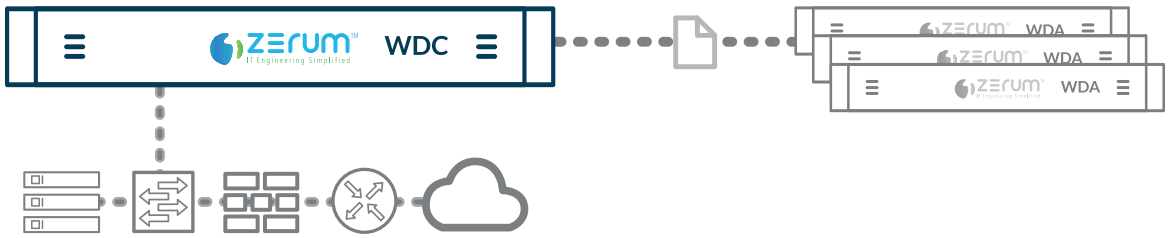
Zerum Falcon™ WDC

O appliance **Zerum Falcon™ WDC** coleta e decodifica eventos e transações de diversos protocolos diretamente da rede, em tempo real. Com alta performance, o appliance processa até 20Gbps de tráfego e decodifica 20 mil transações por segundo, enviando os dados para indexação, armazenagem e processamento pelo **Zerum Falcon™ WDA**. Faz parte da família de produtos **Zerum Falcon™**, a solução integrada de monitoramento e análise de dados da Zerum.



Funcionalidades

Decodificação de transações e extração de metadados em tempo real
O appliance decodifica e extrai metadados de transações dos seguintes protocolos de aplicações, infraestrutura e bancos de dados:

- Hypertext Transfer Protocol (HTTP), versões 1.0 e 1.1;
- Hypertext Transfer Protocol Secure (HTTPS);
- Apache JServ Protocol (AJP);
- Domain Name System (DNS);
- Lightweight Directory Access Protocol (LDAP);
- Fibre Channel over Ethernet (FCoE);
- Oracle Transparent Network Substrate (TNS);
- Tabular Data Stream (TDS);
- Distributed Relational Database Architecture (DRDA);
- PostgreSQL (pgsql);
- MySQL.

Análise de performance de cada transação
Coleta as seguintes métricas de performance, de todas as transações:

- Server Connection Time (tempo para abertura da conexão TCP);
- Client Time (tempo para execução da requisição pelo cliente);
- Server Processing Time (tempo para resposta do servidor, após o request);
- Data Transfer Time (tempo necessário para envios da resposta completa);
- Quantidade de retransmissões TCP;
- Quantidade de pacotes com mensagem de Zero Window.

As métricas são armazenadas de forma individual, sem qualquer tipo de sumarização dos dados.

Análise de TCP
Decodificação e armazenamento do estado das conexões, inclusive sessões TCP não iniciadas corretamente ou que terminaram em erro.

Cálculo de retransmissões e zero windows
Informa quantas retransmissões e zero windows ocorreram por origem e destino de cada evento decodificado dos protocolos suportados.

Classificação de flows com DPI
A classificação com Deep Packet Inspection (DPI) identifica a aplicação mesmo em fluxos de dados criptografados. As seguintes aplicações podem ser detectadas nos flows:

FTP, POP, SMTP, IMAP, DNS, HTTP, NTP, NETBIOS, NFS, BGP, SNMP, SMB, SYSLOG, DHCP, PostgreSQL, MySQL, TDS, VMware, Kazaa/Fasttrack, eDonkey, Bittorrent, Flash, MPEG, QuickTime, RealMedia, Windowsmedia, RTSP, IRC, Jabber, MSN, Yahoo, VRRP, Telnet, STUN, IPSEC, GRE, ICMP, IGMP, SCTP, OSPF, IP in IP, RTP, RDP, VNC, PCAnywhere, SSL, SSH, TFTP, SIP, ICMPv6, DHCPv6, Kerberos, LDAP, msSQL, PPTP, FaceBook, Twitter, DropBox, Gmail, Google Maps, YouTube, Skype, Google, sFlow, HTTP Proxy, Netflix, Citrix, CitrixOnline/GotoMeeting, Webex, WhatsApp, Apple iCloud, Viber, Apple iTunes, Radius, WindowsUpdate, TeamViewer, LotusNotes, SAP, GTP, UPnP, LLMNR, RemoteScan, Spotify, H323, OpenVPN, CiscoVPN, RTCP, RSYNC, Oracle, CNN, Wikipedia, Redis, ZeroMQ, QUIC, WhatsApp Voice, Teredo, Snapchat, OpenSignal, 99Taxi, GloboTV, Deezer, Instagram, entre outras.

Cadastro de aplicações internas
Permite que o usuário cadastre suas aplicações internas, utilizando parâmetros como IP e porta, para identificação pelo sistema de Deep Packet Inspection.

Coleta de dados sem perda de pacotes via SPAN, RSPAN e "taps" em redes 1/10/40GbE
O appliance possui interfaces especializadas para coleta de pacotes espelhados, com buffers maiores que placas comuns e capacidade para registrar o timestamp diretamente via hardware, com precisão de nanossegundos, além de outras funcionalidades como desduplicação de pacotes e hashing (distribuição de tráfego para vários cores).

Coleta de tráfego entre máquinas virtuais
O appliance recebe tráfego em espelhamento ERSPAN (Encapsulated Remote SPAN), para monitoramento em tempo real de transações entre máquinas virtuais e/ou redes remotas.

Descriptografia de SSL/TLS
Permite a descriptografia de túneis SSL/TLS que utilizam a cifra RSA, com performance acelerada por hardware de até 10 Gigabits e 20 mil transações por segundo.

Extração de metadados de flows
Extrai metadados de todos os flows que chegam ao appliance, incluindo Datetime, Bytes, IPs da Tupla, MACs da Tupla, portas da Tupla, aplicação (pela tabela do IANA), aplicação (pelo DPI). Alguns dados possuem prefixo Lower (relativo à porta mais baixa na Tupla) ou Upper (relativo à porta mais alta na Tupla).

Exportação de dados
Todas as informações coletadas são estruturadas em formato JSON e enviadas via protocolo AMPQ (Advanced Message Queuing Protocol) para integração com outros dispositivos de análise e armazenamento de dados. Por padrão, as informações são enviadas para o appliance Zerum Falcon™ WDA.

Trigger monitor
Possibilita a busca em todo o conteúdo dos pacotes recebidos nas interfaces de captura usando expressões regulares ou texto puro, armazenando automaticamente metadados como endereçamento IP, portas, timestamp e payload ao detectar o conteúdo procurado.

Filtro de tráfego nas interface de coleta Ethernet
Permite ao usuário filtrar qual tráfego será capturado e analisado. O filtro é feito utilizando informações de endereçamento IP, máscaras de rede, protocolos e portas TCP/UDP.

Coleta e armazenamento de pacotes
Permite a coleta e o armazenamento de pacotes em formato CAP, através das interfaces de monitoração.

Extração de conteúdo HTTP
O appliance WDC é capaz de reconstruir todo o "body" HTML das transações em HTTP. Com isso, é possível analisar eventos que contêm formulários e outros dados relevantes.

Modelos

Appliance disponível em três modelos:

WDC4	WDC10	WDC20
Capacidade de captura	Capacidade de captura	Capacidade de captura
Até 4Gbps	**Até 10Gbps**	**Até 20Gbps**
Interfaces de captura	Interfaces de captura	Interfaces de captura
8 portas 1 Gigabit	**8 portas 10 Gigabit**	**8 portas 10 Gigabit**

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
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
Interface de captura de pacotes*	

10 Gigabit	• Interface física: 2 portas SFP/SFP+
	• Módulos SFP suportados: Multi-mode SX, single-mode LX e ZX, 1000BASE-T ou 10/100/1000 BASE-T
	• Módulos SFP+ suportados: 10GBASE-SR, singlemode LR e ER, 10GBASE-CR
	• Desempenho (taxa de captura): 2 x 10 Gbps
	• Resolução de time stamp do hardware: nanossegundos
	• Sincronização de tempo:
	  • Conectores externos: conectores dedicados
	  • Conectores internos: 2 para suporte daisy-chain
	• RAM Onboard: 4 Gb DDR3

Gigabit	• Interface física: 4 portas SFP
	• Módulos 1G SFP suportados: 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX e 10/100/1000BASE-T
	• Desempenho (taxa de captura): 4 x 1 Gbps
	• Resolução de time stamp do hardware: nanossegundos
	• Sincronização de tempo:
	  • Conectores externos: conectores dedicados
	  • Conectores internos: 2 para suporte daisy-chain
	• RAM Onboard: 2 Gb DDR3

* Quantidade e tipos de Interfaces de captura de pacotes do appliance são customizadas de acordo com a demanda.

Part number	Descrição
ZRM-WDC	Appliance WDC base (1Gbps)
ZRM-WDCGb	Licenciamento para o WDC (+ 1 Gigabit por segundo)
ZRM-WDCSSL	Módulo WDC para descriptografia de SSL
ZRM-WDC10G	Módulo para WDC com duas portas de captura 10 Gigabit
ZRM-WDC1G	Módulo para WDC com quatro portas de captura Gigabit
ZRM-WDCSVC	Suporte/Garantia de 12 meses para WDC