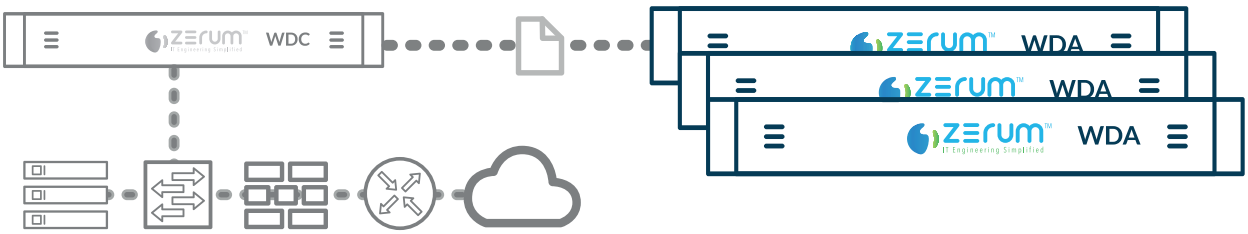
Zerum Falcon™ WDA

O **Zerum Falcon™ WDA** indexa, armazena e analisa os dados recebidos dos appliances **Zerum Falcon™ WDC**. Com recursos avançados de Big Data e Inteligência Artificial, o WDA fornece mecanismos de análise e busca textual de alta performance, além de escalabilidade horizontal, suportando o armazenamento de centenas de terabytes em cluster. Faz parte da família de produtos **Zerum Falcon™**, a solução integrada de monitoramento e análise de dados da Zerum.



Funcionalidades

Busca e análise

Buscas e filtro
Permite a busca textual em todos os campos e valores armazenados.

Armazenamento, indexação e retenção dos metadados decodificados
Todos os dados enviados pelo Zerum Falcon™ WDC são indexados e então armazenados em shards distribuídos em um ou mais WDAs.

Extração customizada de campos e valores
Permite que o usuário extraia a informação de campo/valor de dentro de valores já armazenados, para fins de busca e construção de gráficos.

Detalhamento de eventos
Permite a visualização de todos os detalhes de um determinado evento, incluindo transações relacionadas (quando houver) e reconstrução de conteúdo (quando houver).

Dashboards customizados
Permite ao cliente adicionar à mesma página todos os gráficos e tabelas das análises que deseja realizar. Diversos dashboards podem ser criados simultaneamente e organizados em diferentes workspaces. É possível alterar a posição (com drag and drop) e redimensionar os painéis do dashboards.

Análises por protocolo
Para cada protocolo licenciado, a interface disponibiliza um dashboard dedicado que facilita a análise de milhares de eventos de forma simultânea, com opção de drill down para investigação detalhada.

Exportar eventos para arquivo CSV
Dados exibidos nas tabelas podem ser exportados para arquivos CSV (comumente usados para importação em planilhas eletrônicas, como Excel).

Criar gráficos de barras, linhas, área, dispersão, bullet e pizza
Permite a criação de diferentes visualizações para os dados selecionados/filtrados, no período escolhido – com granularidade de até 1 (um) segundo.

Alarmes

Acionamento facilmente customizável, baseado em metadados de transações e dos flows em rede
Os alarmes estão disponíveis para todos os protocolos licenciados, podendo ser configurados para disparar em diversos cenários, como:

- Erros em aplicações;
- Nível de utilização de rede, por aplicações, IPs, portas, etc;
- Falhas em rede (retransmissões, falhas em conexões TCP, zero window);
- Problemas de performance de aplicações e banco de dados;
- Eventos de segurança.

Acionamento com busca por campo/valor e comparação com valores estáticos
O usuário pode definir quais campos devem ser observados e quais valores (números ou texto) causam o disparo dos alarmes. Exemplo: disparar quando encontrar a palavra "CPF" no conteúdo de um Body HTTP. A busca também pode ser feita com REGEX.

Acionamento com busca por campo/valor e comparação com valores de baselines dinâmicas
Permite que o usuário escolha quais campos devem ser observados, sendo o valor a ser comparado provido pelo algoritmo de baseline dinâmica da solução.

Aprendizado da baseline
O período e ciclo de aprendizado (ex.: 2 dias, 2 semanas) para determinada(s) baseline(s) podem ser definidos pelo usuário, usando histórico de eventos e possibilitando aprendizado contínuo.

Limite/Acumulador
Usuário pode determinar se e como deseja acumular eventos que acionam condições de disparo de alarmes. Pode ser feito por valor estático, porcentagem de eventos e baseline dinâmica, ajudando a reduzir a quantidade de "ruído".

Agrupadores/Classificadores
Permite ao usuário subdividir a análise e visualização dos alarmes por um determinado conjunto de valores, extraídos de um campo. É possível, por exemplo, visualizar todos os alarmes de erros em aplicações separados pelos valores do campo Host.

Notificações via CEF e e-mail
Quando disparados, alarmes podem notificar os usuários através da própria interface (tela de alarmes), mensagem de e-mail para um grupo de envio e/ou mensagem do tipo CEF para um servidor de eventos (SIEM).

Grupos de envio
Permite o cadastro de diversos e-mails que irão receber notificações, por grupos, facilitando a configuração e gerência dos destinatários.

Outras funcionalidades

Limite de acesso aos dados, por grupo/ambiente de usuário
A interface do usuário se adapta ao tamanho da janela e pode ser acessada através de vários navegadores de Internet, como IE, Chrome, Firefox e Safari.

Geolocalização de endereços IP
Permite identificar a localidade (país e cidade) de um determinado IP. Assim, podem ser exibidos, por exemplo, a quantidade de dados enviados/recebidos, ou a performance das transações com origem/destino de cada país. O sistema permite ainda o cadastramento da geolocalização de redes corporativas e privadas, para maior efetividade da solução de GeoIP.

Interface responsiva em HTML5
A interface do usuário responsiva adequa a exibição do conteúdo ao tamanho da janela, podendo ser acessada através de diversos navegadores de Internet, como IE, Chrome, Firefox e Safari.

Armazenamento escalável horizontalmente
Além do armazenamento local é possível aumentar o espaço de armazenamento do sistema apenas com a adição de outros appliances WDA. Dessa forma também é possível espelhar os dados, em diferentes níveis de redundância, e ter alta disponibilidade.

Modelo

Appliance disponível no modelo:

Zerum Falcon™ WDA

Capacidade de análise: **Até 20 mil transações por segundo**

Armazenamento: **Até 20 Tb**

Sobre a Zerum

A Zerum desenvolve produtos inovadores que aliam Inteligência Artificial e Big, Fast e Machine Data para acelerar a compreensão dos dados em movimento e proporcionar visibilidade e entendimento em tempo real a grandes organizações.

Para mais informações, fale com um de nossos representantes ou acesse www.zerum.com.

Especificações Técnicas

Chassi	
Tamanho	1U montável em rack
Dimensões e peso	
Altura	1.7" (43mm)
Largura	17.2" (437mm)
Profundidade	27.82" (707mm)
Peso bruto	48lbs (21.8kg)
Baias de drive NVMe	
Hot-swap	10x 2.5" baias de drive NVMe Hot-swap
Drives NVMe	Até 10x drives NVMe
Refrigeração do sistema	
Exaustores	8 Exaustores com controle de velocidade otimizado
Fonte de alimentação	
Quantidade	2 Fontes de alimentação redundantes
Potência	1000W com PMBus
Ambiente operacional / Conformidade	
RoHS	Em conformidade com RoHS
Especificações ambientais	
Temperatura operacional	De 10°C a 35°C (50°F a 95°F)
Temperatura de armazenamento	De -40°C a 60°C (-40°F a 140°F)
Umidade relativa operacional	De 8% a 90% (sem condensação)
Umidade relativa de armazenamento	De 5% a 95% (sem condensação)
Rede	
Interface de gerência	• 2 portas Ethernet 10/100/1000 RJ45 • 1 porta IPMI LAN dedicada RJ45

Part number	Descrição
ZRM-WDA	Appliance WDA base (sem armazenamento)
ZRM-WDA400G	Módulo WDA de armazenamento NVMe de 400GB
ZRM-WDA1TB	Módulo WDA de armazenamento NVMe de 1TB
ZRM-WDA2TB	Módulo WDA de armazenamento NVMe de 2TB
ZRM-WDAORAC	Licença WDA para análise de protocolo TNS Oracle
ZRM-WDADB2	Licença WDA para análise de protocolo DRDA DB2
ZRM-WDASQLS	Licença WDA para análise de protocolo TDS SQL Server
ZRM-WDAPSQL	Licença WDA para análise de protocolo PostgreSQL
ZRM-WDAMSQL	Licença WDA para análise de protocolo MySQL
ZRM-WDAFCOE	Licença WDA para análise FCOE
ZRM-WDASVC	Suporte/Garantia de 12 meses p/ WDA