

riverbed[®]

Think fast.[®]

riverbed[®]

Think fast.[®]

Riverbed Performance Management

Dipl.-Ing. Alexander Tomik
RPM Solutions Architect

DoS, nás se to netýká?

Správy - Regiony - Služby - Nakupujte - SME.sk

TECHsme.sk Všetko zo sveta vedy a techniky

DOMOV INTERNET MOBIl TESTY A RECENZIE HARDVÉR HRV VESMÍR ČLOVEK BIOLÓGIA FOTOGALÉRIE TANAJ.SME.SK RECENZIE

Zaútočili na web SME.sk, išlo o rekordný útok

Vydanie: 10:00

Po zatvorení volebných miestností prebiehal rozsiahly kyberútok na internetovú stránku denníka SME. Útočili v sobotu a nedeľu.

BRATISLAVA. Online verzia denníka SME sa v noci zo soboty na nedeľu stala terčom rozsiahleho kyberútoku. Na niekoľko hodín nebola internetová stránka vôbec dostupná, útok prítom prebiehal aj počas nedele.

Útok sa zastavil v nedeľu vo večerných hodinách, obranné opatrenia pred kyberútokom však zostali naďalej spustené. To zneškodňovalo prístup na web

Top: 24 hodín 3 dni 7 dní

1. Zaútočili na web SME.sk, išlo o rekordný útok 68 354
2. Takéto zbraňové síly vyrábajú ľudia na Ukrajině. Maj na internete #76 1 804
3. Z možia dotkla vyčítať podoba cudzej tvare 7 665
4. Briti zdieľajú kopírovanie motorových diel 4 551
5. Vedci urobili krok k umeleému životu, otvorili syntetický chromozóm 3 267
6. V Austrálii chcú na 3D tlačiarňami vytlačiť poschodový dom 2 788
7. Alkohol škodí aj na začiatku tehotenstva 2 154

Preraca zľavy

Wellness pobyt na Liptove so vstupom do Gino 62% zľava

<http://tech.sme.sk/c/7153647/zautocili-na-web-smesk-islo-o-rekordny-utok.html>

Žijeme v IT světě bez hranic.

Borderless Network ve smyslu Cisco - umožňuje organizacím připojit kohokoliv, kdekoliv, kdykoliv a na jakémkoliv zařízení - bezpečně, spolehlivě a bez problémů.

Vy, Váš počítač a Vaše data
vždy spolu.



1960

Vytvořené hranice
IT architekturou



Budoucnost IT bez
hranic.



2015

Nové úlohy, staré nástroje

Úlohy 21. století...



-
-
-
-
-
-

video

lasu a

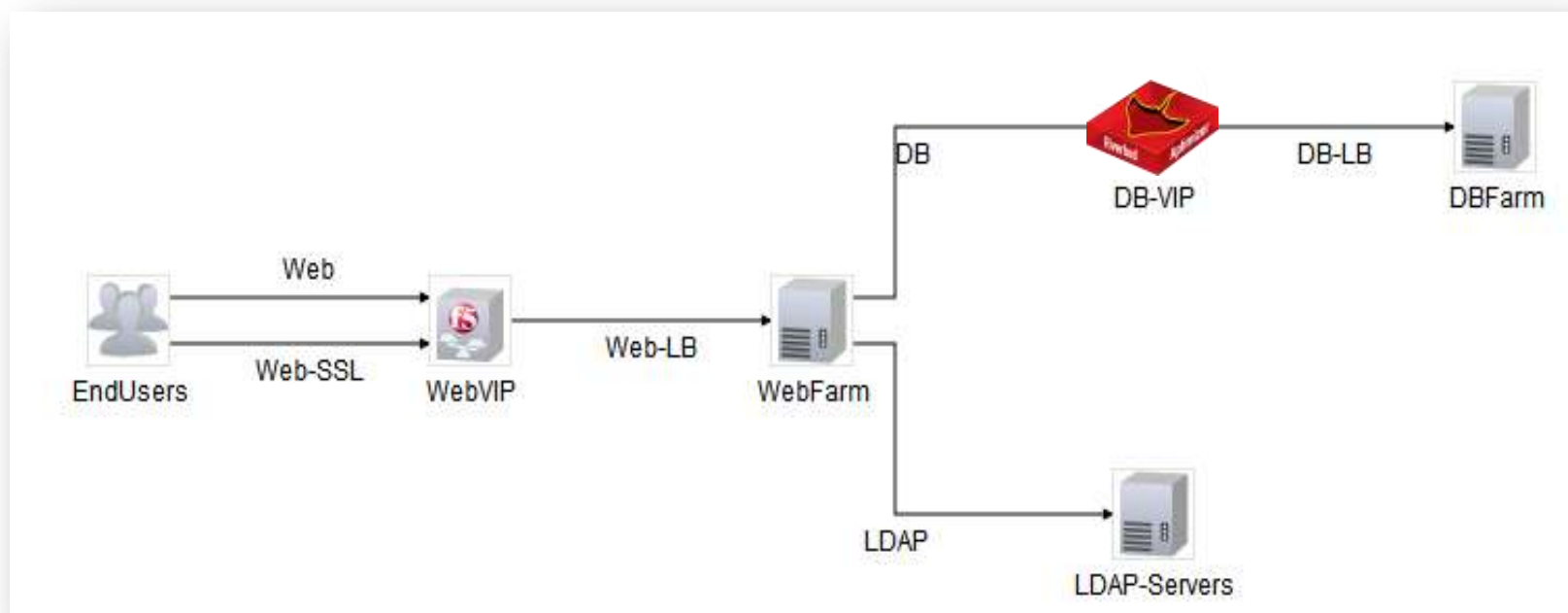
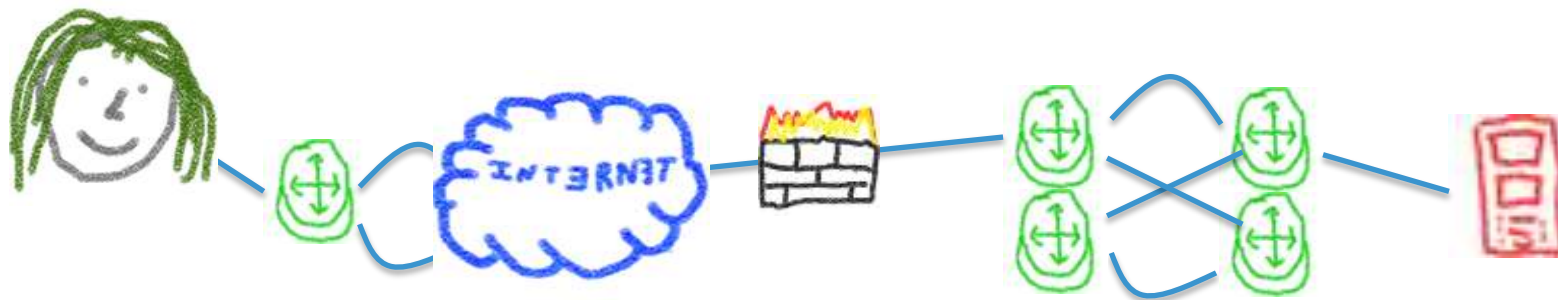
... nástroje 20. století

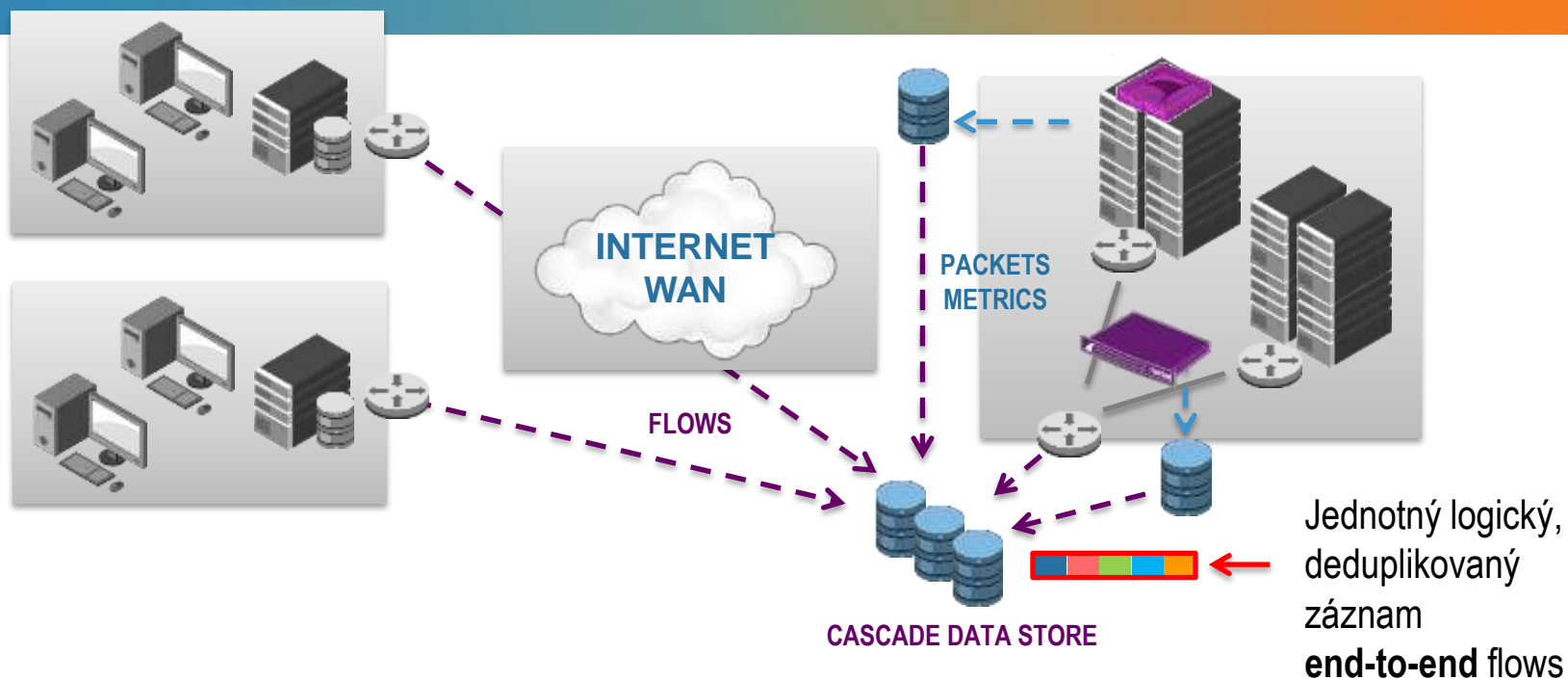


-
-
-

Mo
Ne
An

Znát všechny komponenty!





- **Flow data** poskytuje efektivní viditelnost end-to-end
- **Packet data** poskytuje podrobný přehled o výkonu aplikací - v případě potřeby

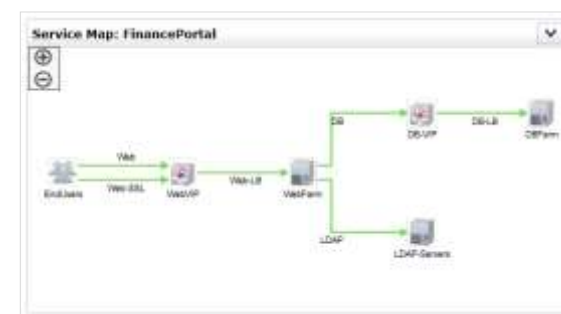
Automatizovaný monitoring

Service Health				
Service Tree	Overall	Connect	User Exp.	EFF
Exchange				
Sharepoint				
Oracle				
ERP				
Twiki				

Dashboards:

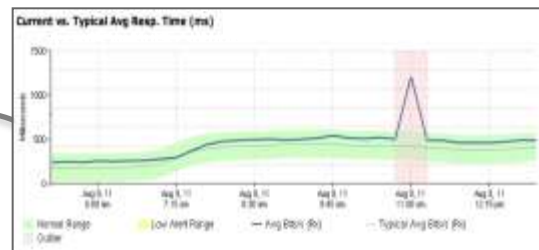
Nástěnka s náhledem stavu sítě a aplikací.

Nástroje na vytváření map a nástěnek

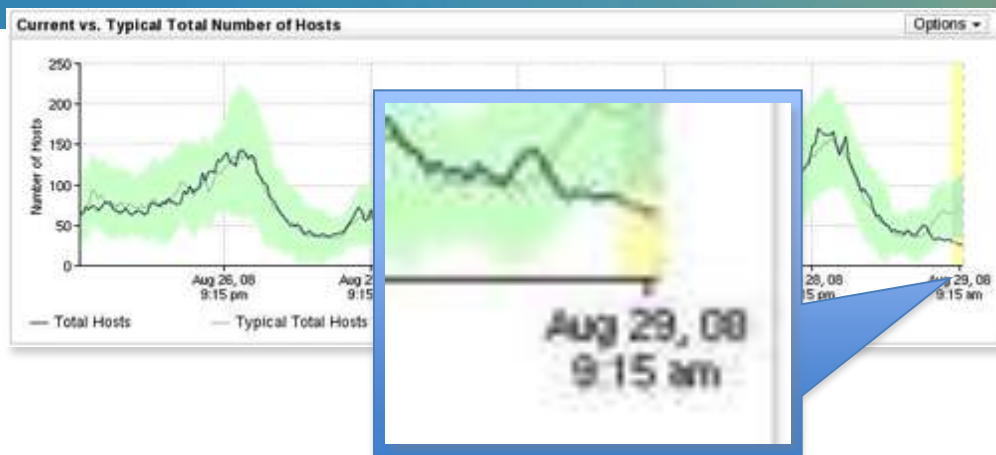


Discovery:

Rychle objevit všechny komponenty aplikace.



Analyze: Automatizovaná analýza změn v chování a zabezpečení včasného varování.

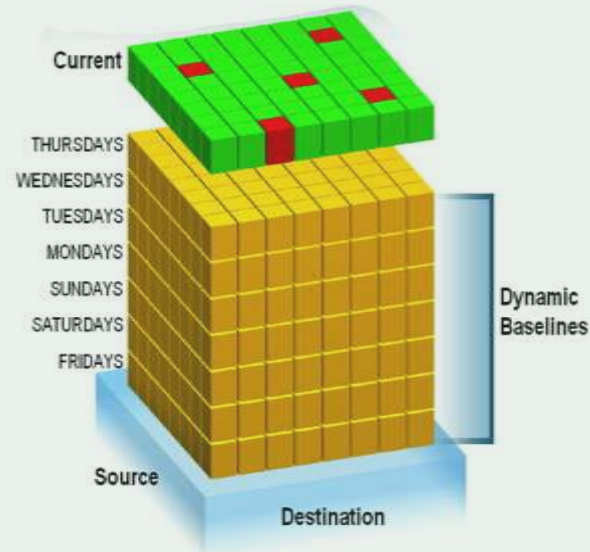


Normalizace dat umožňuje sledovat četné bezpečnostní a výkonnostní metriky ve vaší síti.

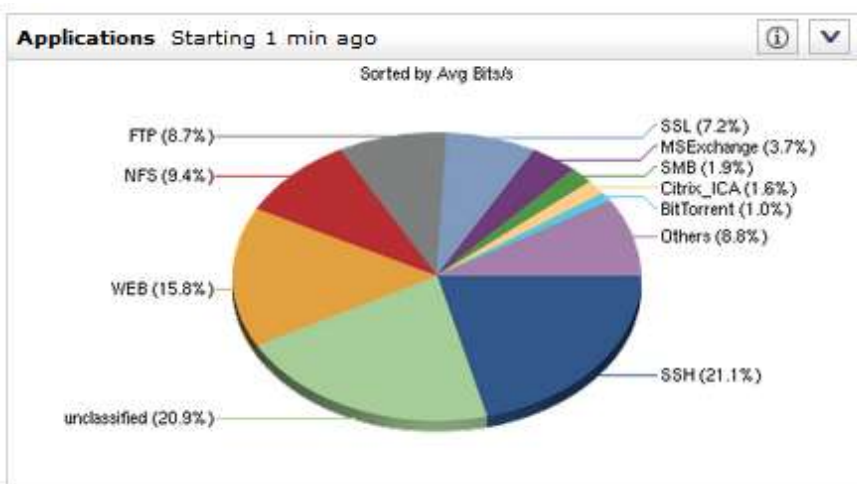
Jakmile systém vytvoří základní linii (šedá čára) můžete nastavit toleranci pro změnu (zelená cesta). Kdykoliv aktuální chování (modrá čára) překročí nakonfigurovanou toleranci, systém pošle upozornění.

Podezřelá spojení

- Kdo s kým
- Jaký protokol
- Přes jaký port
- Které dny, kterou hodinu
- Jakou aplikaci
- Jakou šířku pásma spotřebuje
- Jak často
- Kdo právě používá dané zařízení



Kompletní viditelnost sítě



Event Report (Mar 1, 2014 8:48 AM - Mar 31, 2014 9:48 AM)



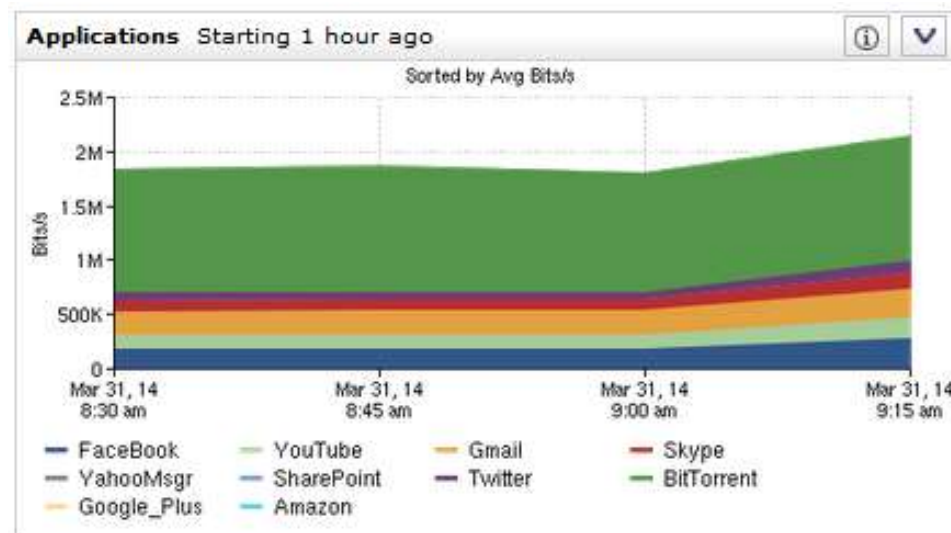
Triggering Policies: Within Security
Time frame behavior: The event period overlaps the time frame

Event List

Events 21 - 40 of 266

Event ID	Alert Level	Severity	Analytic	Policy	Start Time	Duration	Source	Destination
112171	High	100	Host Scan	Host Scan	Mar 30, 2014 9:37 AM	3 minutes 32 seconds	192.168.50.12	Multiple
112035	Med	86	Host Scan	Host Scan	Mar 30, 2014 9:26 AM	51 minutes 57 seconds	colomail-bu.opnet.com	Multiple
111260	Low	64	Worm	Worm	Mar 30, 2014 8:37 AM	3 minutes 59 seconds	Multiple	Multiple
110238	Med	86	Host Scan	Host Scan	Mar 30, 2014 7:26 AM	51 minutes 59 seconds	colomail-bu.opnet.com	Multiple
108982	Med	86	Host Scan	Host Scan	Mar 30, 2014 5:26 AM	51 minutes 58 seconds	colomail-bu.opnet.com	Multiple

- Zjistit, které aplikace jsou v naší síti
- Rozpoznat důležité a “rekreační” aplikace
- Získat viditelnost aplikace - kdo, kdy a odkud aplikaci využíval
- Alarmovat při podezřelém chování



ANALÝZA PROBLÉMU V SÍTI

riverbed

Problém s vysokým vytížením sítě.

Jaké aplikace mám v síti?

Podme nalézt server.

Kto to způsobil?

Našli jsme. Je to John Smith!



Host Pair 1 - 4 of 4

Server	Server Group	Client	Client Group	Avg Bits/s ↓
10.65.3.83	Cambridge	10.192.30.127	Cambridge	20,395,288 (99%)
10.65.3.83	Cambridge	10.192.30.130	Cambridge	93,129 (< 1%) 23 (< 1%)
10.65.3.83	Cs			42,137 (< 1%) 11 (< 1%)
10.65.3.83	Cs			2,502 (< 1%) 3 (< 1%)
Total				533,056 (100%)

Host Info Report
Server Info Report
User Report
External Links
Vulnerability Scan

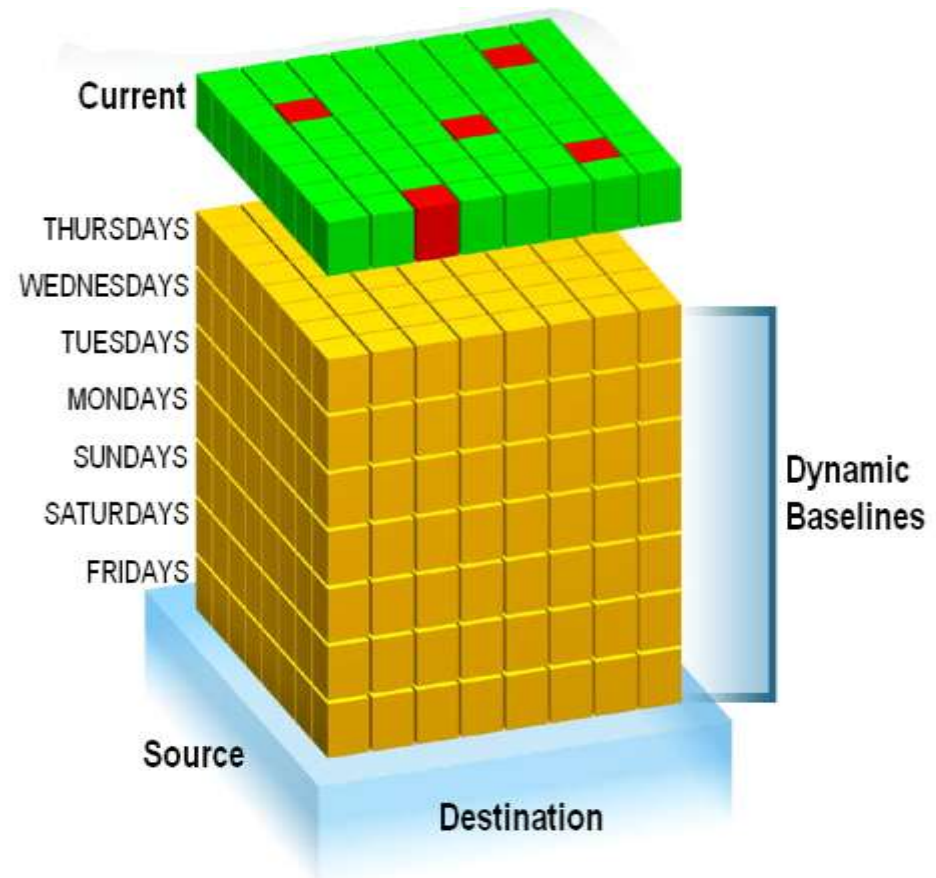
Preserve Timeframe
Last 5 Minutes

User

Host	Time ↓	User	Name	Domain	AD Source	Logged In
<input type="checkbox"/> Workstation-7	Dec 16, 2009 12:30 PM	john-smith		riverbed.com	172.31.0.39	Yes

Traffic between these Hosts in Context
Packets for this Host
Packets between these Hosts

- Host Scans
- Port Scans
- Worm Detection
- New Service/Application
- New Host
- Suspicious Connection
- DoS
- Tunneled Applications
- P2P & BOTS
- User Defined Policies



Configured Policies						
<input checked="" type="checkbox"/> Show alert counts for the last day Global Policy Settings...						
Name *	Low Alerts	Medium Alerts	High Alerts	Enabled	Actions	
DoS/Bandwidth Surge	0	0	0	Yes	Advanced settings	Disable
Host Scan	0	0	2	Yes	Advanced settings	Disable
New Host	0	0	0	Yes	Advanced settings	Disable
New Server Port	0	0	0	Yes	Advanced settings	Disable
Port Scan	0	0	1	Yes	Advanced settings	Disable
Suspicious Connection	0	0	0	Yes	Advanced settings	Disable
Worm	0	0	1	Yes	Advanced settings	Disable

Analýza chování sítě jako jsou DOS útoky, skenování portů, podezřelých serverů DHCP, nových hostů, červy a další.

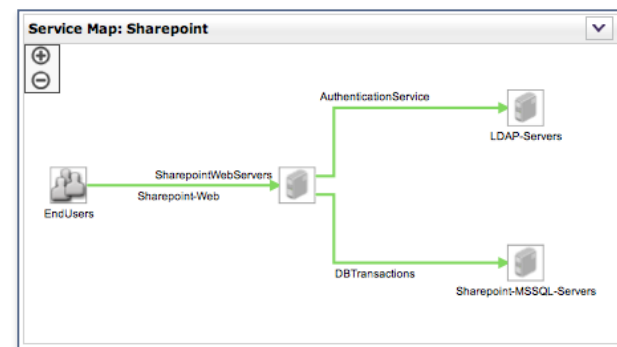
Analýza chování detekuje události založené bez podpisů.



User Defined Policies						
Analytic	Name *	Schedule		Severity	Enabled	Actions
Host	Compliance-RegulatedAccess	Daily	12:00 AM-11:59 PM	100	Yes	View Edit Delete Copy Disable
Host	Firewall Tunneling Activity	Daily	12:00 AM-11:59 PM	50	No	View Edit Delete Copy Enable
Host	P2P Application Activity	Daily	12:00 AM-11:59 PM	100	No	View Edit Delete Copy Enable
Host	P2P Port Activity	Daily	12:00 AM-11:59 PM	75	No	View Edit Delete Copy Enable
Interface	Service Assurance	Weekdays	8:00 AM-5:59 PM	100	No	View Edit Delete Copy Enable
Host	SpamBot Activity	Daily	12:00 AM-11:59 PM	100	No	View Edit Delete Copy Enable
Host	Tunneled Application Activity	Daily	12:00 AM-11:59 PM	75	No	View Edit Delete Copy Enable
Interface	VoIP is not tagged correctly	Daily	12:00 AM-11:59 PM	100	Yes	View Edit Delete Copy Disable

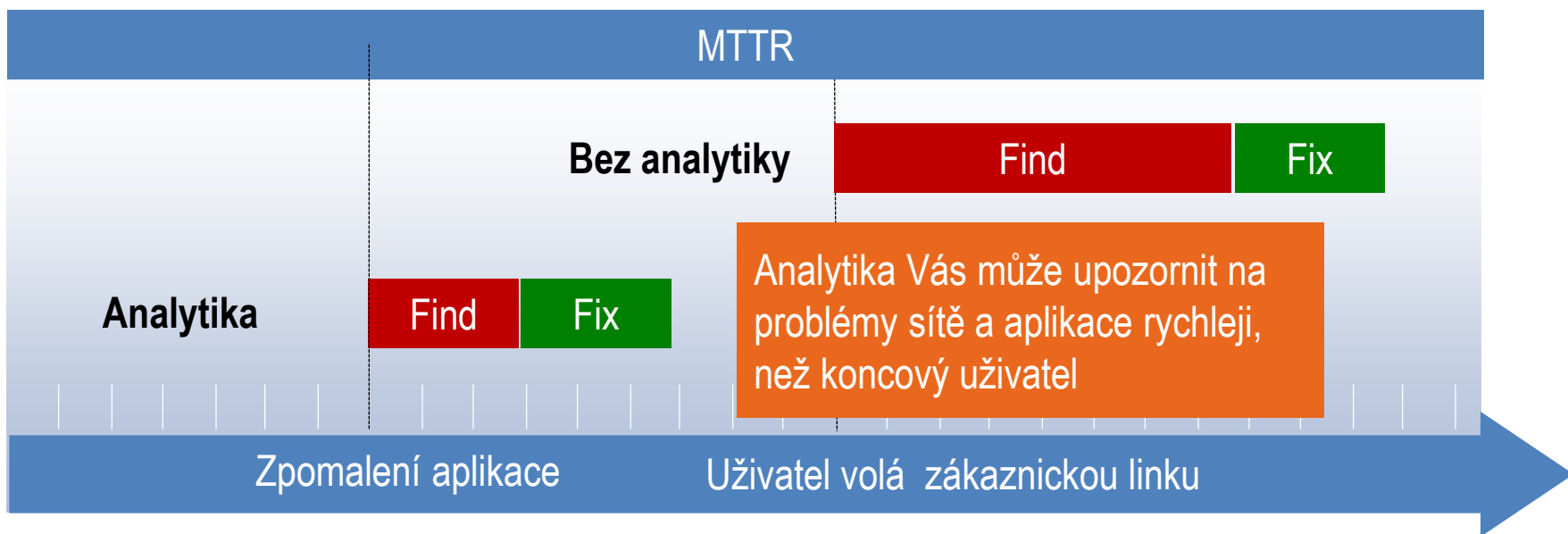
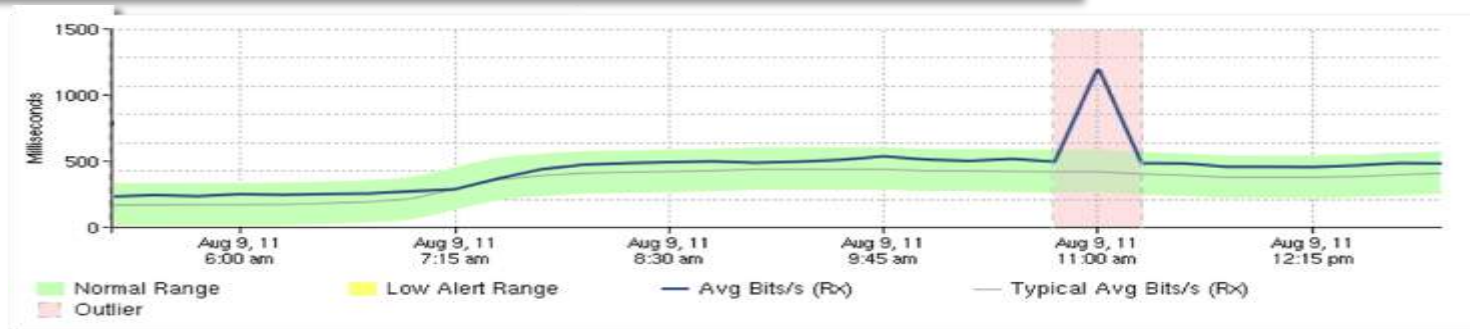
Další postupy pro nepřipustné chování, jako jsou P2P, tunelování a spam činnosti.

Monitorování Vašich firemních aplikací v reálném čase.



INTELIGENTNÍ MONITORING S DYNAMICKOU ANALÝZOU CHOVÁNÍ

Doba odezvy se odchyľuje od normální a spustí se výstraha.



Děkuji!

riverbed