Centrify Privilege Threat Analytics Service

Controlos de Aprendizagem Automática para o Cenário Moderno de Ameaças

Os controlos Zero Trust Privilege precisam de ser adaptáveis ao contexto de risco. A Gartner promove CARTA – Continuous, Adaptive, Risk, and Trust Assessment – e também é absolutamente necessário para acesso privilegiado. Zero Trust Privilege significa saber que, mesmo que as credenciais corretas tenham sido introduzidas por um utilizador com privilégios, mas a solicitação entrar num contexto de risco, será necessária uma verificação mais forte para permitir o acesso. Os algoritmos modernos de aprendizagem automática são agora utilizados para analisar cuidadosamente o comportamento de um utilizador com privilégios e identificar atividades "anómalas" ou "não normais" (e, portanto, com risco acrescido) e aplicar o nível adequado de controlo para o risco correspondente.

O Cenário de Ameaças Atual Requer Controlos Adaptáveis

Os ciberadversários estão cada vez mais sofisticados e, por conseguinte, ao proteger contra o abuso de acesso privilegiado, a melhor prática é aplicar várias camadas de segurança. O cenário de ameaças atual requer a adaptabilidade dos controlos de segurança ao contexto de risco e a utilização da aprendizagem automática na análise cuidadosa do comportamento de utilizadores com privilégios.

Controlo adaptável significa não apenas notificar em tempo real sobre atividades de risco, mas também ser capaz de responder ativamente a incidentes terminando sessões, adicionando monitorização adicional ou sinalizando para acompanhamento forense.

A aprendizagem automática permite que as empresas analisem milhões de eventos e procurem, numa base permanente e contínua, aquela agulha no palheiro, o que nunca seria possível através da análise forense manual. Ainda mais valioso é executar, em linha e em tempo real, análises baseadas em aprendizagem automática e, assim, poder impor controlos preventivos genuinamente adaptativos e não apenas controlos de deteção depois da ocorrência.

Identificar Abuso de Acesso Privilegiado em Tempo Quase Real

O Centrify Privilege Threat Analytics Service aproveita as potencialidades da análise comportamental avançada em combinação com os recursos da autenticação multifator adaptativa (MFA) do Centrify Zero Trust Privilege para adicionar mais uma camada de segurança, aplicando MFA adaptativa para o comportamento anormal do utilizador. Aproveitar o Centrify Privilege Threat Analytics Service pode fazer a diferença entre tornar-se vítima de uma falha de segurança ou travá-la.

AUTENTICAÇÃO MULTIFATOR ADAPTATIVA

Adicione uma camada extra de segurança para travar a falha de segurança com MFA adaptável e com reconhecimento de riscos para administradores de TI que acedem a sistemas Windows e Linux, elevam privilégios ou aproveitam credenciais privilegiadas.

ANÁLISE COMPORTAMENTAL DO UTILIZADOR

Aproveite os algoritmos modernos de aprendizagem automática para analisar cuidadosamente o comportamento de um utilizador com privilégios e identificar atividades "anómalas" ou "não normais" e, portanto, com risco acrescido, além de alertar ou notificar a segurança. Também é aproveitada a deteção de atividades de risco quando forem tomadas decisões de controlo de acesso em tempo real, por exemplo, no contexto da autenticação ou do reforço da mesma. A análise comportamental de utilizadores com privilégios também pode ser utilizada para analisar os privilégios mais e menos utilizados e servir como uma função de governança para sugerir alterações em funções e direitos.

> **"Quando obtém uma ideia clara da variedade de capacidades oferecidas pelos Centrify Zero Trust Privilege Services, começa a entender a quantidade de verificações de segurança que trata. Ainda estou surpreso com a quantidade de problemas que consegui resolver com apenas esta solução individual."**
>
> — Matt Horn, Gestor de Operações de TI, GSI

Reforce o Acesso Seguro a Sistemas Críticos

Adicione uma camada extra de segurança somente quando necessário – e com base na classificação do risco – para reduzir a ameaça associada às credenciais privilegiadas comprometidas. Configure controlo de acesso baseado em comportamento para administradores de TI que acedem a servidores Windows e Linux, elevam privilégios ou aproveitam credenciais privilegiadas.

- Identifique comportamentos anómalos enquanto ocorrem ao impor políticas com reconhecimento de riscos para utilizadores que estão a iniciar uma sessão privilegiada, a verificar uma palavra-passe ou a elevar privilégios. A combinação de políticas que reconhecem riscos com controlos de acesso baseados em funções, o contexto do utilizador e MFA possibilita a tomada de decisões inteligentes, automatizadas e em tempo real sobre a concessão de acesso privilegiado. Estas políticas de acesso impostas dinamicamente concedem acesso ao utilizador, pedem um segundo fator de autenticação ou bloqueiam o acesso completamente.
- Centrify Zero Trust Privilege Services suportam a mais ampla variedade de autenticadores para providenciar a flexibilidade necessária à autenticação da sua equipa de TI utilizando o fator de forma mais conveniente, bem como permitir-lhe aproveitar sistemas e autenticadores MFA existentes dos quais já é proprietário. Autenticadores suportados por Centrify incluem:
  - Notificações push no telemóvel;
  - Perguntas de segurança;
  - Chamada telefónica com verificação do PIN;
  - tokens OATH;
  - Servidores de códigos de acesso únicos;
  - Chaves de segurança U2F FIDO; e
  - Cartões inteligentes (“smart cards”).
- As capacidades adaptativas da MFA do Centrify foram projetadas para funcionarem harmoniosamente com os investimentos existentes em RSA, tokens baseados em OATH e smart cards como PIV/CAC, podendo ser colocados sob a gestão centralizada do Centrify e impostos em toda a empresa.
- A app Centrify para telemóveis iOS e Android disponibiliza ao utilizador com privilégios uma interface simples onde recebe notificações MFA ou solicitações de fluxo de trabalho para aprovação. A app também disponibiliza uma interface para possibilitar que o utilizador faça a gestão de tokens OATH, nos quais a semente ou o segredo é armazenado em segurança pelo Centrify Privileged Access Service para dar suporte à validação de códigos OTP pelo utilizador, como exigido por várias aplicações ou serviços privilegiados que impõem a sua própria Validação MFA conforme OATH, como a Consola AWS®. Além disso, a app móvel suporta a proteção e check-out de palavras-passe em caso de emergência.
- O Centrify também suporta a disponibilização de serviços MFA para dispositivos de rede, como routers, switches ou firewalls, onde o acesso administrativo deveria exigir a MFA antes do acesso do utilizador com privilégios.

Aproveite a Análise Comportamental do Utilizador para Minimizar a Sua Exposição a Riscos

O cenário de ameaças atual requer a adaptabilidade dos controlos de segurança ao contexto de risco, utilizando a aprendizagem automática na análise cuidadosa do comportamento de utilizadores com privilégios. Controlo adaptável significa não apenas ser notificado em tempo real sobre atividades de risco, mas também ser capaz de responder ativamente a incidentes terminando sessões, adicionando monitorização adicional ou sinalizando para acompanhamento forense.

- Aproveite um conjunto de dashboards personalizáveis e widgets interativos para compreender melhor os riscos e os padrões de acesso em toda a sua infraestrutura. Ao ajustar a política de segurança ao comportamento de cada utilizador e sinalizar automaticamente o comportamento de risco, obtenha visibilidade imediata do risco para a conta, eliminando a sobrecarga de filtrar milhões de ficheiros de registo e enormes quantidades de dados históricos.
- Compreenda melhor o histórico de acessos e eventos ao analisar minuciosamente os detalhes relativos a eventos, entre sistemas, localização, tempo, comandos privilegiados e muito mais. Os utilizadores de TI podem analisar eventos individuais para compreender a natureza do risco de qualquer evento específico. O risco é determinado em tempo real para cada evento e expresso como alto, médio ou baixo para qualquer atividade anómala.
- Obtenha insights otimizados da atividade anómala com uma vista de linha cronológica detalhada. Identifique os fatores específicos que contribuem para uma anomalia a fim de obter uma compreensão abrangente de uma ameaça potencial, tudo a partir de uma única consola. As equipas de segurança podem visualizar o acesso ao sistema, a deteção de anomalias em alta resolução com ferramentas de análise, como dashboards, vistas de explorador e ferramentas de investigação.
- Dados de acesso privilegiado são capturados e armazenados a fim de permitir consultas robustas por ferramentas de gestão de registos e a integração com ferramentas de relatórios externas. Integrações otimizadas com ferramentas de SIEM, como Micro Focus® ArcSight™, IBM® QRadar™ e Splunk®, identificam rapidamente riscos ou atividades suspeitas.
- Aproveite qualquer aplicação compatível com Webhook (Slack® ou sistemas já existentes de resposta a incidentes, como o PagerDuty®, por exemplo) para ativar a entrega de alertas em tempo real, eliminando a necessidade de vários pontos de contato de alerta e melhorando o tempo de resposta. Se ocorrer um evento de alerta, o Centrify Privilege Threat Analytics Service permite ao utilizador disparar facilmente, através de Webhook, alertas para aplicações de terceiros. Esta capacidade possibilita que o utilizador responda a um alerta de ameaça e limite o impacto.
- Obtenha informações específicas e detalhadas sobre atividades de acesso privilegiado suspeitas. Os administradores de TI podem executar ações de remediação imediatas para proteger contra riscos potenciais ou uma ameaça em curso, diretamente a partir do ecrã de alerta, e terminar manual ou automaticamente uma sessão com base no risco.
- Os eventos analisados pelo Centrify Privilege Threat Analytics Service são utilizados para criar, para um utilizador, um perfil do padrão de comportamento normal em qualquer login ou atividade privilegiada, incluindo comandos, para que as anomalias possam ser identificadas em tempo real, permitindo um controlo de acesso baseado no risco. Eventos de alto risco são imediatamente sinalizados, alertados, notificados e elevados à atenção do departamento de TI, agilizando a análise e minimizando enormemente o esforço necessário para avaliar o risco nos atuais ambientes de TI híbridos.

A nossa missão é eliminar a principal causa de falhas de segurança: o abuso de acesso privilegiado. Com uma abordagem Zero Trust Privilege pronto para a nuvem, Centrify habilita os nossos clientes a protegerem o acesso à infraestrutura, a DevOps, à nuvem, aos containers, a Big Data e a outras superfícies de ataque de empresas modernas. Para saber mais, visite www.centrify.com.

EUA Sede +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Ásia Pacífico +61 1300 795 789
Brasil +55 11 3958 4876
América Latina +1 305 900 5354
sales@centrify.com

www.centrify.com