PREDSTAVUJEME

Jednoduchá a flexibilná správa

- GUI na webe.
- Veľký výber kontroly prístupov podľa funkcie na obmedzenie prístupu do GUI a k dátam na rôznych úrovniach.
- Všetka komunikácia medzi modulmi chránená HTTPS.
- Kompletná auditná stopa aktivít používateľa FortiSIEM.
- Jednoduchý upgrade softvéru s minimálnou odstávkou a stratou udalostí.
- Jednoduchá aktualizácia FortiSIEM-u (parsery, pravidlá, hlásenia).
- Archivácia na základe opatrení.
- Hešovanie logov pre preverenie integrity.
- Flexibilná autentifikácia používateľov – miestna, externá s Microsoft AD a OpenLDAP, Cloud SSO/SAML pomocou Okta.
- Možnosť prihlásenia do vzdialeného severu cez FortiSIEM GUI pomocou vzdialeného tunelu SSH.

Jednoduché škálovanie virtualizovanej štruktúry

- Prístupné ako virtuálne stroje na lokálne a verejné/súkromné nasadenie Cloudu na nasledujúcich hypervizoroch — VMware ESX, Microsoft HyperV, KVM, Xen, Amazon Web Services AMI, OpenStack, Azure.
- Škálovanie zberu dát nasadením virtuálnych strojov Collector.
- Collectori dokážu bufferovať udalosti, ak je cloud FortiSIEM-u nepristupný.
- Škálovanie analýz nasadením virtuálnych strojov Worker.
- Zabudovaná štruktúra vyrovnania zaťaženia na zber udalostí zo vzdialených miest pomocou Collectorov.

Centrum informácií o ohrozeniach

- FortiSIEM posiela anonymne udalosti do FortiSIEM cloudu.
- Usúvzťaňnenie viacerých programov FortiSIEM identifikuje možné hrozby a vyvíjajúci sa malvér.

Monitorovanie dostupnosti

- Monitorovanie funkčnosti systému — cez Ping, SNMP, WMI, Uptime Analysis, Critical Interface, Critical Process a Service.
- BGP/OSPF/EIGRP zmenu stavu, Storage port.
- Dostupnosť služieb modelovaná cez Synthetic. Transaction Monitoring — Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, a pre porty TCP/UDP.
- Monitorovanie hardvéru a prostredia.
- Kalendár údržieb na plánovanie času na údržbu.
- SLA kalkulácia — s ohľadom na "normálny" pracovný čas a nadčasy.

ŠPECIFIKÁCIE

FortiSIEM Windows Agent

Fortinet vyvinul efektívnu technológiu na zber informácií bez agentov. Externý zber informácií ako monitorovanie integrity súborov je však drahý. FortSIEM skombinoval svoju technológiu bez agentov s novo-vyvinutými vysokovýkonnými agentmi na značné vylepšenie zberu dát.

	TECHNOLÓGIA BEZ AGENTA	ZÁKLADNÝ AGENT	POKROČILÝ AGENT
Bez agenta			
Zistenie	•		
Monitorovanie výkonu	•		
(nízky výkon) Zber systémových, aplikačných a bezpečnostných logov	•		
Agenti			
(vysoký výkon) Zber systémových, aplikačných a bezpečnostných logov		•	•
Zber DNS, DHCP, DFS, IIS Logov		•	•
Až do 1800 udalostí/sekunda/server nízka latencia		•	•

	TECHNOLÓGIA BEZ AGENTA	ZÁKLADNÝ AGENT	POKROČILÝ AGENT
Až 500 agentov na manažéra		•	•
Miestna normalizácia parsingu a času		•	•
Detekcia nainštalovaného softvéru			•
Monitorovani zmien v registri			•
Monitorovanie integrity súborov			•
Monitorovanie logových súborov zákazníka			•
Monitoovanie WMI Command Output			•
Monitorovanie PowerShell Command Output			•

INFORMÁCIE O OBJEDNÁVKE

Licenčná schéma

Licencie FortiSIEM poskytujú základné funkcie pre zistenie zariadení v sieti. Zariadenia sú vrátane switchov, routerov, firewallov, serverov, atď. Každé monitorované zariadenie vyžaduje licenciu. Všetky licencie podporujú zachytávanie údajov a ich koreláciu, výstrahy, hlásenia, analýzy, vyhľadávanie a optimalizovaný repozitár dát a zahŕňajú 10 EPS (udalostí za sekundu). "EPS" je mierka výkonu udávajúca, koľko správ, či udalostí sa vytvára každým zariadením za sekundu. Dodatočné EPS sa dá dokúpiť podľa potreby. Licencie sú prístupné vo forme predplatného, alebo ako stála verzia.

PRODUKT	SKU	POPIS
FortiSIEM All-In-One		
FortiSIEM All-In-One Perpetual License	FSM-AIO-BASE	Základná stála licencia pre bezpečnostné a monitorovacie služby všetko v jednom. Do 50 zariadení a 500 EPS.
	FSM-AIO-XXXX-UG	Pridanie XXXX zariadení a XXXX EPS ku stálej licencii.
FortiSIEM All-In-One Subscription License	FSM-AIO-BASE-DD	Základná predplatená licencia pre monitorovacie a bezpečnostné služby všetko v jednom. Do 50 zariadení a 500 EPS.
	FSM-AIO-XXXX-UG-DD	Pridanie XXXX zariadení a XXXX EPS k predplatenej licencii.
FortiCare Support for FortiSIEM All-In-One License	FC[1-8]-10-FSM00-248-02-DD	24x7 FortiCare zmluva o podpore (YYYY zariadení)
FortiSIEM Windows Agent		
FortiSIEM Perpetual License for Basic Windows Agent	FSM-WIN-BASE	Základná stála licencia na 50 základných agentov Windows.
	FSM-WIN-XXXX-UG	Pridanie XXXX základných agentov Windows ku stálej licencii.
FortiSIEM Subscription License for Basic Windows Agent	FSM-WIN-BASE-DD	Základná predplatená licencia na 50 základných agentov Windows.
	FSM-WIN-XXXX-UG-DD	Pridanie XXXX základných agentov Windows k predplatenej licencii.
FortiSIEM Perpetual License for Advanced Windows Agent	FSM-WIN-ADV-BASE	Základná stála licencia na 50 pokročilých agentov Windows.
	FSM-WIN-ADV-XXXX-UG	Pridanie XXXX pokročilých agentov Windows ku stálej licencii.
FortiSIEM Subscription License for Advanced Windows Agent	FSM-WIN-ADV-BASE-DD	Základná predplatená licencia na 50 pokročilých agentov Windows.
	FSM-WIN-ADV-XXXX-UG-DD	Pridanie XXXX pokročilých agentov Windows k predplatenej licencii.
FortiCare Support for FortiSIEM Windows Agent License	FC[1-8]-10-FSM01-248-02-DD	24x7 FortiCare zmluva o podpore (YYYY zariadení)

FORTISIEM ALL-IN-ONE ENTITLEMENT	ZÁKLAD	VYŠŠIE ÚROVNE (XXXX)						
	Základ	100	250	450	950	1950	3950	4950
Počet zariadení	50	100	250	450	950	1,950	3,950	4,950
Počet EPS	500	1,000	2,500	4,500	9,500	19,500	39,500	49,500

FORTISIEM WINDOWS AGENT ENTITLEMENT	ZÁKLAD	VYŠŠIE ÚROVNE (XXXX)						
	Základ	100	250	450	950	1950	3950	4950
Počet Agentov Windows	50	100	250	450	950	1,950	3,950	4,950

FORTICARE ENTITLEMENT	MOŽNOSTI							
	1	2	3	4	5	6	7	8
Počet zariadení (YYYY)	1–50	1–150	1–300	1–500	1–1,00	1–2,000	1–4,000	1–5,000

FORTINET

GLOBAL HEADQUARTERS
Fortinet Inc.
899 KIFER ROAD
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

FST-PROD-DS-FSIEM

FSIEM-DAT-R2-201701

FORTINET

FortiSIEM®

Zlúčenie korelácie udalostí a manažmentu rizika pre moderné siete

Bezpečnosť už nie je len o ochrane informácií, pre udržanie dôvery klientov vrátane ochrany značky a reputácie organizácie je rozhodujúcim faktorom.

Jednoduchšie dodržiavanie bezpečnosti

Zákazníci odchádzajú pre porušenia bezpečnosti, čo zapríčiňuje materiálny a výrazne negatívny vplyv na základ spoločnosti. Odhaduje sa, že prilákanie nových zákazníkov je sedemkrát drahšie ako udržanie už existujúcich zákazníkov. Pokuty a právne poplatky sa môžu rýchlo nahromadiť. Verejné obchodné spoločnosti môžu badať negatívny a trvalý vplyv na hodnotu akcií, vzťahy s dodávateľmi a na názory akcionárov. Toto všetko vysvetľuje, prečo sa vedenie firiem čoraz viac zapája do rozhodnutí o bezpečnosti. FortiSIEM ponúka spoločnostiam komplexné, holistické a škálovateľné riešenie od prepájania zariadení s internetom až po úložisko Cloud, s patentovanými analýzami, ktoré sa dajú využiť na dôslednú správu bezpečnosti siete, výkonu a dodržiavania noriem, to všetko cez jednu obrazovku s nadhľadom na celú spoločnosť.

Zjednotená analýza operačných centier sieti a bezpečnosti (patentované)

Fortinet vyvinul štruktúru umožňujúcu zjednotenú a usúvzťaž-nenú analýzu z rozličných informačných zdrojov vrátane logov, merania výkonu, SNMP trapov, bezpečnostných výstrah a zmien v nastaveniach. V zásade si berie FortSIEM analýzy bežne monitorované operačnými centrami sietí a bezpečnosti zvlášť a údaje spája pre kompletnejší pohľad na dáta o ohrozeniach prístupné spoločnosti. Všetky informácie sa premenia na udalosti, tieto sa rozoberú a dodajú do analyzačného nástroja podľa udalostí na spracovanie vyhľadávania v reálnom čase, pravidiel, obrazoviek a ad hoc otázok.

Vlastnosti

- Zjednotená neustála analýza siete.
- Všetko na jednej obrazovke.
- Viac užívateľov naraz.
- Pripravené na MSP/MSSP.
- Zjednotenie analýz bezpečnostného a sieťového operačného centra.
- Databáza, ktorá sa učí.
- Škálovateľnosť na Cloud-e.
- Nekonvenčné dodržiavanie bezpečnosti.

VLASTNOSTI

Externé informácie o hrozbách (TI) z otvorených zdrojov informácií o hrozbách, komerčných zdrojov a vlastných zdrojov dát sa ľahko integrujú do štruktúry FortiSIEM TI. Veľkolepé zjednotenie rozličných zdrojov dát umožňuje organizáciám rýchle vytváranie komplexných správ na rýchlejšiu identifikáciu hlavných príčin hrozieb a podniknúť kroky potrebné na ich odstránenie, ako aj budúcu prevenciu pred nimi.

Distribuované usúvzťažnenie udalostí v reálnom čase (patentované)

Distribuované usúvzťažnenie udalostí je komplikovaný problém, keďže na generovanie pravidla zdieľa ich čiastkové stavy viac uzlov. Veľa predajcov SIEM má distribuovaný zber dát a možnosť distribuovaného vyhľadávania, ale Fortinet je jediný predajca so distribučným systémom usúvzťažnenia udalostí v reálnom čase. Komplikované vzory udalostí sa tak môžu detekovať v reálnom čase s minimálnym odstupom. Tento patentovaný algoritmus umožňuje FortiSIEM-u pracovať s veľkým množstvom pravidiel v reálnom čase aj pri vysokom počte udalostí pre vylepšenie času detekcie.

Automatické zisťovanie infraštruktúry a systém zisťovania aplikácií (CMDB)

Rýchle riešenie problémov vyžaduje kontext infraštruktúry. Väčšina analýz logov a predajcov SIEM vyžaduje administrátorov manuálne zadať kontext, čo sa môže rýchlo stať banálnym a je náchylné na ľudské chyby. Fortinet vyvinul inteligentnú infraštruktúru a systém zisťovania aplikácií, ktorý dokáže zistiť a zmapovať topológiu nielen fyzickej, ale aj virtuálnej infraštruktúry, lokálnych aj verejných/súkromných cloudových úložísk jednoducho použitím poverenia bez predošlej informácie o tom, aké zariadenia či aplikácie sa používajú.

Zisťovanie je rozsiahle (zahŕňa veľké množstvo predajcov úrovne 1/2/3 a ide do hĺbky (zahŕňa systém, hardvér, softvér, aktuálne služby, aplikácie, úložiská, používateľov, nastavenie siete, topológiu a vzťahy medzi zariadeniami). Zisťovanie môže prebiehať na požiadanie alebo plánovane na zistenie (v reálnom čase) zmien infraštruktúry a podať správu o všetkých nových zistených zariadeniach a aplikáciách. Toto je podstatná časť spravovania dodržiavania noriem, ktoré dokáže FortiSIEM splniť výnimočným spôsobom. Aktualizovaná CMDB (Databáza centrálnej správy) umožňuje sofistikovanú analýzu udalostí podľa kontextu pomocou použitia objektov CMDB v nastaveniach vyhľadávania.

Dynamické mapovanie identity užívateľov

Podstatným kontextom pri analýze logov je spojenie identity na sieti (IP adresa, MAC adresa) s identitou používateľa (meno logu, celé meno, funkcia v organizácii). Tieto informácie sa neustále menia, keď používatelia získajú nové adresy cez DHCP alebo VPN.

Fortinet vyvinul dynamickú metodológiu mapovania identity používateľov. Najprv sa zistia používatelia a ich funkcia z lokálnych zdrojov ako je Microsoft Active Directory a Open LDAP, alebo z cloudových zdrojov SSO ako je OKTA. Toto sa spúšťa na vyžiadanie alebo plánovane, aby sa zistili noví používatelia. Zároveň sa identita na sieti zistí z dôležitých udalostí na sieti ako preklad sieťovej adresy firewall-u, prihlásení cez Active Directory, prihlásení VPN, WLAN prihlásení, registračných logov Host Agent, atď. Nakoniec FortiSIEM vytvorí skombinovaním identity používateľa, sieťovej identity a geo-identity v distribuovanej pamäťovej databáze v reálnom čase dynamickú auditnú stopu identity používateľa. Umožňuje to vytvárať opatrenia, či vykonávať vyšetrenia založené na identite používateľa, nie IP adries, čo urýchľuje riešenie problémov.

Flexibilný a rýchly systém analýzy logov (patentované)

Efektívna analýza logov vyžaduje vlastné skripty, ale tie môžu pracovať veľmi pomaly, hlavne pri logoch s veľkým objemom ako Active Directory, logy firewall-u, atď. Kompilované kódy pracujú na druhej strane rýchlejšie, ale nie sú flexibilné a vyžadujú nové verzie. Fortinet vyvinul jazyk analýzy udalostí na báze XML, ktorý funguje ako programovací jazyk vysokej úrovne a ľahko sa modifikuje a zároveň sa dá kompilovať počas prevádzky aby bol efektívnejší. Všetky parsingy od FortiSIEM-u prekonávajú ponuku od väčšiny konkurentov, keďže používajú patentované riešenie a dajú sa parsovať aj nad 10K EPS na sieťový uzol.

Hybridná štruktúra databázy – využívanie feed-u údajov s aj bez štruktúry

FortiSIEM využíva dve rozličné zdroje informácií – zistené informácie sú štruktúrované dáta vhodné pre tradičnú relačnú databázu, kým logy, merania výkonu, atď. sú dáta bez štruktúry a potrebujú databázu typu NoSQL. Fortinet vyvinul hybridný prístup, dáta sa ukladajú v optimizovaných databázach s unikátnou logikou poskytujúcou jednu komplexnú databázovú vrstvu.
Používateľ dokáže vyhľadávať udalosti (uložené v NoSQL databáze) pomocou CMDB objektov (uložených v relačnej databáze). Tento prístup využíva potenciál a benefity oboch databáz.

Veľká miera integrácie informácií o ohrozeniach

Zákazníci majú k dispozícii veľa zdrojov na odber informácií o externých ohrozeniach pri správe potenciálnych rizík v sieti. Tieto informácie o ohrozeniach môžu však byť obrovské, obsahovať milióny IP adries, domén malvérov, hašov a URL a tieto informácie môžu rýchlo zastarať, keď sa stránky s malvérom a domény stiahnu a opäť nahrajú. Predstavuje to významnú výzvu pre spotrebiteľov ohrozujúcich dát. Fortinet vyvinul originálne algoritmy umožňujúce získať veľa informácií zo zdroja rýchlo a efektívne ich podať do rozličných uzlov FortiSIEM a vyhodnotiť ich rýchlejšie ako iní dodávatelia (viac ako 10K EPS na uzol).

Poskytovanie služby pre veľké spoločnosti pre viacerých užívateľov

Fortinet vyvinul prispôsobiteľnú štruktúru pre viacerých používateľov, čo umožňuje spoločnostiam a poskytovateľom služieb spravovať veľké množstvo fyzických/logických domén a prekrývajúcich sa systémov a sietí z jedného panelu.
V takomto prostredí je jednoduchšie usúvzťažniť informácie naprieč fyzickými a logickými doménami a individuálnymi sieťami zákazníka. Jednotlivé správy, pravidlá a panely sa dajú jednoducho vybudovať pre každý z nich so schopnosťou zaviesť ich naprieč veľkou sadou domén a zákazníkov. Opatrenia ukladajúce udalosti sa môžu zaviesť aj na každú doménu, alebo na zákazníka.

PREDSTAVUJEME

Operačný kontext v reálnom čase pre rýchlu analýzu bezpečnosti

- Nepretržitá aktualizácia a presný kontext zariadenia – nastavenie, nainštalovaný softvér a patch-e, prebiehajúce úkony.
- Analýzy výkonu systému a aplikácií s kontextuálnymi medzi relačnými údajmi pre rýchlu prioritizáciu bezpečnostných problémov.
- Kontext používateľa v reálnom čase, s auditnou stopou IP adries, zmenami identity používateľa, fyzický a zmapovaný kontext umiestnenia dát.
- Zistenie neoprávnených zariadení a aplikácií v sieti, zmien v nastaveniach.

Ihneď prístupné správy o dodržiavaní noriem

- Ihneď prístupné preddefinované správy podporujúce širokú škálu auditov dodržiavania noriem a správcovských potrieb vrátane – PCI-DSS, SOX, NERC, FISMA, ISO, GLBA, GPG13, SANS Critical Controls.

Monitorovanie výkonu

- Monitorovanie základných systémových údajov.
- Úroveň systému SNMP, WMI, PowerShell.
- Úroveň aplikácie JMX, WMI, PowerShell.
- Virtualizačné monitorovanie pre VMware, HyperV — guest, host, resource pool a úroveň klastrov.
- Využívanie úložiska, monitorovanie výkonu - EMC, NetApp, Isilon, Nutanix, Nimble, Data Domain.
- Špecializovaný monitoring výkonu aplikácií.
- Microsoft Active Directory a Exchange s pomocou WMI a Powershell-u.
- Databázy — Oracle, MS SQL, MySQL cez JDBC.
- VoIP infraštruktúra cez IPSLA, SNMP, CDR/CMR.
- Analýza flow a výkonu aplikácií — Netflow, SFlow, Cisco AVC, NBAR.
- Možnosť pridať vlastnej metriky.
- Základná metrika a zistenie značných odchýlok.

Monitorovanie zmien nastavení v reálnom čase

- Zbieranie súborov o nastaveniach siete, uložených vo verziách.
- Zbieranie údajov o verziách nainštalovaného softvéru, uložených vo verziách.
- Automatické zistenie zmien nastavení siete a nainštalovaného softvéru.
- Automatické zistenie zmien v súboroch a folderoch pre Windows a Linux s detailami.
- Automatické zistenie zmien z odsúhlaseného konfiguračného súboru.
- Automatické zistenie zmien v registri pomocou agenta FortiSIEM.

Kontext zariadenia a aplikácií

- Zariadenia siete (switche, routery, Wireless LAN.
- Bezpečnostné zariadenia — Firewally, IPS sietí, Web/Email brány, ochrana pred malvérom, skenovanie zraniteľnosti.
- Servery vrátane Windows, Linux, AIX, HP UX.
- Infraštruktúrne služby vrátane DNS, DHCP, DFS, AAA, VoIP.
- Aplikácie používateľov vrátane Web serverov, App serverov, Mail, databáz.
- Úložné zariadenia vrátane NetApp, EMC, Isilon, Nutanix, Data Domain.
- Cloud aplikácie vrátane AWS, Box.com, Okta, Salesforce.com.
- Cloud infraštruktúry vrátane AWS.
- Environmentálne zariadenia vrátane UPS, HVAC, hardvér zariadenia.
- Virtualizačná infraštruktúra vrátane VMware ESX, Microsoft HyperVScalable a flexibilného zberu logov.

Škálovateľný a flexibilný zber logov

- Zbieranie, triedenie, normalizácia, indexovanie and uloženie bezpečnostných logov rýchlo (nad 10K udalostí/sek na uzol).
- Ihneď prístupná podpora pre široký záber bezpečnostných systémov a API, lokálne aj cez cloud.
- Windows Agent poskytuje škálovateľný a rozsiahly zber udalostí vrátane monitorovania integrity súborov, zmien nainštalovaných súborov a monitorovanie zmien v registri.
- Linux Agent pre monitorovanie integrity súborov.
- Zmena triedenia z GUI a jej zavedenie na bežiacom systéme bez odstávky a straty udalostí.
- Vytváranie nového triedenia (XML vzorov) cez integrovaný vývoj parserov a zdieľanie používateľom cez funkciu export/import.
- Bezpečný a spoľahlivý zber udalostí od používateľov a zariadení nezávisle od ich umiestnenia.

Notifikácie a správa prípadov

- Systém notifikácie incidentov na základe opatrení.
- Možnosť spustiť remediačný skript pri výskyte špecifického incidentu.
- Integrácia externých tiketov n základe API — ServiceNow, ConnectWise, and Remedy.
- Zabudovaný systém tiketov.

Bohatá prispôsobiteľná platforma

- Nastaviteľná platforma v reálnom čase s kľúčovými ukazovateľmi výkonnosti.
- Zdieľanie správ a analýz organizáciám a používateľom.
- Farebné kódovanie na rýchlu identifikáciu hlavných problémov.
- Rýchlosť — aktualizované výpočtami v rámci pamäti.
- Špecializovaná vrstvená platforma pre obchodné služby, virtualizovanú infraštruktúru a špecializované aplikácie.

Integrácia informácií o externých ohrozeniach

- API na integráciu informácií o externých ohrozeniach — malvérové domény, IP adresy, URL, haše, Tor uzly.
- Zabudovaná integrácia populárnych zdrojov informácií o ohrozeniach — ThreatStream, CyberArk, SANS, Zeus.
- Technológia pre zaobchádzanie s veľkými zdrojmi o ohrozeniach.

Silné a škálovateľné analýzy

- Vyhľadávanie udalostí bez potreby indexácie.
- Vyhľadávanie na základe kľúčových slov a vyhľadávanie na základe vlastností parsovaných udalostí.
- Vyhľadávanie v histórii — vyhľadávanie podobné SQL s podmienkami filtrovania Boolean, zoskupenie podľa relevantných agregácií, časových filtrov, zhôd v GUI a API.
- Spúšťač pri komplexných vzoroch udalostí v reálnom čase.
- Použitie objavených objektov CMDB a používateľa/identity a dát o polohe vo vyhľadávaniach a pravidlách.
- Plánovanie správ a doručenie výsledkov emailom hlavným akcionárom.
- Vyhľadávanie udalostí v celej organizácii alebo obmedzene na fyzickú alebo logickú doménu.
- Dynamické kontrolné zoznamy na sledovanie kritických narušiteľov – s možnosťou použiť takéto sledovanie v ako pravidlo hlásenia.
- Škálovanie zdrojov pre analýzu pridaním uzlov Worker bez odstávky.
- Prioritizácia hlásenia incidentov sa môže zaviesť cez hlavný Business Service.

Baselining a odhalenie štatistických anomálií

- Baseline správanie koncového bodu/serveru/používateľa —granularita hodinová alebo cez pracovné dni/víkend.
- Vysoko flexibilné — všetky sady kľúčov a metrík sa dá “baselinovať”.
- Zabudované a nastaviteľné spúšťače pri štatistických anomáliách.

Integrácia externých technológií

- Integrácia s externou webstránkou na vyhľadanie IP adresy.
- Integrácia na základe API pre externé zdroje informácií o ohrozeniach.
- Dvojsmerná API integrácia so systémom helpdesk — okamžitá podpora pre ServiceNow, ConnectWise a Remedy.
- Dvojsmerná API integrácia s externým CMDB — okamžitá podpora ServiceNow a ConnectWise.
- Podpora Kafka pre integráciu s vylepšeným hlásením analýz — t.j. ELK, Tableau a Hadoop.
- API pre ľahkú integráciu so systémom provisioning.
- API na pridávanie organizácií, vytváranie poverení, spúšťanie zisťovania, obmenu udalostí monitorovania.