com base em sensibilidade ou obrigações regulatórias. Embora a Elastic não seja um motor dedicado à classificação de dados, suas poderosas capacidades de busca e análise podem ser integradas a programas mais amplos de governança de dados para ajudar a rastrear e inventariar dados em sistemas em nuvem e no local.

Controle de acesso por função (RBAC)

Embora a Elastic não seja uma ferramenta RBAC, a plataforma pode ingerir logs nos sistemas de uma organização para ajudar a identificar lacunas no gerenciamento de permissões. As organizações podem analisar os padrões de acesso para identificar sistemas aos quais os grupos de usuários podem ou não precisar acessar e usar isso para informar a atribuição de privilégios de acesso. A Elastic também ajuda nossos clientes a realizar a ingestão de políticas de acesso de grupos de vários sistemas, permitindo que as empresas gerem relatórios a partir desses dados para demonstrar a aplicação dos direitos de acesso em auditorias ou investigações de conformidade. E a Elastic contém recursos RBAC integrados em suas interfaces Elastic Security e Kibana. Os administradores podem definir funções que limitam o acesso do usuário a índices, dashboards ou ações específicas (como visualização versus edição), apoiando os princípios de acesso com menos privilégios.

Logging e monitoramento

Um dos principais pontos fortes da Elastic, e um de seus casos de uso mais comuns, é a agregação, armazenamento e análise de logs em escala. Usando Elastic Agent, as empresas podem realizar a ingestão de logs de endpoints, servidores, serviços em nuvem e aplicações. Esses logs são indexados no Elasticsearch, permitindo análise e visualização em tempo real no Kibana. A Elastic oferece suporte à retenção de logs a longo prazo, alertas e detecção de anomalias, tornando-a uma solução ideal para agregação de logs e monitoramento de segurança, além de uma ferramenta eficaz para relatório de conformidade. Sua suíte de observabilidade também fornece monitoramento de performance de aplicação (APM), métricas e monitoramento de tempo de funcionamento para uma visibilidade holística da infraestrutura.

Muitas regulamentações, como a M-21-31 para agências do governo federal dos EUA, exigem que as organizações armazenem logs por um determinado período de tempo. A estrutura de hierarquização de dados da Elastic permite que os dados sejam armazenados de forma econômica com base na frequência e rapidez com que precisam ser acessados e usados. O modo de índice logsdb do Elasticsearch **reduz o espaço de armazenamento de dados de log em até 65%,** aumentando a visibilidade e a conformidade enquanto mantém todos os dados imediatamente acessíveis para análise.

Para citar apenas um exemplo, a Universidade de York fez a transição de seu sistema SIEM para o Elastic Security, a fim de aprimorar as capacidades de segurança cibernética, melhorar a eficiência operacional e reduzir custos. Ao implantar aproximadamente 9.000 agentes da Elastic em servidores, desktops e laptops e coletar logs de toda a infraestrutura híbrida de nuvem da universidade, incluindo Google Cloud, AWS, Azure e servidores no local, a Universidade ingere 500 gigabytes de dados por dia, com 35 terabytes de logs em armazenamento. Também se conecta a ferramentas de segurança como firewalls Palo Alto Networks, Cloudflare e Duo, garantindo monitoramento abrangente em diversas plataformas. Essa configuração permite buscas rápidas em grandes volumes de dados, reduzindo os tempos de consulta de horas para segundos.

Detecção e resposta a intrusões

Elastic Security inclui recursos de detecção e resposta a endpoints (EDR) e integra feeds de inteligência de ameaças para oferecer suporte à detecção de intrusões. Permite que as equipes de segurança monitorem ameaças conhecidas e desconhecidas usando análises comportamentais, mapeamento de ataques e regras de detecção personalizadas. Com o logging centralizado, os analistas podem rapidamente correlacionar eventos entre sistemas, investigar alertas em contexto e orquestrar fluxos de trabalho de resposta. A Elastic também oferece suporte a respostas automatizadas por meio de integrações com plataformas de orquestração, automação e resposta de segurança (SOAR) de terceiros, tornando-se uma ferramenta poderosa para melhorar a prontidão para resposta a incidentes e a caça a ameaças. Essas capacidades avançadas reduzem a probabilidade de uma violação e aceleram o tempo de resposta em caso de uma invasão bem-sucedida, o que, por sua vez, mitiga potenciais responsabilidades legais associadas a um incidente.

AHEAD, uma fornecedora líder de plataforma digital e de transformação, aprimorou significativamente suas capacidades de detecção e resposta a intrusões ao integrar o Elastic Security em seus serviços gerenciados de segurança. A AHEAD agora ingere dados de segurança dos clientes na Elastic executado no Elastic Cloud, onde os dados são enriquecidos, agregados e conectados a feeds de inteligência de ameaças. A Elastic também é a fonte de dados para o sistema SOAR da organização. Os analistas de segurança da AHEAD também podem aproveitar alarmes impulsionados por IA que destacam informações relevantes dentro de eventos de segurança, reduzindo o tempo necessário para peneirar manualmente grandes quantidades de dados e ajudando a diminuir a carga de falsos positivos.

Conclusão

À medida que o cenário das ameaças à segurança cibernética continua a apresentar desafios sofisticados para as organizações, cumprir a lista cada vez maior de requisitos regulatórios relacionados à segurança e privacidade de dados e reduzir riscos também se torna mais complexo. A falha em fazer isso expõe as empresas não apenas a consequências legais e financeiras significativas, mas também a danos operacionais e reputacionais. A Elastic pode ajudar os CIOs e CISOs a melhorar a conformidade de suas organizações com esses vários requisitos legais, especialmente nas áreas de mapeamento e classificação de dados, RBAC, logging e monitoramento, e detecção e resposta a intrusões.

